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

На правах рукописи

Поспелов Алексей Дмитриевич

Сложность умножения в ассоциативных алгебрах

Специальность 01.01.09 – дискретная математика
и математическая кибернетика

Автореферат
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2008

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 механико-математического факультета МГУ Гашков Сергей Борисович;

кандидат физико-математических наук, ведущий научный сотрудник ИСП РАН Шокуров Александр Владимирович.

Ведущая организация: Вычислительный центр РАН.

Защита диссертации состоится 31 октября 2008 г. в 11:00 на заседании диссертационного совета Д 501.001.44 в Московском государственном университете имени М. В. Ломоносова по адресу: 119991, ГСП–1, Москва, Ленинские горы, МГУ, 2–ой учебный корпус, факультет ВМиК, аудитория 685.

С диссертацией можно ознакомиться в библиотеке факультета ВМиК МГУ. С текстом автореферата можно ознакомиться на официальном сайте ВМиК МГУ имени М. В. Ломоносова http://www.cmc.msu.ru в разделе «Наука» – «Работа диссертационных советов» – «Д 501.001.44».

Автореферат разослан «29» сентября 2008 г.

Ученый секретарь
диссертационного совета
профессор Трифонов Н. П.

Общая характеристика работы

Актуальность темы. Значительное место в современной математике занимают задачи сложности вычислений, связанные с проблемами существования эффективных алгоритмов решения задач линейной алгебры, а также построение этих алгоритмов. Речь может идти, например, о минимальном числе элементарных арифметических операций, таких как сложение и умножение чисел, достаточном для вычисления произведения двух матриц, произведения двух полиномов одного или нескольких переменных, определителя квадратной матрицы, решения системы линейных алгебраических уравнений. В диссертации решаются некоторые задачи алгебраической теории сложности. Оценивается сложность умножения в групповых алгебрах, то есть в алгебрах, в которых существует базис, элементы которого образуют группу относительно умножения в алгебре. Устанавливается сложность умножения в коммутативных групповых алгебрах над произвольными алгебраически замкнутыми полями, а также над полем вещественных чисел. Устанавливается сложность умножения в некоммутативных групповых алгебрах симметрий треугольника, симметрий квадрата и чётных подстановок четвёртого порядка, а также тесная связь этих алгебр с алгеброй квадратных матриц. Особенность данной работы заключается в использовании алгебраических методов.

Пусть A — конечномерное линейное пространство над полем k. A называется *алгеброй*, если в A определено умножение векторов, обладающее свойством ассоциативности и дистрибутивности относительно сложения в A. Пусть $a = \{a_1, \ldots, a_n\}$ — базис в A, и умножение определяется формулами

$$a_i a_j = \sum_{\nu=1}^{n} \alpha_{ij}^{\nu} a_\nu, \quad 1 \leqslant i, j \leqslant n.$$

Нетрудно видеть, что для умножения двух векторов

$$\sum_{i=1}^{n} \beta_i a_i \quad \text{и} \quad \sum_{j=1}^{n} \beta'_j a_j,$$

где β_i и β'_j — числа из k, являющиеся координатами векторов-множителей в базисе a, по определённым выше формулам необходимо выполнить n^2 операций умножения переменных из k и $n^2 - n$ операций сложения. Для многих важных алгебр, таких как алгебра многочленов и алгебра

квадратных матриц размера $n \times n$, известны более эффективные по числу арифметических операций алгоритмы.

В 1962 году А. А. Карацуба и Ю. П. Офман предложили алгоритм умножения чисел длины n в двоичной системе счисления со сложностью $O(n^{\log_2 3})$. Этот алгоритм легко трансформируется в алгоритм умножения многочленов одного переменного степени n. Таким образом, впервые было установлено, что традиционный алгоритм не является оптимальным. Предложенный алгоритм использовал технику «разделяй-и-властвуй» и неявно основывался на вычислении и последующей интерполяции многочлена второй степени по трём точкам. Более полно этот подход был использован А. Л. Тоомом в 1963 году, предложившим для любого $\varepsilon > 0$ алгоритм умножения чисел длины n в двоичной системе счисления сложности

$$O(n^{1+o(1)}),$$

основанный на алгоритме умножения многочленов степени n той же сложности. В 1971 году данный результат был улучшен А. Шёнхаге и Ф. Штрассеном, предложившими алгоритмы сложности

$$O(n \log n \log \log n)$$

для умножения многочленов степени n и чисел длины n в двоичной записи. Этот алгоритм оставался асимптотически самым быстрым на протяжении 26 лет и был улучшен в 2007 году Мартином Фюрером, предложившим алгоритм сложности

$$n \log n 2^{O(\log^* n)}$$

для умножения чисел длины n.

Нетривиальные нижние оценки сложности умножения полиномов известны только в моделях с ограничениями. В общем случае из линейной независимости коэффициентов полинома-произведения следует только, что для умножения полиномов степени n требуется не менее

$$2n - 1$$

арифметических операций. Большинство асимптотически быстрых алгоритмов основаны на дискретном преобразовании Фурье. В 1973 году Ж. Моргенштерн заметил, что дискретное преобразование Фурье имеет суперлинейную сложность, а именно,

$$\Omega(n \log n),$$

если в алгоритме трансформации использовать только коэффициенты, ограниченные некоторой константой. В 2004 году Петер Бюргиссер и Мартин Лотц обобщили эту оценку на произвольные алгоритмы умножения полиномов. Существует гипотеза о том, что в действительности сложность умножения многочленов равна

$$O(n \log n),$$

однако до сих пор это утверждение не доказано и не опровергнуто.

В 1969 году Ф. Штрассен опубликовал алгоритм умножения квадратных матриц порядка n сложности

$$O(n^{\log_2 7}).$$

Этот результат послужил отправной точкой развития алгебраической теории сложности. В течение 9 лет результат Штрассена не удавалось улучшить, однако в 1978 году В. Пан посредством анализа трилинейных форм предложил первую нетривиальную конструкцию для вычисления произведения матриц сложности, меньшей во втором знаке после десятичной запятой в показателе, чем алгоритм Штрассена. После этого в течение 10 лет несколько групп учёных из разных университетов мира, предлагая новые подходы и конструкции, понижали верхнюю оценку сложности умножения матриц. На сегодняшний день уже более 20 лет лучшую известную верхнюю оценку дает алгоритм Копперсмита и Винограда (опубликованный несколько позже, чем стал известным), использующий практически все предложенные за время изучения задачи подходы, имеющий сложность

$$O(n^{2{,}376})$$

для умножения двух квадратных матриц порядка n.

Нелинейные нижние оценки сложности умножения матриц отсутствуют. В 2002 году Ран Раз доказал нижнюю оценку

$$\Omega(n^2 \log n)$$

для сложности умножения квадратных матриц порядка n в модели с ограниченными коэффициентами. Для общего случая известна нижняя оценка числа

$$2n^2 - 1$$

требуемых активных скалярных умножений алгоритма (являющаяся одновременно нижней оценкой числа всех арифметических операций). В

1999 году Маркус Блезер улучшил этот результат, доказав, что умножение матриц требует не менее

$$\frac{5}{2}n^2 - 3n$$

операций умножения чисел. Амир Шпилька в 2001 году улучшил этот результат для конечных полей:

$$3n^2 - o(n^2) \quad \text{для поля } GF(2)$$

и

$$\left(\frac{5}{2} + \frac{3}{2(p^3-1)}\right) n^2 - o(n^2) \quad \text{для поля } GF(p).$$

Для малых значений n лучшей на сегодняшний день является оценка

$$2n^2 + n - 2 \quad (n \geqslant 3),$$

принадлежащая Маркусу Блезеру. Существует гипотеза о том, что в действительности сложность умножения матриц порядка n равна

$$n^2 \cdot 2^{o(\log n)},$$

однако до сих пор это утверждение не доказано и не опровергнуто.

В 2003 году Генри Коэн и Кристофер Уманс предложили новый подход для получения верхних оценок сложности умножения матриц, основанный на вложениях в групповые алгебры. В частности, было показано, что установление сложности умножения в групповых алгебрах влечёт определение сложности умножения матриц. В 2005 году при помощи этого подхода были получены первые алгоритмы сложности ниже, чем $O(n^3)$. Несмотря на то, что все улучшения, полученные этим подходом, по сути представляют собой изложение классических результатов, переписанное на теоретико-групповом языке, эти работы стимулировали рост интереса к задаче сложности умножения в групповых алгебрах.

Цель диссертации. Целью данной диссертации является изучение вопроса сложности умножения в групповых алгебрах, разработка быстрых алгоритмов умножения и получение точных нижних оценок, а также приложения к задачам сложности умножения матриц и полиномов многих переменных. В процессе решения этой задачи возникли следующие вспомогательные подзадачи:

1. Получение всех максимальных идеалов в групповых алгебрах.

2. Сведение умножения в групповых алгебрах к умножению полиномов одного переменного.

Вторая цель диссертации состоит в описании спектра всевозможных сложностей умножения в коммутативных групповых алгебрах.

Научная новизна. Все результаты диссертации являются новыми.

1. Установлена сложность умножения в коммутативных групповых алгебрах над алгебраически замкнутыми полями и над полем вещественных чисел. Описан оптимальный алгоритм умножения в этих алгебрах. Описана структура коммутативных групповых алгебр над алгебраически замкнутыми и вещественным полями.

2. Изучены некоторые некоммутативные групповые алгебры, установлены верхние и нижние оценки их сложности и связь сложности умножения в некоммутативных групповых алгебрах со сложностью умножения матриц.

3. Предложен метод умножения полиномов многих переменных оптимальной сложности, основанный на сведении задачи к умножению в групповых алгебрах.

Научная и практическая ценность. Работа имеет теоретическую направленность. Установлена сложность умножения в ряде групповых алгебр, для некоторых алгебр получены нижние и верхние оценки сложности, установлена связь сложности умножения матриц со сложностью умножения в групповых алгебрах.

Полученные при этом методы могут применяться для дальнейшей характеризации сложности умножения в алгебрах над произвольными полями. Работа дает пример применения методов оценки сложности умножения в групповых алгебрах к сложности умножения полиномов многих переменных.

Методы исследования. В диссертации используются методы теории сложности, компьютерной алгебры, теории групп и теории полей.

Публикации и апробирование. Результаты диссертации докладывались на семинаре мехмата МГУ «Математические вопросы кибернетики» (руководитель — академик РАН О. Б. Лупанов), на VI Междунарожной конференции «Дискретные модели в теории управляющих

систем» (Москва, 2004 г.), на XIV Международной конференции «Проблемы теоретической кибернетики» (Пенза, 2005 г.), на VII Международрожной конференции «Дискретные модели в теории управляющих систем» (Москва, 2006 г.), на XIX Международной конференции «IEEE Computational Complexity Conference» (Прага, 2006 г.), на семинаре факультета информатики университета Саарланда (Саарбрюкен, Германия) «Computational Complexity» (руководитель — профессор М. Блезер), на семинаре факультета информатики университета Технион (Хайфа, Израиль) «Algebraic Complexity» (руководитель — профессор М. Каминский) и на семинаре факультета информатики университета Технион (Хайфа, Израиль) «Complexity Theory» (руководитель — профессор А. Шпилька).

По теме диссертации опубликовано 6 работ.

Структура и объем работы. Диссертация состоит из введения, пяти глав и списка литературы. Объем работы 102 страницы.

Краткое содержание диссертации

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

Глава 1 посвящена методам получения нижних оценок и описания структуры групповой алгебры, позволяющим применять ряд известных результатов алгебраической теории сложности к групповым алгебрам.

В разделе 1.1 даются основные определения и факты из теории групп.

Теорема 1. *Любая коммутативная группа G порядка $n \geqslant 2$ разлагается в прямое произведение циклических групп:*

$$G \cong \mathbb{Z}_{n_1} \otimes \cdots \otimes \mathbb{Z}_{n_m}, \tag{1}$$

где $n_\mu \geqslant 2$, $\mu = 1, \ldots, m$, $n_1 \cdots n_m = n$. Числа $n_1, \ldots, n_m$ можно выбрать так, что $n_\mu = p_\mu^{d_\mu}$, где p_μ — простые числа, а $d_\mu > 0$ (такие группы $\mathbb{Z}_{n_\mu}$ называются примарными*), в этом случае представление* (1) *единственно с точностью до перестановки множителей.*

В разделе 1.2 вводятся модель вычисления и постановка задачи. Пусть U, V, W — конечномерные линейные пространства над полем k, и $\varphi : U \times V \to W$ — билинейное отображение. *Билинейным вычислением (билинейным алгоритмом)* для φ называется такая последовательность

$(f_1, g_1, w_1, \ldots, f_r, g_r, w_r)$, где $f_\rho \in U^*$, $g_\rho \in V^*$, $w_\rho \in W$, $1 \leqslant \rho \leqslant r$, что для любых $u \in U$, $v \in V$

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

r называется *длиной* билинейного вычисления. *Рангом* или *билинейной сложностью* φ называется длина кратчайшего билинейного вычисления для φ. Ранг φ обозначается $\operatorname{rk} \varphi$.

Ранг умножения в алгебре A (являющегося билинейнейным отображением $A \times A \to A$) называется *рангом алгебры* A и обозначается $\operatorname{rk} A$.

Обобщением билинейного вычисления и ранга является квадратичное вычисление и мультипликативная сложность. *Квадратичным вычислением (квадратичным алгоритмом)* для φ является такая последовательность $(f_1, g_1, w_1, \ldots, f_\ell, g_\ell, w_\ell)$, где $f_\lambda, g_\lambda \in (U \times V)^*$, $w_\lambda \in W$, $1 \leqslant \lambda \leqslant \ell$, что для любых $u \in U$, $v \in V$

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

ℓ называется *длиной* квадратичного вычисления. *Мультипликативной сложностью* φ называется длина кратчайшего квадратичного вычисления для φ. Мультипликативная сложность φ обозначается $C(\varphi)$.

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

Основными характеристиками сложности алгебр в данной работе являются мультипликативная и билинейная сложности умножения.

В разделе 1.3 приводятся результаты о нижних оценках и способах их получения.

Теорема 2 (А. Алдер, Ф. Штрассен)**.** *Для произвольной ассоциативной алгебры A выполняется*

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

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

Отсюда, в частности, следует, что $\operatorname{rk} A \geqslant 2 \dim A - t(A)$. Алгебры, для которых оценка Алдера-Штрассена совпадает с верхней, называются *алгебрами минимального ранга.*

Левый (правый, двусторонний) идеал I в A называется *нильпотентным*, если для некоторого целого числа n выполняется $I^n = \{0\}$. Сумма всех нильпотентных левых идеалов алгебры A является нильпотентным двусторонним идеалом в A, называется *радикалом* A и обозначается $\operatorname{rad} A$. Известно, что $\operatorname{rad} A$ содержится в любом максимальном двустороннем идеале A. Так, например, если пересечение всех максимальных двусторонних идеалов A равно $\{0\}$, то $\operatorname{rad} A = \{0\}$. Обратно, если пересечение всех максимальных двусторонних идеалов A является левым нильпотентным идеалом, то оно совпадает с $\operatorname{rad} A$.

Элемент a алгебры A называется обратимым, если существует такой $a^{-1} \in A$, что $aa^{-1} = a^{-1}a = e$, где e — единица алгебры. Обозначим множество обратимых элементов алгебры A через $A^\times$. Алгебра D называется *алгеброй с делением*, если $D^\times = D \setminus \{0\}$. Алгебра A называется *локальной*, если фактор-алгебра $A/\operatorname{rad} A$ является алгеброй с делением, и A называется *основной*, если $A/\operatorname{rad} A$ является прямым произведением алгебр с делением. Будем называть алгебру A над полем k *сверхосновной*, если $A/\operatorname{rad} A \cong k^t$ для некоторого t. Очевидно, что любая сверхосновная алгебра является основной.

Пусть $k^{n\times n}$ — алгебра матриц порядка $n \times n$ над полем k.

Теорема 3 (М. Блезер)**.** *Алгебра A над полем k является алгеброй минимального ранга тогда и только тогда, когда*

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

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

$$\operatorname{rad} B = \mathsf{L}_B + Bw_1B + \cdots + Bw_mB = \mathsf{R}_B + Bw_1B + \cdots + Bw_mB$$

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

Также в разделе 1.3 доказывается теорема 4, являющаяся основным инструментом получения нижних и верхних оценок в групповых алгебрах.

Теорема 4. *Ортогональное дополнение левого (правого) идеала групповой алгебры A относительно покоординатного скалярного произведения в произвольном групповом базисе является левым (соответственно правым) идеалом.*

Глава 2 посвящена коммутативным групповым алгебрам над полями, поддерживающими быстрое преобразование Фурье.

В разделе 2.1 приводится постановка задачи и её решение в простейшем случае. Доказывается, что в случае циклической группы, порядок которой не делится на характеристику поля, соответствующая алгебра изоморфна степени поля, и сложность умножения в ней совпадает с размерностью.

В разделе 2.2 доказываются теоремы об определителе циклической матрицы над алгебраически замкнутым полем произвольной характеристики и матриц, получаемых кронекеровскими произведениями циклических матриц.

Теорема 5. *Пусть D — блочная циклическая матрица (блочного) порядка p над произвольным полем $\mathbb{F}$ простой характеристики p, все блоки которой являются квадратными матрицами,*

$$D = \begin{pmatrix} A_0 & A_1 & \dots & A_{p-1} \\ A_1 & A_2 & \dots & A_0 \\ \dots & \dots & \dots & \dots \\ A_{p-1} & A_0 & \dots & A_{p-2} \end{pmatrix}.$$

Тогда D эквивалентна[1] *матрице F,*

$$F = \begin{pmatrix} \dots & \dots & \dots & S \\ \dots & \dots & S & 0 \\ \dots & \dots & 0 & \dots \\ S & 0 & \dots & 0 \end{pmatrix}, \qquad S = A_0 + \dots + A_{p-1}.$$

[1] В данном случае эквивалентность означает существование невырожденных матриц P и Q, таких что $\det P \cdot \det Q = 1$ и $F = PDQ$. Первое свойство в данном случае необходимо для того, чтобы определители D и F совпадали.

Теорема 6. *Пусть поле* $\mathbb{F}$ *имеет характеристику* p*. Определитель циклической матрицы* C*, где*

$$C = \begin{pmatrix} a_0 & a_1 & \dots & a_{n-1} \\ a_1 & a_2 & \dots & a_0 \\ \dots & \dots & \dots & \dots \\ a_{n-1} & a_0 & \dots & a_{n-2} \end{pmatrix},$$

равен в случае, если $p \nmid n$*,*

$$\det C = (-1)^{\frac{(n-1)(n-2)}{2}} \prod_{\varepsilon,\, \varepsilon^n=1} \sum_{i=0}^{n-1} \varepsilon^i a_i.$$

Теорема 7. *Пусть* C *— циклическая матрица размера* $n \times n$*,* $n = p^k t$*, где* $p \nmid t$ *и* $k > 0$*, над алгебраически замкнутым полем характеристики* p*.*

$$C = \begin{pmatrix} c_0 & c_1 & \dots & c_{n-1} \\ c_1 & c_2 & \dots & c_0 \\ \dots & \dots & \dots & \dots \\ c_{n-1} & c_0 & \dots & c_{n-2} \end{pmatrix}.$$

Тогда

$$\det C = (-1)^{\frac{p(p^k-1)}{2} + \frac{p^k(t-1)(t-2)}{2}} \left(\prod_{\varepsilon:\, \varepsilon^t=1} \sum_{i=0}^{n-1} \varepsilon^i c_i \right)^{p^k}.$$

Теорема 8. *Пусть для каждого* σ*,* $\sigma = s, \dots, 2$*, блочная циклическая матрица* D_σ *над полем характеристики* p *построена из* q_σ *различных матриц* $D^j_{\sigma-1}$*,* $j = 0, \dots, q_\sigma - 1$*,* $q_\sigma = p^{r_\sigma}$ *для некоторого натурального* r_σ*, следующим образом:*

$$D_\sigma = \begin{pmatrix} D^0_{\sigma-1} & \dots & D^{q_\sigma-1}_{\sigma-1} \\ \dots & \dots & \dots \\ D^{q_\sigma-1}_{\sigma-1} & \dots & D^{q_\sigma-2}_{\sigma-1} \end{pmatrix}.$$

При этом матрицы D^j_1 *имеют размер* 1×1 *(*$q_1 = 1$*,* $r_1 = 0$*). Тогда*

$$\det D_s = (-1)^{\frac{p(n-1)}{2}} \Big(\sum d^{(s)}_i \Big),$$

где $n = \prod_{i=1}^s q_i$ *— порядок матрицы* D_s*, а* $d^{(s)}_i$ *суть различные скалярные элементы* i*-го столбца матрицы* D_s*.*

В разделе 2.3 устанавливается сложность умножения в групповых алгебрах циклических групп над полями, поддерживающими быстрое преобразование Фурье.

Теорема 9. *Пусть алгебраически замкнутое поле $\mathbb{F}$ имеет характеристику p, $n = p^k t$, $p \nmid t$. Тогда алгебра $\mathbb{F}[\mathbb{Z}_n]$ является алгеброй минимального ранга и*

$$\operatorname{rk} \mathbb{F}[\mathbb{Z}_n] = 2n - t.$$

Попутно устанавливается структура таких алгебр.

Теорема 10. *Пусть алгебраически замкнутое поле $\mathbb{F}$ имеет характеристику p, $n = p^k t$, $p \nmid t$. Тогда алгебра $\mathbb{F}[\mathbb{Z}_n]$ является алгеброй минимального ранга и*

$$\mathbb{F}[\mathbb{Z}_n] \cong B^t.$$

В разделе 2.4 получаются точные оценки сложности умножения в произвольных коммутативных групповых алгебрах над полями, поддерживающими быстрое преобразование Фурье.

Теорема 11. *Пусть A — коммутативная групповая алгебра над полем $\mathbb{F}$ характеристики p, поддерживающим быстрое преобразование Фурье. Тогда*

$$A \cong B^t,$$

где B — алгебра Блезера с $B/\operatorname{rad} B \cong \mathbb{F}$, $\dim A = p^k t$, $p \nmid t$. В этом случае

$$\operatorname{rk} A = 2 \dim A - t.$$

Пусть A — коммутативная групповая алгебра над полем $\mathbb{F}$ характеристики 0, поддерживающим быстрое преобразование Фурье. Тогда

$$A \cong \mathbb{F}^{\dim A}.$$

В этом случае

$$\operatorname{rk} A = \dim A.$$

Глава 3 посвящена коммутативным групповым алгебрам над полем вещественных чисел.

В разделе 3.1 доказаны теоремы, описывающие структуру, и определяющие сложность циклических групповых алгебр над полем вещественных чисел.

Обозначим $e(n) = n - 2\left\lfloor \frac{n}{2} \right\rfloor$.

Теорема 12. *Для любого n*

$$\mathbb{R}[\mathbb{Z}_n] \cong \mathbb{R}^{e(n)} \times \left(\mathbb{R}[x]/(x^2+1)\right)^{\left\lfloor \frac{n-1}{2} \right\rfloor}.$$

Теорема 13. $\operatorname{rk} \mathbb{R}[\mathbb{Z}_n] = 3\left\lfloor \frac{n-1}{2} \right\rfloor + e(n)$.

В разделе 3.2 изучаются произвольные коммутативные групповые алгебры над полем вещественных чисел, определяется структура и устанавливается сложность таких алгебр, вводится понятие константы асимптотики сложности, и доказывается теорема, полностью описывающая спектр таких констант для произвольных последовательностей коммутативных групповых алгебр над полем вещественных чисел.

Теорема 14.

$$\operatorname{rk} \mathbb{R}[\mathbb{Z}_m \times \mathbb{Z}_n] \geqslant \frac{3}{2}mn - \frac{1}{2}e(m)e(n).$$

Теорема 15.

$$\mathbb{R}[\mathbb{Z}_m \times \mathbb{Z}_n] \cong \mathbb{R}^{e(m)e(n)} \times \left(\mathbb{R}[x]/(x^2+1)\right)^{\frac{mn-e(m)e(n)}{2}}.$$

Пусть абелева группа G разлагается в прямое произведение циклических групп следующим образом:

$$G = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_t}.$$

Обозначим $e(G) = e(n_1) \cdots e(n_t)$.

Теорема 16. *Пусть G — абелева группа. Тогда*

$$\operatorname{rk} \mathbb{R}[G] \geqslant \frac{3}{2}\left|G\right| - \frac{1}{2}2^{e(G)}.$$

Теорема 17. *Пусть G — абелева группа, $n = \left|G\right|$, $e(G) = \ell$. Тогда*

$$\operatorname{rk} \mathbb{R}[G] = \frac{3}{2}n - \frac{1}{2}2^{\ell}.$$

Пусть $\{A_i\}_{i=1}^{\infty}$ — последовательность алгебр над одним и тем же полем k, причём $\dim A_i = n_i$ и $n_i \xrightarrow[i\to\infty]{} \infty$. Назовём *константой асимптотики сложности* величину

$$C(A) = \lim_{i\to\infty} \frac{\operatorname{rk} A_i}{n_i},$$

если данный предел существует.

Теорема 18. *1. Пусть* $\{A_i\}_{i=1}^{\infty}$ *— последовательность групповых алгебр абелевых групп над* $\mathbb{C}$*. Тогда* $C(A) = 1$*.*

2. Пусть

$$C_0 = \frac{3}{2}, \qquad C_m = \frac{3}{2} - \frac{1}{2m}, \quad m = 1, 2, \ldots .$$

Для каждого m*,* $m = 0, 1, 2, \ldots$*, существует такая последовательность групповых алгебр* $\left\{A_i^m\right\}_{i=1}^{\infty}$ *абелевых групп над* $\mathbb{R}$*, что для любого* m *константа асимптотики сложности равна* $C(A^m) = C_m$*.*

3. Пусть $\{A_i\}_{i=1}^{\infty}$ *— произвольная последовательность групповых алгебр абелевых групп над* $\mathbb{R}$*, для которой существует* $C(A)$*. Тогда существует* $m \geqslant 0 :\ C(A) = C_m$

Глава 4 посвящена задаче умножения полиномов одного и нескольких переменных.

В разделе 4.1 вводятся основные понятия и постановка задачи.

В разделе 4.2 приводятся лучшие известные оценки сложности умножения полиномов в различных моделях вычисления над различными полями.

В разделе 4.3 демонстрируется способ получения быстрых алгоритмов умножения полиномов многих переменных посредством сведения к умножению в коммутативных групповых алгебрах.

Теорема 19. *Пусть* p_1 *и* p_2 *— полиномы* m *переменных* $X_1, \ldots, X_m$ *степеней* d_μ *по переменным* X_μ*,* $d_\mu > 0$*,* $1 \leqslant \mu \leqslant m$ *над полем* k*, содержащим все корни степени* $M = \prod_{\mu=1}^{m}(2d_\mu+1)$ *из* 1*. Пусть также* p *— характеристика поля* k*, и* $M = p^d t$*, где* $p \nmid t$*. Тогда существует билинейный алгоритм умножения полиномов* p_1 *и* p_2 *длины* $2M - t$*.*

Глава 5 посвящена некоторым некоммутативным алгебрам.

В разделе 5.1 получены структура и сложность групповой алгебры подстановок третьего порядка. Доказаны теоремы о структуре, сложности алгебры подстановок третьего порядка, а также единственности вложения алгебры матриц второго порядка в алгебру подстановок третьего порядка.

Теорема 20. *Имеет место изоморфизм:*

$$\mathbb{C}[S_3] \cong \mathbb{C}^{2\times 2} \times \mathbb{C}^2. \tag{2}$$

Теорема 21. $\mathbb{C}[S_3]$ *является алгеброй минимального ранга.*

Теорема 22. *Для сложности умножения в* $\mathbb{C}[S_3]$ *выполняется*

$$\operatorname{rk}\mathbb{C}[S_3] = 9.$$

Теорема 23. *Алгебра* $\mathbb{C}[S_3]$ *содержит единственную подалгебру, изоморфную алгебре матриц* $\mathbb{C}^{2\times 2}$.

В разделе 5.2 доказаны теоремы о структуре и сложности групповой алгебры симметрий квадрата.

Теорема 24. $\mathbb{C}[Q] \cong \mathbb{C}^{2\times 2} \times \mathbb{C}^4$.

Теорема 25. $\operatorname{rk}\mathbb{C}[Q] = 11$.

Гипотеза о прямой сумме в теории сложности алгебр гласит, что для любых алгебр A и B над полем k справедливо $\operatorname{rk} A \times B = \operatorname{rk} A + \operatorname{rk} B$. На сегодняшний день эта гипотеза не доказана и не опровергнута.

В разделе 5.3 доказаны теоремы о структуре и сложности групповых алгебр чётных подстановок над полями комплексных и вещественных чисел, а также теорема о гипотезе о прямой сумме и сложности умножения матриц третьего порядка.

Теорема 26. *Пусть характеристика* k *отлична от* 2. *Тогда в* $k[A_4]$ *существует подалгебра, изоморфная* $k^{3\times 3}$.

Теорема 27. *Имеет место изоморфизм*

$$\mathbb{C}[A_4] \cong \mathbb{C}^3 \times \mathbb{C}^{3\times 3},$$

а также сложностное равенство

$$\operatorname{rk}\mathbb{C}[A_4] = \operatorname{rk}\mathbb{C}^{3\times 3} + 3.$$

Теорема 28. *Имеет место изоморфизм*

$$\mathbb{R}[A_4] \cong \mathbb{R} \times \mathbb{R}[X]/(X^2+1) \times \mathbb{R}^{3\times 3},$$

а также следующая нижняя оценка сложности умножения матриц третьего порядка

$$\operatorname{rk}\mathbb{R}^{3\times 3} \geqslant \operatorname{rk}\mathbb{R}[A_4] - 4.$$

Теорема 29. *Справедливо, по крайней мере, одно из следующих утверждений:*

1. $\operatorname{rk}\mathbb{C}^{3\times 3} < \operatorname{rk}\mathbb{R}^{3\times 3}$,

2. $\operatorname{rk}\mathbb{C}[A_4] < \operatorname{rk}\mathbb{R}[A_4]$,

3. гипотеза о прямой сумме является неверной.

Основные результаты диссертации

1. Разработан метод получения нижних оценок мультипликативной сложности групповых алгебр.

2. Установлена структура и получены точные значения мультипликативной сложности коммутативных групповых алгебр над полями, содержащими достаточное количество корней нужной степени из единицы.

3. Описана структура и мультипликативная сложность коммутативных групповых алгебр над полем вещественных чисел. Полностью описан спектр констант асимптотики сложности всех таких алгебр.

4. Разработан метод быстрого умножения полиномов многих переменных над полями, поддерживающими быстрое преобразование Фурье, основанный на умножении в групповых алгебрах.

5. Изучены некоммутативные групповые алгебры групп подстановок третьего порядка, симметрий квадрата и чётных подстановок четвёртого порядка, установлена связь сложности умножения в этих алгебрах со сложностью умножения квадратных матриц второго и третьего порядков.

Публикации по теме диссертации

1. Алексеев В. Б., Поспелов А. Д. *Сложность умножения в групповой алгебре симметрий квадрата.* Тезисы 6-ой Международной конференции «Дискретные модели в теории управляющих систем». Москва, издательский отдел ф-та ВМиК МГУ им. М. В. Ломоносова (2004), 8–11.

2. Алексеев В. Б., Поспелов А. Д. *О ранге групповых алгебр.* «Математические методы решения инженерных задач». Москва, Министерство обороны Российской Федерации (2005), 5–25 .

3. Алексеев В. Б., Поспелов А. Д. *Сложность умножения в некоторых групповых алгебрах.* Дискретная математика (2005) **17**, №1, 3–17.

4. Поспелов А. Д. *Ранг коммутативных групповых алгебр над полями комплексных и вещественных чисел.* Тезисы докладов XIV Международной конференции «Проблемы теоретической кибернетики» (Пенза, 23–28 мая 2005 г.). Издательство центра прикладных исследований при механико-математическом факультете МГУ (2005), с. 125.

5. Поспелов А. Д. *Билинейная сложность умножения в коммутативных групповых алгебрах.* Сборник тезисов лучших дипломных работ 2005 года. Москва, издательский отдел ф-та ВМиК МГУ им. М. В. Ломоносова (2005), с. 75–76.

6. Поспелов А. Д. *О сложности умножения полиномов и матриц.* Сборник статей молодых учёных факультета ВМиК МГУ, 2008, выпуск №5. Москва, издательский отдел ф-та ВМиК МГУ им. М. В. Ломоносова (2008), с. 83–97.