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

На правах рукописи

Лысиков Владимир Владимирович

Некоторые вопросы теории сложности билинейных отображений

01.01.09 – дискретная математика и математическая кибернетика

АВТОРЕФЕРАТ
диссертации на соискание ученой степени
кандидата физико-математических наук

Москва – 2013

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, руководитель отдела теоретической кибернетики ИСП РАН Кузюрин Николай Николаевич
	кандидат физико-математических наук, старший разработчик ООО «Яндекс» Поспелов Алексей Дмитриевич
Ведущая организация:	Национальный исследовательский университет «МЭИ»

Защита состоится «____» _____ 20__ г. в ____ часов на заседании диссертационного совета Д 501.001.44 при Московском государственном университете имени М. В. Ломоносова, расположенном по адресу: 119991, Москва, ГСП-1, Ленинские горы, МГУ, 2-й учебный корпус, факультет вычислительной математики и кибернетики, ауд. 685. Желающие присутствовать на заседании диссертационного совета должны сообщить об этом за 2 дня по тел. 939-30-10 (для оформления заявки на пропуск).

С диссертацией можно ознакомиться в Фундаментальной библиотеке МГУ.
С текстом автореферата можно ознакомиться на официальном сайте факультета ВМК МГУ `http://cs.msu.ru/` в разделе «Наука» – «Работа диссертационных советов» – «Д 501.001.44».

Автореферат разослан «____» _____ 20__ г.

Ученый секретарь
диссертационного совета Костенко В. А.

Общая характеристика работы

Актуальность темы. Одним из направлений в теории сложности вычислений является алгебраическая теория сложности. Естественно, что алгоритмы, вычисляющие функции, связанные с какой-либо алгебраической структурой 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 важных проблем алгебраической теории сложности является задача определения сложности умножения матриц[1,2]. В 1969 г. был опубликован алгоритм Ф. Штрассена[3] 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. После нескольких лет исследований в этой области Д. Копперсмитом и Ш. Виноградом[4] был получен алгоритм с асимптотической сложностью $O(n^{2.376})$. Недавние исследования с использованием компьютерных средств[5,6,7] позволили улучшить эту оценку до $O(n^{2.373})$.

Штрассен также заметил связь алгоритмов умножения матриц с алгебра-

---

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

[2] Bürgisser P., Clausen M., Shokrollahi M.A. Algebraic Complexity Theory. — Springer, 1997.

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

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

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

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

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

ическим понятием тензорного ранга, что позволило применять для изучения сложности этих алгоритмов конструкции мультилинейной алгебры. Эти конструкции и связанная с ними 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. Модель вычислений, связанная с этим подходом к сложности умножения матриц и вычисления билинейных отображений, называется моделью билинейных алгоритмов.

Определение. 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 $(f_1, g_1, z_1; f_2, g_2, z_2; \ldots; f_r, g_r, z_r)$, где $f_s \in U^*$, $g_s \in V^*$, $z_s \in W$, такая, что для любых $x \in U$, $y \in V$ выполняется

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

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 $R(\varphi)$.

Важным классом билинейных отображений является класс ассоциативных алгебр, то есть билинейных отображений вида $A \times A \to A$, обладающих свойством ассоциативности. Этот класс отображений удобен тем, что, с одной стороны, включает в себя умножение квадратных матриц, таким образом результаты о сложности умножения в ассоциативных алгебрах могут использоваться при анализе матричного умножения и наоборот, а с другой стороны, позволяет использовать классические результаты о структуре алгебр. Например, базовая конструкция в алгоритме Копперсмита-Винограда[4] умножения матриц 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[8] была получена нижняя оценка

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

сложности умножения в алгебрах в терминах их структуры.

Теорема (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.

Эта оценка оказалась неулучшаемой, в связи с чем возник вопрос об описании всех алгебр, на которых она достигается — алгебр минимального ранга. Эта задача решалась несколько десятков лет многими исследователями, окончательное описание было получено М. Блезером[9]. Одним из ключевых элементов этого описания являются улучшенные нижние оценки сложности умножения в алгебрах матриц[10,11].

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

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

Теорема (М. Блезер)**.** *Для ранга алгебры матриц размера 3×3 над произвольным полем F справедлива оценка*

$$R(F^{3 \times 3}) \geqslant 19.$$

После этого М. Блезером и А. М. де Вольтером[12] было начато изучение алгебр почти минимального ранга, т. е. алгебр, для которых билинейная сложность на 1 больше оценки Алдера-Штрассена. Ими было получено, в частности, описание полупростых алгебр почти минимального ранга над полем действительных чисел.

---

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

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

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

[12] 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.

Теорема (М. Блезер, А. М. де Вольтер)**.** *Любая полупростая алгебра почти минимального ранга над* $\mathbb{R}$ *имеет вид*

$$A \cong \mathbb{H} \times \mathbb{R}^{2\times 2} \times \cdots \times \mathbb{R}^{2\times 2} \times \mathbb{C} \times \cdots \times \mathbb{C} \times \mathbb{R} \times \cdots \times \mathbb{R}.$$

В данной диссертации обобщается результат Блезера и де Вольтера о полупростых алгебрах почти минимального ранга на случай произвольного основного поля, характеристика которого отлична от 2.

Блезером и де Вольтером были отмечены несколько ключевых проблем на пути к этому обобщению. Одним из ключевых вопросов на пути к описанию алгебр почти минимального ранга является вопрос о билинейной сложности умножения обобщенных кватернионов. Оптимальный алгоритм умножения кватернионов над полем действительных чисел был получен в 70х годах[13,14,15], однако он не обобщается непосредственным образом на алгебры обобщенных кватернионов над произвольным полем. В диссертации получен критерий почти минимальности для класса локальных алгебр, позволяющий получить оптимальный алгоритм в общем случае.

Для рассмотрения другого проблемного случая необходимо улучшить упомянутую выше нижнюю оценку М. Блезера для сложности умножения в простых алгебрах. Несмотря на то, что методы, использованные М. Лэндсбергом[16] позволяют получить оценку, более сильную асимптотически (порядка $3n^2$), они неприменимы для алгебр малой размерности. В данной работе оценка Блезера улучшается на единицу для матричных алгебр над расширениями основного поля.

Другим вопросом, рассматриваемым в диссертации, является исследование связи между алгоритмами вычисления билинейного отображения с целыми коэффициентами (например, умножения матриц или полиномов) над

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

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

[15] 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.

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

полями различных характеристик. Т. Д. Хауэлл[17] 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[18] 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[19] показал, что этот множитель не превосходит 4 при выполнении гипотезы Штрассена о прямой сумме.

В данной работе рассматривается связь рангов билинейного отображения с целочисленными коэффициентами над полями различных характеристик. Насколько известно автору, этот вопрос ранее не рассматривался.

Цель работы: описание структуры различных классов алгебр почти минимального ранга; исследование билинейной сложности $\mathbb{Z}$-билинейных отображений над различными полями.

Методы исследования. В диссертации используются методы алгебраической теории сложности, линейной алгебры, теории колец и теории моделей.

Научная новизна. Результаты диссертации являются новыми.

Основные результаты:

1. Описана структура оптимальных алгоритмов для класса билинейных отображений, ранг которых равен сумме размерностей аргументов.

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

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

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

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.

Теоретическая и практическая значимость. Диссертация носит теоретический характер. Полученные результаты могут быть применены для анализа других задач теории сложности билинейных отображений. Приведенный в диссертации алгоритм умножения обобщенных кватернионов может быть использован для построения более сложных алгоритмов.

Публикации. По теме диссертации опубликовано 5 работ, среди них 2 работы [2, 4] в рецензируемых изданиях, включенных в перечень ВАК.

Апробация результатов. Результаты диссертации докладывались на следующих семинарах и конференциях:

— на семинаре «Дискретные функции и сложность алгоритмов» под руководством В. Б. Алексеева, С. С. Марченкова и А. А. Вороненко (кафедра математической кибернетики ВМК МГУ) в 2011-13 гг.;

— на XI международном семинаре «Дискретная математика и ее приложения» (Москва, 18-23 июня 2012);

— на международной конференции «Мальцевские чтения» (Новосибирск, 12-16 ноября 2012);

— на семинаре «Дискретная математика и математическая кибернетика» под руководством В. Б. Алексеева, А. А. Сапоженко и С. А. Ложкина (кафедра математической кибернетики ВМК МГУ) в 2012-13 гг.;

— на международном молодежном научном форуме «Ломоносов-2013»;

Структура и объем диссертации. Работа состоит из введения, четырех глав и списка литературы, содержащего 41 наименование. Диссертация содержит 73 страницы и включает 1 таблицу.

Краткое содержание работы

Во введении приводится обзор исследований, связанных с темой диссертации, и кратко излагается содержание работы.

В главе 1 приводятся основные определения и известные факты, касающиеся билинейных отображений, алгебр и билинейной сложности. В разделе 1.1 приводятся определения билинейного отображения и алгебры. В разделе 1.2 рассматриваются основные понятия теории конечномерных ассоциативных алгебр. В разделе 1.3 вводится рассматриваемая модель вычислений — модель билинейных алгоритмов — и приводятся простейшие оценки сложности билинейных алгоритмов. В разделе 1.4 приводится определение и основные свойства тензорного произведения.

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

В разделе 2.1 вводится понятие алгебры обобщенных кватернионов и описывается их структура.

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

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. [2] *Пусть F — поле, U, V, W — векторные пространтсва над F, и $\varphi\colon U \times V \to W$ — билинейное отобораженне. 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.*

Теорема 2.4. [2] *Пусть F — поле, U, V, W — векторные пространтсва над F, и $\varphi\colon U \times V \to W$ — билинейное отобораженне. 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

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

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

Теорема 2.6. [2] *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*

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

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

В разделе 2.3 приводится билинейный алгоритм умножения обобщенных кватернионов, имеющий сложность 8, тем самым доказывается почти минимальность алгебр обобщенных кватернионов с делением.

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

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

Теорема 2.8. [2] *Пусть F — поле. Если H_1 и H_2 — алгебры обобщенных кватернионов с делением над F, а $A = H_1 \times H_2$, то $R(A) = 16$.*

Глава 3 посвящена классификации полупростых алгебр почти 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. Эти оценки позволяют доказать то, что алгебры с делением размерности больше 4 и алгебры матриц над алгебрами с делением, за исключением двух случаев, не являются алгебрами почти минимального ранга.

В разделе 3.2 доказывается новая нижняя оценка билинейной сложности матричных алгебр над расширением основного поля, позволяющая разобрать оставшиеся два случая. Вместе с результатами второй главы этот результат позволяет завершить классификацию полупростых алгебр почти минимального ранга над полем характеристики, отличной от 2.

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

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

Теорема 3.6. [2] *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.*

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 является тривиальным.

В разделах 4.2 и 4.3 приводятся два разных доказательства основного результата главы. 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.

Теорема 4.1. [4] *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.

В разделе 4.2 приведено доказательство этой теоремы, основанное на установлении непосредственной связи между билинейными алгоритмами над различными полями и кольцами. Раздел 4.3 содержит другое доказательство, основанное на методах теории моделей.

Публикации по теме диссертации

1. 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.

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

3. 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.

4. 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.

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