О некоторых результатах теории алгебраической сложности

Алексеев В.Б.

В данной работе приведен обзор некоторых результатов о вычислительной сложности алгебр, в частности, результатов, полученных на кафедре математической кибернетики МГУ им. М.В. Ломоносова автором и его учениками: Поспеловым А.Д., Чокаевым Б.В., Лысиковым В.В.

Ключевые слова: алгебраическая сложность, алгебра, ранг алгебры, билинейная сложность, мультипликативная сложность, сложность умножения матриц.

Понятие алгебраической сложности связано с алгебраическими моделями вычислений. Входными элементами в таких моделях являются переменные и константы — элементы какой-нибудь алгебраической структуры, обычно, элементы кольца или поля. В качестве элементарных операций в этом случае рассматриваются 4 алгебраические операции (сложение, вычитание, умножение, деление). Каждая операция может применяться к входным элементам или к уже построенным выражениям. Задача состоит в построении семейства заданных алгебраических выражений. Сложностью вычисления (алгоритма) называют число примененных операций (аналог сложности схем из функциональных элементов). Сложностью задачи называют минимум сложности алгоритмов, вычисляющих заданное семейство выражений. Хорошим введением в алгебраическую теорию сложности может служить книга [1]. Одна из центральных задач в алгебраической теории сложности — сложность умножения (вычисления произведений) в алгебрах. Среди важнейших задач — сложность умножения матриц и полиномов.

Пусть $\|a_{ij}\|_{m\times n}$ обозначает матрицу размера $m \times n$ над некоторым кольцом. Задача умножения матрицы $\|a_{ij}\|_{m\times n}$ на матрицу $\|b_{kl}\|_{n\times p}$ — это задача вычисления системы из mp билинейных форм вида $\sum_{j=1}^{n} a_{ij}b_{jl}$. При этом элементы a_{ij} и b_{kl} рассматриваются как отдельные независимые входные переменные, а на каждом шаге вычисления

разрешается применить любую из 4 арифметических операций к уже построенным выражениям и элементам кольца. Число арифметических операций в алгоритме называют арифметической сложностью (обычно просто сложностью) алгоритма, а наименьшую сложность алгоритмов, вычисляющих систему билинейных форм $\sum_{j=1}^{n} a_{ij}b_{jl}$, называют сложностью задачи умножения матрицы размера $m \times n$ на матрицу размера $n \times p$. Стандартный алгоритм («строка на столбец») для умножения матриц размера $n \times n$ использует порядка n^3 арифметических операций. Первый асимптотически более быстрый алгоритм умножения матриц размера $n \times n$ (с числом арифметических операций $O\left(n^{\log_2 7}\right)$) построил Ф. Штрассен [2] в 1969 году. В последующие 20 лет верхняя оценка сложности умножения двух матриц размера $n \times n$ была понижена до $O\left(n^{2.38}\right)$ [3], но с тех пор существенных продвижений в этой задаче нет.

Чтобы лучше понять проблемы, возникающие при поиске быстрых алгебраических вычислений, математики начали рассматривать более общую задачу — вычисления в произвольных алгебрах. Напомним, что алгебра — это линейное пространство, на котором задана операция умножения, обладающая свойством линейности по каждому из сомножителей. С учетом линейности, для задания алгебры достаточно в рассматриваемом линейном пространстве рассмотреть какой-нибудь базис $e_1, \ldots, e_n$ и задать произведения базисных элементов: $e_i \cdot e_j = \sum_{k=1}^{n} t_{ijk}e_k$. Тогда произведение произвольных элементов $\sum_{i=1}^{n} a_i e_i$ и $\sum_{j=1}^{n} b_j e_j$ будет вычисляться по формуле:

$$\left(\sum_{i=1}^{n} a_i e_i\right) \cdot \left(\sum_{j=1}^{n} b_j e_j\right) = \sum_{k=1}^{n} \left(\sum_{i=1}^{n}\sum_{j=1}^{n} t_{ijk} a_i b_j\right) e_k.$$

Таким образом, если сомножители задаются коэффициентами при разложении по некоторому базису, то коэффициенты произведения являются билинейными формами от коэффициентов сомножителей. И мы приходим к важному классу задач в теории алгебраической сложности — сложности вычисления систем билинейных форм. В рекурсивных алгоритмах для умножения матриц (таким является алгоритм Штрассена) элементы a_{ij} и b_{kl} сами могут являться матрицами, которые не коммутируют между собой. При этом основную роль для оценки сложности рекурсивных алгоритмов играет число умножений. В связи с этим важное значение придается изучению билинейной сложности умножения матриц, а вместе с этим и изучению билинейной сложности умножения в произвольных алгебрах.

Пусть U, V, W — конечномерные линейные пространства над некоторым полем F.

Определение 1. Отображение $\varphi\colon U \times V \to W$ называется *билинейным*, если

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

Если $u_1, u_2, \ldots, u_n$ — базис U, $v_1, v_2, \ldots, v_m$ — базис V, $w_1, w_2, \ldots, w_l$ — базис W, то билинейное отображение задается набором коэффициентов t_{ijk}:

$$\varphi(\sum_{i=1}^{n} a_iu_i, \sum_{j=1}^{m} b_jv_j) = \sum_{k=1}^{l} c_kw_k \Leftrightarrow c_k = \sum_{i=1}^{n}\sum_{j=1}^{m} t_{ijk}a_ib_j.$$

Определение 2. *Билинейным алгоритмом сложности* r для вычисления билинейного отображения φ называется набор r троек f_s, g_s, z_s, где $f_s \in U^*$, $g_s \in V^*$, $z_s \in W$, такой, что

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

(Здесь U^*, V^* — пространства, двойственные к U и V, то есть f_s и g_s — это линейные формы на U и V.)

Минимально возможная сложность билинейного алгоритма называется *билинейной сложностью* или *рангом* φ (обозначение: $R(\varphi)$).

Определение 3. *Квадратичным алгоритмом сложности* r для вычисления φ называется набор r троек f_s, g_s, z_s, где $f_s \in (U \times V)^*$, $g_s \in (U \times V)^*$, $z_s \in W$, такой, что

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

(Здесь все линейные формы f_s и g_s могут зависеть как от x, так и от y.)

Минимально возможная сложность квадратичного алгоритма называется *мультипликативной сложностью* φ (обозначение: $C(\varphi)$).

Нетрудно получить следующие неравенства для любого билинейного отображения (семейства билинейных форм) φ:

$$rg(\varphi) \le R(\varphi) \le dimX \cdot dimY,$$

$$C(\varphi) \le R(\varphi) \le 2C(\varphi),$$

где $rg(\varphi)$ — размерность образа при отображении φ (число линейно независимых билинейных форм в заданной системе φ).

Существуют семейства билинейных форм P такие, что

$$C(P) < R(P).$$

Один из простейших нетривиальных примеров — задача умножения матрицы размера 2×2 на матрицу размера 2×3. Обозначим семейство из 6 билинейных форм в этой задаче как $< 2, 2, 3 >$. Тогда

$$C(< 2, 2, 3 >) = 10 \text{ (Waksman A., 1970, [4])},$$

$$R(< 2, 2, 3 >) = 11 \text{ (Алексеев В.Б., 1985 [5])}.$$

Для любых семейств билинейных форм P и Q выполняются следующие неравенства для ранга и мультипликативной сложности:

$$R(P \cup Q) \leq R(P) + R(Q),$$

$$C(P \cup Q) \leq C(P) + C(Q).$$

Известна следующая гипотеза.

Гипотеза о прямой сумме. *Если в семействах билинейных форм P и Q нет общих переменных, то*

$$R(P \cup Q) = R(P) + R(Q).$$

Фактически, Штрассен установил, что билинейная сложность умножения двух квадратных матриц порядка 2 не превосходит 7, откуда вытекал и его общий результат.

Установить точное значение билинейной сложности редко удается даже в задачах перемножения двух матриц достаточно малого размера. Например, для задачи перемножения двух матриц размера 3×3 к настоящему моменту известно только, что билинейная сложность заключена между 19 и 23 [6, 7]. Для задачи перемножения двух матриц размера 4×4 верхняя оценка 49 на число умножений (вместо обычных 64) получается двукратным использованием алгоритма Штрассена, и эта оценка пока не понижена. Для задачи перемножения двух матриц размера 5×5 наилучшим остается алгоритм из [8] с числом умножений 100 вместо обычных 125. Из недавних результатов интересен результат А.В. Смирнова [9], который построил билинейный алгоритм для умножения матрицы размера 3×3 на матрицу размера 3×6 с 40 умножениями (вместо обычных 54).

Обозначим через $R_F < m, n, p >$ билинейную сложность задачи умножения матрицы размера $m \times n$ на матрицу размера $n \times p$ над некоторым полем F. Теорема о двойственности [10] утверждает, что $R_F < m, n, p >$ не изменяется при любой перестановке чисел m, n, p.

Нетрудно показать, что $R_F < m, 1, p >= mp$. В работе [11] показано, что $R_F < 2, 2, 2 >= 7$ для любого поля F. (При этом в работе [12] доказано, что все билинейные алгоритмы билинейной сложности 7 для умножения матриц порядка 2 в определенном смысле эквивалентны друг другу). Применяя результат Штрассена, можно несложно получить, что $R_F < m, 2, 2 >\leq \lceil \frac{7m}{2} \rceil$ для произвольного поля F. В работе [13] получен более общий результат:

$$R_F(< 2, m, n >) \leq \lceil \frac{3mn + max(m, n)}{2} \rceil.$$

Там же получена и такая же нижняя оценка, но только для поля из 2 элементов. Автором в работе [5] был рассмотрен случай $m = 3$ и доказано, что $R_F < 3, 2, 2 >= 11$ для произвольного поля F. В статье [14] доказано, что $R_F < 4, 2, 2 >= 14$ для произвольного поля F. Пока только для этих параметров и двойственных к ним установлено точное значение для $R_F < m, n, p >$ над произвольным полем F.

В работе [15] рассмотрена величина $R_F < 5, 2, 2 >$, для которой получена нижняя оценка $R_F < 5, 2, 2 > \geq 17$ над произвольным полем F. (Отметим, что наилучшая известная верхняя оценка для этой задачи равна 18.) В работе [16] этот результат обобщен: а именно, показано, что $R_F < m, 2, 2 > \geq 3m + 2$ над произвольным полем F для всех $m \geq 3$.

Одним из первых общих результатов о нижних оценках сложности вычислений в алгебрах явилась теорема Алдера - Штрассена [17]. Напомним, что двухсторонним идеалом в алгебре A называется подпространство, замкнутое относительно умножения на любой элемент из A как слева, так и справа. Максимальный двухсторонний идеал в алгебре A — это двухсторонний идеал, отличный от A и не содержащийся ни в каком другом двухстороннем идеале, кроме A.

Теорема 1. *(Alder A., Strassen V., 1981.) Для ранга умножения в ассоциативной алгебре A с единицей справедлива нижняя оценка*

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

где $t(A)$ — количество максимальных двухсторонних идеалов в A.

Поскольку в алгебре матриц порядка n ровно один двухсторонний идеал, отличный от A (нулевая матрица), то для билинейной сложности умножения в алгебре матриц порядка n теорема Алдера - Штрассена дает нижнюю оценку:

$$R(< n, n, n >) \geq 2n^2 - 1.$$

Теорема Алдера - Штрассена породила следующие новые понятия.

Определение 4. Ассоциативная алгебра A с единицей называется *алгеброй минимального ранга*, если $R(A) = 2\dim A - t(A)$, и алгеброй *почти минимального ранга*, если $R(A) = 2\dim A - t(A) + 1$, где $t(A)$ — количество максимальных двухсторонних идеалов в A.

Одна из задач, которая при этом возникла, — описать все алгебры минимального ранга. Вскоре эту задачу удалось решить для локальных алгебр. *Локальная* алгебра — это ассоциативная алгебра с единицей, в каждом базисе которой найдется обратимый элемент. Поскольку в локальной алгебре ровно один двухсторонний идеал $\{0\}$, то теорема Алдера - Штрассена для произвольной локальной алгебры A дает нижнюю оценку:

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

Описание всех локальных алгебр минимального ранга, то есть тех, для которых $R(A) = 2\dim A - 1$, было получено в 1985 году (*Büchi, Clausen* [18]).

Задача полного описания произвольных алгебр минимального ранга с точки зрения их алгебраической структуры решалась многими математиками в течение почти 20 лет. В 2002 году Маркус Блезер получил полное описание всех алгебр минимального ранга над произвольными полями [19].

Теорема 2. *(Bläser M.) Алгебра A над полем k является алгеброй минимального ранга тогда и только тогда, когда*

$$A \cong C_1 \times C_2 \ldots \times C_s \times k^{2\times 2} \times \ldots \times k^{2\times 2} \times B,$$

где $C_1, \ldots, C_s$ — локальные алгебры минимального ранга, $k^{2\times 2}$ — алгебра матриц порядка 2 над полем k, а B — сверхосновная алгебра минимального ранга.

Для билинейной сложности умножения в алгебре матриц порядка 3 теорема Алдера - Штрассена дает нижнюю оценку 17. Однако с помощью

результата Блезера можно показать, что алгебра матриц порядка 3 не является алгеброй минимального ранга, что повышает эту оценку до 18.

Еще одна из алгебр, которая не является алгеброй минимального ранга, — это алгебра кватернионов. Это 4-мерная ассоциативная алгебра, которая в базисе $\{1, i, j, k\}$ задается следующей таблицей умножения:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Теорема Алдера - Штрассена дает для билинейной сложности умножения в этой алгебре нижнюю оценку 7. Однако еще в 1975 году было доказано [20], что билинейная сложность умножения в алгебре кватернионов равна 8, то есть алгебра кватернионов — это алгебра почти минимального ранга. Вопрос об описании всех алгебр почти минимального ранга пока не решен. Но для алгебры матриц порядка 3 Блезер [7] доказал, что она не является алгеброй почти минимального ранга, что повышает оценку билинейной сложности умножения в этой алгебре до 19 (напомним, что наилучшая верхняя оценка для этой сложности — 23).

Одним из камней преткновения при описании алгебр почти минимального ранга оказались алгебры обобщенных кватернионов над произвольным полем отличной от 2 характеристики. Это 4-мерные ассоциативные алгебры, которые в базисе $\{1, i, j, k\}$ задаются следующей таблицей умножения (p, q — ненулевые скаляры):

	1	i	j	k
1	1	i	j	k
i	i	p	k	pj
j	j	$-k$	q	$-qi$
k	k	$-pj$	qi	$-pq$

Известно, что любая алгебра обобщенных кватернионов над полем F отличной от 2 характеристики либо изоморфна алгебре матриц порядка 2 над F (и тогда ее билинейная сложность равна 7), либо является алгеброй с делением, то есть алгеброй, в которой все ненулевые элементы обратимы. В последнем случае из результата Блезера (теорема 2) следует, что алгебра обобщенных кватернионов не является алгеброй минимального ранга и, следовательно, ее билинейная сложность не меньше 8. В 2012 году Лысиков В.В. [21] получил следующий результат.

Теорема 3. *(Лысиков В.В.) Пусть F — поле характеристики, отличной от 2, H — алгебра обобщенных кватернионов с делением над F. Тогда $R_F(H) = 8$.*

Билинейный алгоритм сложности 8 в этой теореме был построен с использованием более общего результата Лысикова В.В. [21].

Теорема 4. *(Лысиков В.В.) Пусть F — поле, A — локальная алгебра над F, $\dim A = n$. Пусть известно, что $R_F(A) > 2n - 1$, то есть A не является алгеброй минимального ранга. Тогда $R(A) = 2n$ (то есть A — алгебра почти минимального ранга) в том и только в том случае, когда в A существуют 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 $\lambda_{ij}, \mu_{ij} \in F$.

Решение задачи о сложности алгебры обобщенных кватернионов позволило полностью завершить описание алгебр почти минимального ранга для случая полупростых алгебр. *Полупростыми* называются алгебры, которые можно представить в виде прямого произведения $D_1^{n_1 \times n_1} \times D_2^{n_2 \times n_2} \times \cdots \times D_t^{n_t \times n_t}$, где все D_i — алгебры с делением, и $D_i^{n_i \times n_i}$ — алгебра матриц порядка n_i над D_i. Поскольку в такой алгебре ровно t максимальных двухсторонних идеалов, то для билинейной сложности умножения в такой алгебре теорема Алдера - Штрассена дает нижнюю оценку: $R(A) \geqslant 2 \dim A - t$.

Известно описание полупростых алгебр почти минимального ранга над полем действительных чисел [22].

Теорема 5. *(Bläser, de Voltaire, 2009). Любая полупростая алгебра почти минимального ранга над $\mathbb{R}$ имеет вид $\mathbb{H} \times \mathbb{R}^{2\times 2} \times \cdots \times \mathbb{R}^{2\times 2} \times \mathbb{C} \times \cdots \times \mathbb{C} \times \mathbb{R} \times \cdots \times \mathbb{R}$.*

Лысикову удалось обобщить этот результат на произвольные поля характеристики, отличной от 2.

Теорема 6. *(Лысиков В.В. [21]) Пусть F — бесконечное поле характеристики, отличной от 2. Любая полупростая алгебра почти минимального ранга над F имеет вид H или $H \times M$, где H — алгебра обобщенных кватернионов с делением, M — алгебра минимального ранга.*

Выше отмечалось, что мультипликативная сложность семейства билинейных форм (при которой предполагается, что все переменные коммутируют между собой) не превосходит билинейной сложности этого же семейства, причем существуют семейства билинейных форм, для которых мультипликативная сложность строго меньше, чем билинейная сложность. Из доказательства теоремы Алдера - Штрассена легко следует, что нижняя оценка этой теоремы справедлива не только для ранга алгебры, но и для мультипликативной сложности. Алгебры, для которых мультипликативная сложность совпадает с этой оценкой, называют *алгебрами минимальной мультипликативной сложности*. Таким образом, любая алгебра минимального ранга является и алгеброй минимальной мультипликативной сложности. Однако в принципе могли бы существовать алгебры, в которых ранг не достигает нижней оценки, а мультипликативная сложность досигает. На самом деле оказывается, что это невозможно. Еще в 1981 году Фейг получил такой результат для алгебр с делением [23].

Теорема 7. *(Feig E., 1981) Алгебра с делением D является алгеброй минимальной мультипликативной сложности тогда и только тогда, когда она является алгеброй минимального ранга.*

Окончательно, для произвольных алгебр этот вопрос разрешил Чокаев в совместных исследованиях с Блезером [24].

Теорема 8. *Произвольная алгебра является алгеброй минимальной мультипликативной сложности тогда и только тогда, когда она является алгеброй минимального ранга.*

Теорема Алдера-Штрассена дает нижнюю оценку на ранг алгебры с коэффициентом 2 при размерности алгебры. Если ограничить семейство алгебр, то удается получать более высокие оценки. Например, для алгебр матриц над алгебрами с делением Блезером [25] был получен следующий результат.

Теорема 9. *(Bläser M., 2005). Пусть F — поле, D — алгебра с делением над F, $D^{n\times n}$ — алгебра матриц порядка n над D и $A \cong D^{n\times n}$. Тогда $R(A) \geqslant \frac{5}{2}\dim A - 3n$.*

Лысикову удалось немного усилить эту оценку для случая, когда D — расширение основного поля.

Теорема 10. *(Лысиков В.В. [21]). Пусть F — поле, K — расширение F, $A \cong K^{n\times n}$. Тогда $R(A) \geqslant \frac{5}{2}\dim A - 3n + 1$.*

Эта оценка лучше других известных оценок при $\dim K = 2$, $n = 3$ и $\dim K = 3$, $n = 2$.

При рассмотрении сложности вычисления систем билинейных форм интересен вопрос о влиянии на эту сложность поля или кольца, над которым эти формы рассматриваются.

Пусть $\varphi\colon U \times V \to W$ — билинейное отображение. Если $x = (a_1, \ldots, a_n)$, $y = (b_1, \ldots, b_m)$, $\varphi(x, y) = (c_1, \ldots, c_l)$ в некоторых базисах, то

$$c_k = \sum_{i=1}^{n}\sum_{j=1}^{m} t_{ijk} a_i b_j.$$

Если коэффициенты t_{ijk} являются целыми числами, то отображение φ можно рассмотреть при a_i и b_j, принадлежащих произвольному кольцу. Такое отображение называется $\mathbb{Z}$-*билинейным*.

Примеры $\mathbb{Z}$-билинейных отображений: умножение матриц; умножение полиномов.

Для умножения матриц известно, например, следующее утверждение [26].

Теорема 11. *Если сложность умножения матриц порядка n над некоторым полем не превосходит $O(n^\alpha)$, то она также не превосходит $O(n^\alpha)$ над любым полем той же характеристики.*

Вопрос о связи сложности $\mathbb{Z}$-билинейных отображений над полями разной характеристики более сложен. Здесь интересный результат получил Лысиков В.В. [27].

Пусть $R_F(\varphi)$ — ранг φ, рассматриваемого как билинейное отображение над полем F. Пусть $\bar{\mathbb{Q}}$ — поле алгебраических чисел (алгебраически замкнутое поле характеристики 0), $\bar{\mathbb{F}}_p$ — алгебраически замкнутое поле характеристики p.

Теорема 12. *(Лысиков В.В. [27]) Пусть φ — $\mathbb{Z}$-билинейное отображение. Тогда*

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

для всех простых характеристик за исключением, может быть, конечного числа.

В 2003 году Генри Коэн и Кристофер Уманс [28] 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 влечет определение сложности умножения матриц.

Определение 5. Алгебра A над полем F называется *групповой алгеброй*, если существует такой базис $g_1, g_2, \ldots, g_n$ этой алгебры, что множество $\{g_1, g_2, \ldots, g_n\}$ образует некоторую группу G относительно умножения в A. В этом случае алгебра A обозначается $F[G]$.

Элементы групповой алгебры можно рассматривать как формальные суммы

$$a_1 g_1 + \ldots + a_n g_n,$$

где $g_1, g_2, \ldots, g_n$ — это все n элементов группы, упорядоченные некоторым образом, а коэффициенты при них — произвольные элементы рассматриваемого поля. При этом элементы групповой алгебры умножаются с учетом дистрибутивности, g_i перемножаются как в группе, а коэффициенты при них перемножаются как элементы поля. Интерес к изучению групповых алгебр в связи с изучением сложности умножения матриц обусловлен следующим результатом из теории представлений групп.

Теорема 13. *Каждая групповая алгебра над полем комплексных чисел является прямым произведением матричных алгебр.*

Поспелов А.Д., Чокаев Б.В. и автор изучали билинейную и мультипликативную сложность умножения в групповых алгебрах для различных групп и полей. Достаточно глубоко был изучен случай групповых алгебр для коммутативных групп. Если рассматривать коммутативные групповые алгебры над алгебраически замкнутыми полями характеристики 0, то ситуация очень проста.

Теорема 14. *Пусть A — коммутативная групповая алгебра над алгебраически замкнутым полем k характеристики 0. Тогда $A \cong k^{\dim A}$ и $R(A) = C(A) = \dim A$. При этом A является алгеброй минимального ранга.*

Для случая алгебраически замкнутых полей простой характеристики p удалось получить следующий результат.

Теорема 15. *(Поспелов А.Д.) Пусть A — коммутативная групповая алгебра размерности n над алгебраически замкнутым полем k простой характеристики p, и $n = p^d t$, $p \nmid t$. Тогда существует такая сверхосновная алгебра B над k минимального ранга, что $A \cong B^t$ и $R(A) = C(A) = 2 \dim A - t$. При этом A является алгеброй минимального ранга.*

Над алгебраически незамкнутыми полями ситуация оказывается намного сложнее. В частности, для поля $\mathbb{R}$ вещественных чисел Поспелов [29] получил следующие результаты.

Теорема 16. *(Поспелов А.Д.) Пусть $G \cong \mathbb{Z}_{n_1} \times \ldots \times \mathbb{Z}_{n_s}$, $n = n_1 \times \ldots \times n_s$ — порядок группы и m — число четных чисел среди $n_1, \ldots, n_s$. Тогда*

$$\mathbb{R}[G] \cong \mathbb{R}^{2^m} \times (\mathbb{R}[X]/(X^2+1))^{\frac{n-2^m}{2}}$$

и

$$R(\mathbb{R}[G]) = C(\mathbb{R}[G]) = \frac{3}{2} \dim \mathbb{R}[G] - 2^{m-1}.$$

Теорема 17. *(Поспелов А.Д.) Пусть $A_1, A_2, \ldots$ — последовательность коммутативных групповых алгебр над полем вещественных чисел.*

1) *Если существует предел $c_A = \lim_{n\to\infty} \frac{R(A_n)}{\dim A_n}$, то он равен одному из чисел $c_0 = \frac{3}{2}$, $c_i = \frac{3}{2} - \frac{1}{2i}$, $i \geq 1$.*

2) *Если $c_A = c_i$, $i \geq 1$, то, начиная с некоторого N, для всех $n \geq N$ выполняется равенство $R(A_n) = c_i \dim A_n$. Если $c_A = c_0$, то всегда $R(A_n) < c_0 \dim A_n$.*

3) *Для любого c_i, $i \geq 0$, существует последовательность коммутативных групповых алгебр над полем вещественных чисел, константа асимптотики сложности которой равна c_i.*

Полностью завершил исследование сложности коммутативных групповых алгебр над полями характеристики 0 Чокаев Б.В. [30]

Теорема 18. *(Чокаев Б.В.) Пусть $A = F[G]$ — групповая алгебра коммутативной группы порядка n над произвольным полем F характеристики 0. Тогда алгебра A является алгеброй минимального ранга и*

$$R(A) = 2n - \sigma_F,$$

где σ_F определяется (довольно сложно) по параметрам разложения группы G в прямое произведение примарных групп и параметрам некоторых неприводимых многочленов над полем F. В частности, для любого поля F характеристики 0 выполняется $\sigma_F \geq \sigma_Q$, где σ_Q — значение параметра σ для поля рациональных чисел.

При этом Чокаевым для любого поля F характеристики 0 описано разложение групповой алгебры коммутативной группы в прямое произведение неразложимых алгебр.

Блезеру удалось построить специальную последовательность алгебр, для которой в нижней оценке мультипликативной сложности (а значит и ранга) коэффициент при размерности алгебры может быть сколь угодно близким к 3. Для полей ненулевой характеристики Чокаеву удалось показать [31], что последовательность алгебр с такой нижней оценкой мультипликативной сложности можно выбрать и среди коммутативных групповых алгебр.

Теорема 19. *(Чокаев Б.В.) Пусть $F[G]$ — групповая алгебра коммутативной группы $G \cong \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$ (n сомножителей) над произвольным полем характеристики p. Тогда*

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

С использованием результатов о сложности групповых алгебр Поспеловым А.Д. получены интересные результаты о сложности умножения полиномов многих переменных [32].

Теорема 20. *(Поспелов А.Д.) Существует алгоритм умножения полиномов над алгебраически замкнутым полем характеристики 0 от m переменных степени N, имеющий билинейную сложность N.*

Теорема 21. *(Поспелов А.Д.) Существует алгоритм умножения полиномов над алгебраически замкнутым полем простой характеристики p от m переменных степени N, имеющий билинейную сложность $2N - t$, где t — наибольший натуральный делитель N, не делящийся на p.*

Соответствующие алгоритмы строятся путем сведения к умножению в коммутативных групповых алгебрах.

Из некоммутативных групп нами были рассмотрены 2 группы — группа подстановок третьего порядка и группа симметрий квадрата [33, 34]. Получены следующие результаты.

Теорема 22. *(Поспелов А.Д., Алексеев В.Б.) Пусть S_3 — полная группа подстановок третьего порядка. Тогда $\mathbb{C}[S_3] \cong \mathbb{C}^{2\times 2} \times \mathbb{C}^2$, $\mathbb{R}[S_3] \cong \mathbb{R}^{2\times 2} \times \mathbb{R}^2$, $R(\mathbb{C}[S_3]) = C(\mathbb{C}[S_3]) = 9$, $R(\mathbb{R}[S_3]) = C(\mathbb{R}[S_3]) = 9$, причем в $\mathbb{C}[S_3]$ (в $\mathbb{R}[S_3]$) существует единственная подалгебра, изоморфная $\mathbb{C}^{2\times 2}$ (соответственно, изоморфная $\mathbb{R}^{2\times 2}$).*

Теорема 23. *(Поспелов А.Д., Алексеев В.Б.) Пусть Q — группа симметрий квадрата. Тогда $\mathbb{C}[Q] \cong \mathbb{C}^{2\times 2} \times \mathbb{C}^4$, $R(\mathbb{C}[Q]) = C(\mathbb{C}[Q]) = 11$. При этом $\mathbb{C}[Q] \cong \mathbb{C}[H]$, где H — группа кватернионов (порядка 8) с элементами ± 1, $\pm i$, $\pm j$, $\pm k$, $H \ncong Q$.*

Нижние оценки в теоремах 22 и 23 легко вытекали бы из гипотезы о прямой сумме (см. первую половину статьи), однако ее справедливость пока не установлена. Поэтому во всех случаях нижние оценки получены независимо с использованием теоремы Алдера-Штрассена.

Для других некоммутативных групп получение точных значений билинейной сложности проблематично, поскольку в их разложениях в прямое произведение матричных групп начинают появляться алгебры матриц порядка большего чем 2. А как отмечено в начале статьи, точное значение билинейной сложности умножения в таких алгебрах пока неизвестно даже для алгебры матриц порядка 3.

Одну из таких групп — группу четных подстановок четвертого порядка — исследовал А.Д. Поспелов [32]. Он установил интересные связи между сложностью соответствующей групповой алгебры и сложностью алгебры матриц порядка 3. Из этих связей он получил очень интересный результат, который гласит, что либо хотя бы в одной из этих алгебр переход от поля вещественных чисел к полю комплексных чисел уменьшает сложность, либо гипотеза о прямой сумме неверна.

Теорема 24. *(Поспелов А.Д.) Пусть A_4 — группа четных подстановок четвертого порядка. Тогда $\mathbb{C}[A_4] \cong \mathbb{C}^{3\times 3} \times \mathbb{C}^3$, $\mathbb{R}[A_4] \cong \mathbb{R}^{3\times 3} \times \mathbb{R} \times \mathbb{R}[X]/(X^2+1)$, $R(\mathbb{C}^{3\times 3}) = R(\mathbb{C}[A_4]) - 3$, $R(\mathbb{R}^{3\times 3}) \geq R(\mathbb{R}[A_4]) - 4$.*

Справедливо, по крайней мере, одно из следующих утверждений:

1) $R(\mathbb{C}^{3\times 3}) < R(\mathbb{R}^{3\times 3})$.

2) Гипотеза о прямой сумме неверна.

3) $R(\mathbb{C}[A_4]) < R(\mathbb{R}[A_4])$.

В заключение отметим, что задача о наименьшей асимптотической сложности умножения матриц порядка n, которая полвека назад дала толчок развитию алгебраической теории сложности, остается пока одной из важнейших нерешенных задач этой теории.

Работа выполнена при финансовой поддержке РФФИ (проект 17-01-00782-а).

Список литературы

[1] Burgisser P., Clausen M. Shokrollahi M.A. Algebraic Complexity Theory. Berlin: Springer-Verlag, 1997.

[2] Strassen V. Gaussian elimination is not optimal // Numer. Math. 1969. Vol. 13. P. 354-356. [Имеется перевод: Штрассен В. Алгоритм Гаусса не оптимален // Кибернетический сборник, вып. 7. М.: Мир, 1970. С. 67-70].

[3] Coppersmith D., Winograd S. Matrix Multiplication via Arithmetic Progressions // J. Symbolic Computation. 1990. Vol. 9, no. 3. P. 251-280.

[4] Waksman A. On Winograd's algorithm for inner products // IEEE Trans. Comput. 1970. Vol. C-19, no. 4. P. 360-361.

[5] Alekseyev V.B. On the complexity of some algorithms of matrix multiplication // Journal of Algorithms. 1985. Vol. 6, no. 1. P. 71-85.

[6] Laderman J.D. A noncommutative algorithm for multiplying 3×3 matrices using 23 multiplications // Bull. Amer. Math. Soc. 1976. Vol. 82, no. 1. P. 126-128.

[7] Bläser M. On the complexity of the multiplication of matrices of small formats // J. Complexity. 2003. Vol. 19. P. 43-60.

[8] Макаров О.М. Некоммутативный алгоритм умножения квадратных матриц пятого порядка, использующий сто умножений // Журн. выч. матем. и матем. физики. 1987. Т. 27, вып. 2. С. 311-315.

[9] Смирнов А.В. О билинейной сложности и практических алгоритмах умножения матриц // Журн. выч. матем. и матем. физики. 2013. Т. 53, вып. 12. С. 1970-1984.

[10] Hopcroft J.E., Musinski J. Duality applied to the complexity of matrix multiplication and other bilinear forms // SIAM J. Comput. 1973. Vol. 2, no. 3. P. 159-173.

[11] Winograd S. On multiplication of 2×2 matrices // Linear Algebra and Appl. 1971. Vol. 4. P. 381-388.

[12] de Groote H.F. On varieties of optimal algorithms for the computation of bilinear mappings. II. Optimal algorithms for 2×2 matrix multiplication // Theoret. Comput. Sci. 1978. Vol. 7, no. 2. P. 127-148.

[13] Hopcroft J.E., Kerr L.R. On minimizing the number of multiplications necessary for matrix multiplication // SIAM J. Appl. Math. 1971. Vol. 20, no. 1. P. 127-148.

[14] Алексеев В.Б., Смирнов А.В. О точной и приближенной билинейных сложностях умножения матриц размеров 4×2 и 2×2 // Современные проблемы математики. 2013. Вып. 17. С. 135-152.

[15] Алексеев В.Б. О билинейной сложности умножения матриц размеров 5×2 и 2×2 // Ученые записки Казанского университета. Серия Физико-математические науки. 2014. Т. 156, вып. 3. С. 19-29.

[16] Алексеев В.Б. О билинейной сложности умножения матриц размеров $m \times 2$ и 2×2 // Чебышевский сборник. 2015. Т. 16, вып. 4. С. 11-27.

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

[18] Büchi W, Clausen M. On a class of primary algebras of minimal rank // Lin. Alg. Appl. 1985. Vol. 69. P. 249-268.

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

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

[21] Лысиков В. В. Об алгебрах почти минимального ранга // Дискретная математика. 2012. Т. 24, вып. 4. С. 3-18.

[22] 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.

[23] Feig E. On systems of bilinear forms whose minimal division-free algorithms are all bilinear // J. Algorithms. 1981. Vol. 2, no. 3. P. 261-281.

[24] Bläser M., Chokaev B. Algebras of minimal multiplicative complexity. // Proc. 27th Ann. IEEE Computational Complexity Conference (CCC). 2012. P. 224-234.

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

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

[27] Лысиков В. В. О билинейных алгоритмах над полями различных характеристик // Вестник Московского Университета. Серия 15: Вычислительная математика и кибернетика. 2013, вып. 4. С. 33-38.

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

[29] Поспелов А. Д. Ранг коммутативных групповых алгебр над полями комплексных и вещественных чисел // Проблемы теоретической кибернетики. Тезисы докладов XIV Международной конференции (Пенза, 23-28 мая2005 г.) Под редакцией О. Б. Лупанова. М.: Изд-во мех.-мат. ф-та МГУ, 2005. С. 125.

[30] Чокаев Б. В. Сложность умножения в коммутативных групповых алгебрах над полями характеристики 0 // Вестник Московского Университета. Серия 15: Вычислительная математика и кибернетика. 2010, вып. 4. С. 30-40.

[31] Чокаев Б. В. Сложность умножения в коммутативных групповых алгебрах над полями простой характеристики // Дискретная математика. 2010. Т. 22, вып. 4. С. 121-137.

[32] Поспелов А. Д. Сложность умножения в ассоциативных алгебрах // Диссертация на соискание ученой степени кандидата физико-математических наук / Московский государственный университет им. М.В. Ломоносова. М., 2008.

[33] Алексеев В. Б., Поспелов А. Д. Сложность умножения в некоторых групповых алгебрах // Дискретная математика. 2005. Т. 17, вып. 1. С. 3-17.

[34] Алексеев В. Б., Поспелов А. Д. Сложность умножения в групповой алгебре симметрий квадрата // Труды 6-ой Международной конференции « Дискретные модели в теории управляющих систем», 7-11 декабря 2004 г. М.: Изд. отдел ф-та ВМиК МГУ, 2004. С. 8-11.

On some results in algebraic complexity theory

Alekseev V.B.

In this paper we give a survey of some results on the computational complexity of algebras, in particular, obtained at the Department of Mathematical Cybernetics of the M.V. Lomonosov Moscow State University by the author and his students: Pospelov A.D., Chokaev B.V., Lysikov V.V.

Keywords: algebraic complexity, algebra, rank of algebra, bilinear complexity, multiplicative complexity, complexity of matrix multiplication.