АЛГОРИТМИЧЕСКАЯ СЛОЖНОСТЬ ЛИНЕЙНЫХ АЛГЕБР

А.Альдер, Ф.Штрассен,
Цюрих, Швейцария

Резюме. Сложность $L(A)$ конечномерной ассоциативной алгебры A – это число нескалярных умножений/делений оптимального алгоритма, вычисляющего произведение двух элементов этой алгебры. Мы показываем, что

$$L(A) \geq 2 \cdot \dim A - t,$$

где t – число максимальных двусторонних идеалов A.

Введение

I. Пусть k – поле. Чтобы избежать трудностей с моделью вычислений, мы считаем k бесконечным. Пусть $x_1, \ldots, x_n$ – переменные над k. Следуя **Ostrowski** (I954), введем

О п р е д е л е н и е I. Последовательность рациональных функций $g_1, \ldots, g_r \in k(x_1, \ldots, x_n)$ называется вычислительной последовательностью, если для любого $\rho \leq r$ имеются

$u_\rho, v_\rho \in k + kx_1 + \ldots + kx_n + kg_1 + \ldots + kg_{\rho-1}$, такие что

$$g_\rho = u_\rho \cdot v_\rho \quad \text{или} \quad g_\rho = u_\rho / v_\rho$$

(В последнем случае предполагается, что $v_\rho \neq 0$).

О п р е д е л е н и е 2. Пусть $f_1, \ldots, f_q \in k(x_1, \ldots, x_n)$. Сложность $L(f_1, \ldots, f_q)$ набора $f_1, \ldots, f_q$ – это наименьшее r со следующим свойством: существует вычислительная последовательность $g_1, \ldots, g_r$, такая что для всех $i \leq q$

$$f_i \in k + kx_1 + \ldots + kx_n + kg_1 + \ldots + kg_r.$$

Идея этой модели состоит в том, что линейные операции, такие как сложения, вычитания и скалярные умножения допускают-

ся бесплатно и что ставится задача минимизации умножений/делений. Переменные $x_1, \ldots, x_n$ представляют входы. (Детали см. в **Borodin-Munro** (1975)).

В этой статье под алгеброй мы всегда понимаем конечномерную ассоциативную алгебру с единицей. Пусть $e_1, \ldots, e_n$ – базис векторного пространства A,

$$e_i \cdot e_j = \sum_{l=1}^{n} \tau_{ijl} e_l,$$

где $\tau_{ijl} \in k$. Тогда мы имеем

$$\left(\sum_{i=1}^{n} \xi_i e_i\right) \cdot \left(\sum_{j=1}^{n} \eta_j e_j\right) = \sum_{l=1}^{n} \left(\sum_{i,j=1}^{n} \tau_{ijl} \xi_i \eta_j\right) e_l.$$

О п р е д е л е н и е 3. Сложность A – это

$$L(A) = L\left(\left\{\sum_{i,j=1} \tau_{ijl} x_i y_j : 1 \le l \le n\right\}\right),$$

где $\sum_{i,j=1}^{n} \tau_{ijl} x_i y_j \in k(x_1, \ldots, x_n, y_1, \ldots, y_n)$.

Очевидно, что сложность $L(A)$ не зависит от выбора базиса и инварианта относительно изоморфизмов. Более того, сложность не возрастает при переходе от алгебры к подалгебре или гомоморфному образу и всегда выполняется

$$L(A \times B) \le L(A) + L(B).$$

Если $\dim A = n$, то $L(A) \ge n$, где равенство достигается тогда и только тогда, когда $A \simeq k^n$ (**Strassen** (1973); в действительности в этой работе перечисленные факты сформулированы и доказаны для ранга, а не для сложности).

Изучение взаимосвязи между алгебраическим и алгоритмическим аспектами алгебр, как это представляется структурной теорией и теорией сложности, является, по-видимому, темой, достойной Аль-Хорезми, от имени которого происходят слова алгебра и алгоритм.

Несколько авторов заметили, что $L(\mathbb{C}) = 3$, где $\mathbb{C}$ рассмат-

ривается как алгебра над вещественными числами. **Fiduccia-Zalcstein** (I977) доказали, что для алгебры с делением

$$L(A) \geq 2 \cdot \dim A - 1. \qquad (1)$$

Они также показали, что здесь достигается равенство, когда A является простым расширением некоторого поля. Однако равенство имеет место **не**всегда. **Dobkin** (I973), **de Groote** (I975), **Howell-Lafon** (I975) и **Stoss** (I979) доказали

$$L(\text{вещественные кватернионы}) = 8 \qquad (2)$$

Очень важной задачей является изучение сложности полной алгебры матриц M_n или, что то же самое, сложности умножения матриц. Старый результат

$$L(M_{2^q}) \leq 7^q, \quad L(M_n) = O(n^{2 \cdot 81}),$$

который получил **Strassen** (I969), недавно улучшили **Pan** (I978), **Bini-Capovani-Lotti-Romani** (I979), **Bini** (I979), **Schönhage** (I979,I980), **Pan** (I979,I980) до

$$L(M_n) = O(n^{2 \cdot 52}).$$

Что касается нижних оценок, то **Hopcroft-Kerr** (I97I) и **Winograd** (I97I) доказывают

$$L(M_2) = 7,$$

а **Brockett-Dobkin** (I978) и **Lafon-Winograd** (I980) приводят общую нижнюю оценку

$$L(M_n) \geq 2n^2 - 1. \qquad (3)$$

Кое-что также известно о не полупростых алгебрах. Пусть нильалгебра имеет базис $1, e_2, \ldots, e_n$, где $e_i \cdot e_j = 0$ для всех i,j. Тогда

$$L(\text{нильалгебра}) = 2n - 1. \qquad (4)$$

Прекрасный результат **Fiduccia-Zalcstein** (I977) и **Winograd** (I977) дает сложность алгебры, порождаемой одним элементом:

пусть $f \in k[t]$ – ненулевой полином степени n, имеющий m различных простых множителей. Тогда

$$L(k[t]/(f)) = 2n - m. \qquad (5)$$

Хотя доказательства нижних оценок, о которых шла речь выше, сильно отличаются друг от друга, все они используют в качестве основного инструмента, так называемый, метод подстановок, Пан (I966). Это наводит на мысль, что нужно попытаться объединить эти результаты в один. Следующая теорема, доказанная в разделе 2, почти достигает эту цель.

Т е о р е м а. Пусть A – произвольная алгебра. Тогда $L(A) \geq 2 \cdot \dim A$ – (число максимальных двусторонних идеалов алгебры A).

Поскольку алгебры с делением и полные матричные алгебры, а также нильалгебра, имеют только один максимальный двусторонний идеал, мы получаем (I), (3) и (4). Так как число максимальных идеалов в $k[t]/(f)$ равно числу различных простых множителей полинома f, мы получаем оценку снизу из (5). (Оценка сверху легко следует из китайской теоремы об остатках). Следствием не является лишь результат о кватернионах (2). С другой стороны, конечно, имеются многочисленные новые приложения. Приведем пример одного из них.

Пусть $k = \mathbb{C}$. Если G – конечная абелева группа порядка g, $\mathbb{C}[G]$ – ее групповая алгебра, то, очевидно,

$$L(\mathbb{C}[G]) = L(\mathbb{C}^g) = g.$$

Пусть D_{2n} – диэдральная группа порядка $2n$. Тогда наша теорема влечет

$$L(\mathbb{C}[D_{2n}]) = \begin{cases} (7n - 3)/2, & \text{если } n \text{ нечетное,} \\ (7n - 6)/2, & \text{если } n \text{ четное.} \end{cases}$$

Действительно, если n нечетное, то мы имеем (используя теорию характеров)

$$\mathbb{C}[D_{2n}] \simeq \mathbb{C}^2 \times M_2(\mathbb{C})^{(n-1)/2},$$

если n четное, то мы имеем

$$\mathcal{C}[D_{2n}] \simeq \mathcal{C}^4 \times M_2(\mathcal{C})^{n/2-1}.$$

Доказательства

2. Умножение в алгебре A – это билинейное отображение $A \times A \to A$. Нам нужно будет рассмотреть вычислительную сложность несколько более общих отображений, а именно, однородных квадратичных отображений.

О п р е д е л е н и е 4. Пусть E, W – конечномерные векторные k-пространства с базисами, соответственно $e_1, \ldots, e_n$ и $\hat{e}_1, \ldots, \hat{e}_q$. Отображение $f: E \to W$ называется квадратичным, если имеются квадратичные формы $f_1, \ldots, f_q$ из $k[x_1, \ldots, x_n]$, такие что для всех $\xi_1, \ldots, \xi_n \in k$

$$f\left(\sum_{j=1}^{n} \xi_i e_i\right) = \sum_{l=1}^{q} f_l(\xi_1, \ldots, \xi_n)\hat{e}_l.$$

Мы называем $L(f) = L(f_1, \ldots, f_q)$ сложностью f ($f_1, \ldots, f_q$ рассматриваются здесь как элементы $k(x_1, \ldots, x_n)$).

Понятие квадратичного отображения и сложности f не зависит от выбора базисов. Если $\varphi: E' \to E$, $\phi: W \to W'$ – линейные отображения, то отображение $\phi f \varphi$ является снова квадратичным и

$$L(f) \geq L(\phi f \varphi). \qquad (6)$$

П р е д л о ж е н и е . Пусть $f: E \to W$ – квадратичное отображение. Тогда $L(f) \leq r$ тогда и только тогда, когда имеются $u_\rho, v_\rho \in E^*$, $w_\rho \in W$ ($\rho = 1, \ldots, r$), такие что для всех $x \in E$

$$f(x) = \sum_{\rho=1}^{r} u_\rho(x) \cdot v_\rho(x) \cdot w_\rho,$$

где E^* обозначает пространство, двойственное к E.

Доказательство этого предложения хорошо известно и следу-

ет из того факта, что множество квадратичных форм можно оптимально вычислять без деления (см. Strassen 1973).

В следующей лемме собрано несколько фактов об алгебрах, которые понадобятся позже. Все они являются немедленными следствиями классической структурной теории Веддерберна. Если A – алгебра, то через $\mathrm{rad}\,A$ мы обозначаем радикал (Джекобсона) алгебры A.

Лемма 1. A и $A/\mathrm{rad}\,A$ имеют одно и то же число максимальных двусторонних идеалов. (7)

$A/\mathrm{rad}\,A$ является полупростой. (8)

Любой левый идеал полупростой алгебры имеет дополнение, которое является левым идеалом. Аналогично для правых идеалов. (9)

Любая полупростая алгебра является конечным прямым произведением простых алгебр. (10)

Если A простая, а L и R – минимальный левый и правый идеал соответственно, то

$$\dim L = \dim R. \tag{11}$$

Если A простая, $x \in A$ и R ненулевой правый идеал, такой, что $ax = 0$ для всех $a \in R$, то $x = 0$.

Аналогично, если L ненулевой левый идеал, такой что $xa = 0$ для всех $a \in L$, то $x = 0$. (12)

Бо́льшую часть доказательства нашей теоремы разобьем на две леммы.

Лемма 2. Пусть A,B – алгебры. Тогда

$$L(A\times B) \geq L((A/\mathrm{rad}\,A)\times B) + 2\cdot\dim(\mathrm{rad}\,A).$$

Доказательство. Мы покажем, что

$$L(A) \geq L(A/\mathrm{rad}\,A) + 2\cdot\dim(\mathrm{rad}\,A)$$

(принимая во внимание, что тогда B тривиальна).
Пусть $L(A) = r$. Тогда имеются $u_\rho, v_\rho \in (A\times A)^*$, $w_\rho \in A$, такие, что для всех $a,b \in A$

$$a\cdot b = \sum_{\rho=1}^{r} u_\rho(a, b)\cdot v_\rho(a, b)\cdot w_\rho. \tag{13}$$

Пусть $q = \dim(\mathrm{rad}\, A)$. Достаточно найти представление (I3) с дополнительным свойством

$u_1, \ldots, u_{2q}$ линейно независимы в $\mathrm{rad}\, A \times \mathrm{rad}\, A$ (в частности, $2q \le r$). (14)

Действительно, допустим (I4) и пусть

$$E = \{u_1 = \ldots = u_{2q} = 0\} \subset A \times A$$

и пусть $f: E \to A$ – ограничение умножения. Тогда f – квадратичное отображение с $L(f) \le r - 2q$, (15)

(ибо $f(a, b) = \sum_{\rho=2q+1}^{r} u_\rho(a, b) \cdot v_\rho(a, b) \cdot w_\rho$ на E.)

Пусть μ (соответственно μ') – умножение в A (соответственно $A/\mathrm{rad}\, A$).

Коммутативная диаграмма

$$\begin{array}{ccc} A \times A & \xrightarrow{\mu} & A \\ \downarrow & & \downarrow \\ A/\mathrm{rad}A \times A/\mathrm{rad}A & \xrightarrow{\mu'} & A/\mathrm{rad}\, A \end{array}$$

дает (с помощью ограничения) коммутативную диаграмму

$$\begin{array}{ccc} E & \xrightarrow{f} & A \\ \downarrow \alpha & & \downarrow \\ A/\mathrm{rad}\, A \times A/\mathrm{rad}\, A & \xrightarrow{\mu'} & A/\mathrm{rad}\, A \end{array}$$

Поскольку $E \cap (\mathrm{rad}\, A \times \mathrm{rad}\, A) = 0$, то α – изоморфизм. Тогда

$$\begin{array}{ccc} E & \xrightarrow{f} & A \\ \downarrow \alpha^{-1} & & \downarrow \\ A/\mathrm{rad}\, A \times A/\mathrm{rad}A & \xrightarrow{\mu'} & A/\mathrm{rad}\, A \end{array}$$

коммутативна. Поэтому, в силу (6) и (I5), мы имеем

$$L(A/\operatorname{rad} A) = L(\mu') \le L(f) \le r - 2q = L(A) - 2\cdot\dim(\operatorname{rad} A).$$

Это показывает, что достаточно иметь (I3) со свойством (I4).

Мы утверждаем, что это можно достичь перестановкой членов суммы (I3) и взаимозаменой некоторых u_ρ и v_ρ. Если это не так, то существует $p < 2q$, $p \le r$ такое, что, не умаляя общности

$$\begin{cases} u_1, \dots, u_p & \text{линейно независимы в } \operatorname{rad} A \times \operatorname{rad} A, \\ u_{p+1}, \dots, u_r, v_{p+1}, \dots, v_r & \text{линейно независимы на } u_1, \dots, u_p \\ \text{как линейных формах на } \operatorname{rad} A \times \operatorname{rad} A. & \end{cases} \tag{16}$$

Поскольку $p < 2q$, то имеются $x, y \in \operatorname{rad} A$, не равные оба нулю, такие что $u_1(x, y) = \dots = u_p(x, y) = 0$, а поэтому в силу (I6)

$$u_1(x, y) = \dots = u_r(x, y) = v_{p+1}(x, y) = \dots = v_r(x, y) = 0.$$

Для дальнейшего зафиксируем такую пару (x, y). Если $a, b \in A$, $u_1(a, b) = \dots = u_p(a, b) = 0$, то мы имеем

$$(a + x)(b + y) = \sum_{\rho=1}^{r} u_\rho(a + x, b + y)\cdot v_\rho(a + x, b + y)\cdot w_\rho =$$

$$= \sum_{\rho=1}^{r} (u_\rho(a, b) + u_\rho(x, y))\cdot(v_\rho(a, b) + v_\rho(x, y))\cdot w_\rho =$$

$$= \sum_{\rho=p+1}^{r} u_\rho(a, b)\cdot v_\rho(a, b)\cdot w_\rho = a\cdot b. \tag{17}$$

Если $a, b \in A$ произвольны, то мы используем линейную независимость $u_1, \dots, u_p$ на $\operatorname{rad} A \times \operatorname{rad} A$, чтобы найти $s, t \in \operatorname{rad} A$, такие что

$$\forall i \le p \quad u_i(s, t) = -u_i(a, b).$$

Тогда

$$u_1(a + s, b + t) = \dots = u_p(a + s, b + t) = 0.$$

Вместе с (I7) это дает следующее.

Если $a,b \in A$, то имеются $s,t \in \operatorname{rad} A$, такие что

$$(a + s)(b + t) = (a + s + x)(b + t + y). \tag{18}$$

Для некоторого $i \geq 1$ мы имеем

$$x,y \in (\operatorname{rad} A)^i \text{ и, скажем, } x \notin (\operatorname{rad} A)^{i+1}.$$

Взяв $a = 0, b = 1$ в (I8), мы получаем

$$s(1 + t) = (s + x)(1 + t + y),$$

поэтому

$$x = -x(t + y) - sy \in (\operatorname{rad} A)^{i+1},$$

получили противоречие.

Л е м м а 3. Пусть A, B – алгебры, причем A – простая. Тогда

$$L(A \times B) \geq 2 \cdot \dim A - 1 + L(B).$$

Д о к а з а т е л ь с т в о . Как и в предшествующей лемме мы удовлетворимся тем, что покажем

$$L(A) \geq 2 \cdot \dim A - 1.$$

Пусть

$$\dim A = n,$$

$$L(A) = r.$$

Тогда имеются u_ρ, $v_\rho \in (A \times A)^*$, $w_\rho \in A$, такие что

$$\forall a, b \in A \quad a \cdot b = \sum_{\rho=1}^{r} u_\rho(a, b) \cdot v_\rho(a, b) \cdot w_\rho. \tag{19}$$

Пусть

$$A = R_1 \oplus R_2,$$

где R_1, R_2 – правые идеалы, R_1 – минимальный. Положим

$$\dim R_1 = m,$$

тогда

$$\dim R_2 = n - m.$$

(i) Ясно, что $w_1,\ldots, w_r$ порождают A. Поэтому $r \geq n$ и, не умаляя общности, мы можем считать, что $w_1,\ldots,w_{m-1}$ линейно независимы и что, взяв

$$W = kw_1 + \ldots + kw_{m-1},$$

мы имеем

$$W \cap R_2 = 0 \qquad (20)$$

($w_1,\ldots,w_{m-1}$ следует выбрать так, что $w_1 + R_2,\ldots,w_{m-1} + R_2$ линейно независимы в A/R_2).

Пусть $\pi : A \to R_1$ – проекция вдоль R_2.

$$(\pi(W) : R_1) = \{a : R_1 \mid a \subset \pi(W)\}$$

является левым идеалом, отличным от A, и поэтому он содержится в некотором максимальном левом идеале L_2. Пусть L_1 – дополнительный левый идеал. Тогда

$$A = L_1 \oplus L_2$$

и по лемме I

$$\dim L_1 = m,$$

$$\dim L_2 = n - m.$$

Если $n = m$, то следующие два шага доказательства следует опустить.

Мы утверждаем, что, не умаляя общности, $u_m,\ldots,u_{n-1}$ линейно независимы на $O \ltimes L_2$. Мы действуем так же, как в доказательстве леммы 2, и пытаемся добиться желаемой линейной независимости, переставляя члены $\rho = m,\ldots,r$ суммы (I9) и переставляя некоторые u_ρ с v_ρ для $\rho \geq m$. Неудача дала бы p, такое что $m - 1 \leq p < n - 1$ и, не умаляя общности,

$u_1,\ldots,u_p$ линейно независимы на $O \ltimes L_2$.

$$u_{p+1},\ldots,u_r, v_{p+1},\ldots,v_r \qquad (21)$$

линейно зависят от $u_m, \ldots, u_p$ как линейные формы на $0 \times L_2$.

Поскольку $p - m + 1 < n - m = \dim L_2$, то мы можем выбрать

$$y \in L_2, \ y \neq 0, \tag{22}$$

так чтобы $u_m(0, y) = \ldots = u_p(0, y) = 0$, и поэтому в силу (21),

$$u_m(0, y) = \ldots = u_r(0, y) = v_{p+1}(0, y) = \ldots = v_r(0, y) = 0.$$

Если $a, b \in A$, $u_m(a, b) = \ldots = u_p(a, b) = 0$, то мы имеем

$$a(b + y) = \sum_{\rho=1}^{r} (u_\rho(a, b) + u_\rho(0, y))(v_\rho(a, b) + v_\rho(0, y)) \cdot w_\rho =$$

$$= \sum_{\rho=1}^{r} u_\rho(a, b) \cdot v_\rho(a, b) \cdot w_\rho + \tilde{w} = a \cdot b + \tilde{w},$$

где $\tilde{w} \in k \cdot w_1 + \ldots + k \cdot w_{m-1} = W$, т.е.

$$ab - a(b + y) \in W. \tag{23}$$

Мы не упрощаем член в левой части (23), поскольку настоящее рассуждение будет служить моделью для случаев (iii) и (iv).

Если $a, b \in A$ произвольны, то мы используем линейную независимость $u_m, \ldots, u_p$ на $0 \times L_2$, чтобы найти $t \in L_2$, такое что

$$u_m(a, b + t) = \ldots = u_p(a, b + t) = 0.$$

Вместе с (23) мы получаем

$$\forall a, b \in A \quad \exists t \in L_2 \quad a(b + t) - a(b + t + y) \in W. \tag{24}$$

С использованием (20) отсюда следует

$$\forall a \in R_2 \quad a \cdot y \in W \cap R_2 = 0,$$

что невозможно в силу леммы I и (22).

(iii) Не умаляя общности, $u_m, \ldots, u_{2n-m-1}$ линейно независимы на $R_2 \times L_2$ (в частности, $r \geq 2n - m - 1$). В противном случае мы действуем как в (ii), оставляя фиксиро-

ванными первые $n-1$ членов суммы (I9). Мы получаем

$$x \in R_2,\ y \in L_2,\ x \neq 0,$$

такие что

$$\forall a, b \in A\ \exists s \in R_2,\ t \in L_2\ (a+s)(b+t) - (a+s+x)(b+t+y) \in W.$$

(Ср. с (24). Случай $x = 0, y \neq 0$ невозможен, ибо $u_m(0,y) = \ldots = u_{n-1}(0,y) = 0$ влечет $y = 0$ в силу (ii)). Мы выбираем $a = 0$, $b \in L_1$. Тогда

$$x(b+t+y) + sy \in W.$$

Так как $x, s \in R_2$, то используя (20), мы имеем

$$xb + x(t+y) + sy = 0$$

и ввиду $t, y \in L_2$, $b \in L_1$ получаем

$$xb \in L_1 \cap L_2 = 0.$$

Поскольку элемент $b \in L_1$ произволен, получаем $x = 0$ в силу леммы I – противоречие.

(iv) Не умаляя общности, $u_m, \ldots, u_{2n-1}$ линейно независимы на $R_2 \times A$ (в частности, $r \geq 2n-1$, что и составляет утверждение доказываемой леммы). В противном случае существуют

$$x \in R_2,\ y \in A,\ y \notin L_2,$$

такие что

$$\forall a, b \in A\ \exists s \in R_2,\ t \in A$$

$$(a+s)(b+t) - (a+s+x)(b+t+y) \in W.$$

(На этот раз следует фиксировать первые $2n-m-1$ членов в (I9)). Мы выбираем $a \in R_1$, $b = 0$. Тогда

$$(a+s)y + x(t+y) \in W,$$

поэтому

$$\pi((a + s)y + x(t + y)) = ay \in \pi(W).$$

Поскольку элемент $a \in R_1$ произволен, то мы получаем

$$y \in (\pi(W):R_1) \subset L_2$$

- противоречие.

Доказательство теоремы. Пусть

$$A/\mathrm{rad}\, A \simeq A_1 \times \ldots \times A_t,$$

где $A_1, \ldots, A_t$ - простые алгебры. Тогда по лемме 2

$$L(A) \geq L(A_1 \times \ldots \times A_t) + 2 \cdot \dim(\mathrm{rad}\, A) \geq$$

$$\geq \sum_{i=1}^{t} (2 \cdot \dim A_i - 1) + 2 \cdot \dim(\mathrm{rad}\, A) =$$

(по лемме 3, используя индукцию)

$$= 2 \cdot \dim - t =$$

= 2·dim A - число максимальных двусторонних идеалов алгебры $A/\mathrm{rad}\, A$ =

= 2·dim A - число максимальных двусторонних идеалов алгебры A.

Наше доказательство этой теоремы в действительности дает следующий более общий результат:

Если A,B - алгебры, то

$L(A \times B) \geq L(B) + 2 \cdot \dim A$ - число максимальных идеалов алгебры A.

Это верно, даже если заменить в произвольным квадратичным отображением.

Авторы благодарны Вальтеру Бауру за помощь в доказательстве леммы 2.

Литература

D.Bini, M.Capovani, G.Lotti and F.Romani. $O(n^{2.7799})$ complexity for matrix multiplication. - Inform.Process.Lett. 1979, v.8, p. 234-235.

D.Bini. Relations between EC-algorithms and APA-algorithms, applications. - Nota interna B79/8 (march 1979) I.E.I. Pisa.

A.Borodin and I.Munro. The computational complexity of algebraic and numeric problems. American Elsevier, 1975.

R.W.Brockett and D.Dobkin. On the optimal evaluation of a set of bilinear forms. - Linear Algebra and Its Applications, 1978, 19, p. 207-235.

D.Dobkin. On the arithmetic complexity of a class of arithmetic computations. Thesis, Harvard University, 1973.

C.M.Fiduccia and I.Zalcstein. Algebras having linear multiplicative complexity. - J. Assoc. Comput. Mach., 1977, 24, p. 311-331.

H.F. de Groote. On varieties of optimal algorithms for the computation of bilinear mappings II. Optimal algorithms for 2x2-matrix multiplication. - Theor. Comput. Sci.,1978, no.7, p. 127-148.

J.Hopcroft and L.Kerr. On minimizing the number of multiplications necessary for matrix multiplication. - SIAM J. Applied Math., 1971, 20, p. 30-36.

T.D.Howell and J.C.Lafon. The complexity of the quaternion product. - Cornell University TR 75-245, 1975.

J.C.Lafon and S.Winograd. to appear, 1980.

A.M.Ostrowski. On two problems in abstract algebra connected with Horner's rule. - Studies Presented to R. von Mises, Academic Press, New York, 1954, p. 40-48.

В.Я.Пан. О способах вычислений значений многочленов. - Успехи мат. наук, 1966, вып.21, № 1, с. 103-134.

V.Ya.Pan. Strassen's algorithm is not optimal. - Proc. 19th Ann. Symp. on Foundations of Comput. Sci., 1978, p. 166-176.

V.Ya.Pan. New fast algorithms for matrix operations. - SIAM J. on Comput., 1980, v.9, no.2, p. 321-342.

V.Ya.Pan. Field extension and trilinear aggregating, uniting and cancelling for the acceleration of matrix multiplication. - Proc. 20th Ann. Symp. on Foundations of Comput. Sci., 1979, p. 28-38.

V.Ya.Pan. New combination of methods for the acceleration of matrix multiplication. - Preprint, State University of New York at Albany, 1980.

A.Schönhage. Partial and total matrix multiplication. - TR, Math. Inst. Uni. Tübingen, June 1979.

A.Schönhage. Partial and total matrix multiplication. - TR, Math. Inst. Uni. Tübingen, January 1980. To appear.

H.J.Stoss. Private communication, 1979.

V.Strassen. Gaussian elimination is not optimal. - Numer. Math., 1969, 13, p. 354-356.

V.Strassen. Vermeidung von Divisionen. - J. für reine und angew. Mathematik, 1973, 264, p. 184-202.

S.Winograd. On multiplication of 2x2 matrices. - Linear Algebra Appl., 1971, 4, p. 381-388.

S.Winograd. Some bilinear forms whose multiplicative complexity depends on the field of constants. - Math. Syst. Theory, 1977, 10, p. 169-180.