stichting
mathematisch
centrum

DEPARTMENT OF COMPUTER SCIENCE IW 41/76 FEBRUARY

J. VAN LEEUWEN & P. VAN EMDE BOAS

SOME ELEMENTARY PROOFS OF LOWER-BOUNDS IN COMPLEXITY THEORY

Prepublication

Second edition

2e boerhaavestraat 49 amsterdam

Printed at the Mathematical Centre, 49, 2e Boerhaavestraat, Amsterdam.

The Mathematical Centre, founded the 11-th of February 1946, is a non-profit institution aiming at the promotion of pure mathematics and its applications. It is sponsored by the Netherlands Government through the Netherlands Organization for the Advancement of Pure Research (Z.W.O), by the Municipality of Amsterdam, by the University of Amsterdam, by the Free University at Amsterdam, and by industries.

AMS(MOS) subject classification scheme (1970): 68A20

ACM -Computing Reviews- Categories: 5.25

First printing August 1975

Second edition February 1976

Some elementary proofs of lower-bounds in complexity theory [*)]

by

J. Van Leeuwen & P. van Emde Boas

ABSTRACT

We introduce a new and easily applicable criterion called rank-immunity for estimating the minimal number of multiplications needed to compute a set of bilinear forms in commuting variables. The result is obtained by an elimination argument after canonically embedding computations in a quotient-ring R/I where I is an appropriately choosen ideal that is left invariant under the eliminations. The criterion combines the wellknown arguments based on elimination and on row-rank, but in contrast to for instance column- and mixed rank arguments it normally leads to better elementary estimates than were derivable in a uniform manner before.

KEY WORDS & PHRASES: *lower bounds, minimal number of multiplications, rank-immunity, bilinear problems.*

"Get the most for the least"
The minimizer, M & T Bank

[*)] This paper is not for review; it is meant for publication elsewhere

1. Let k be a field, and let $x_1,\dots,x_n$ and $y_1,\dots,y_m$ be distinct and independent commuting indeterminates.

WINOGRAD [22] proved that even in a more general setting lowerbounds on the number of multiplications needed to compute a finite set of bilinear forms $\sum \alpha_\ell x_{i_\ell} y_{j_\ell}$ over $k \cup \{x_1,\dots,x_n\} \cup \{y_1,\dots,y_m\}$ may be obtained using criteria of linear independence. FIDUCCIA [8] was probably among the first to notice that fast algorithms for bilinear forms relate to an appropriate matrix-decomposition, and in an interesting argument STRASSEN [21] proved that indeed the minimal number of multiplications to compute such forms is exactly equal to the minimal rank of an associated tensor.

Although the tensor-rank is certainly an exact bound it is classically known that in nearly all practical cases it is very hard to compute. Thus BROCKETT & DOBKIN [2] and DOBKIN [4] had to go through involved arguments to obtain for instance a lowerbound of $3n^2 - 3n + 1$ multiplications to form the product of two n × n matrices by actually estimating the rank of the 3rd order tensor involved. (The proof however has since fallen apart and the presently provable best lowerbound on the complexity of matrix multiplication is $2n^2 - 1$, DOBKIN [6]). The lowerbounds and optimality-proofs for matrix-products in HOPCROFT & KERR [13] and HOPCROFT & MUSINSKI [14] again use the variable-elimination and rank-arguments of Winograd but only by assuming non-commutativity of the indeterminates to further restrain the straight-line programs which they had to consider and to reduce problems to the case of separated variables.

In this paper we shall prove some theorems which lead to easy proofs of various non-trivial lowerbounds for bilinear forms in commuting variables by cleaning up the straight line programs pertaining in these problems over a ring R through the generous act of also giving the elements of an appropriate ideal I for free, and thus effectively considering computations in the ring R/I.

The theorems of Winograd and Fiduccia are also valid in R/I, but we shall prove that the kinds of argument known from these studies can be extended in the factor-ring so that we can in fact obtain a stronger, although still elementary criterion for lowerbounds in the computational complexity of bilinear forms.

Instead of the traditional notions of rank, we shall prove that a concept called rank-immunity can be entirely justified in the factor-ring. Rank-immunity relates to the observed phenomenon that the rank of a matrix may be insensitive to the elimination of some of the occurring variables, but an argument based on it is only correct over R/I. Thus in general there is hope that intricate arguments with tensors may be replaced by the easier argument of factoring over the appropriate ideal.

The use of rank-immunity in proofs of lowerbounds will be illustrated in a variety of practical examples most of which are known but seldomly shown by a uniform argument.

2. Let R be a ring extending $k \cup \{x_1,\ldots,x_n\} \cup \{y_1,\ldots,y_m\}$ and consider the computation of some elements of R.

To estimate the minimal number of multiplications required for this task we shall first have to settle on the precise class of algorithms among which we search for the best and on what we shall actually count in these algorithms.

As motivated in AHO, HOPCROFT & ULLMAN [1] (ch.12) it appears that in these problems it is useful to choose for straight-line programs (or schemes), which are finite sequences $s_1,s_2,\ldots$ in R such that each s_i is either in $k \cup \{x_1,\ldots,x_n\} \cup \{y_1,\ldots,y_m\}$ or the sum or product of previous elements in the sequence, and which contain the elements of R which we wished to compute. The mathematical implications of this definition in structures of arbitrary type were given by STRASSEN [19], [20]. We shall sometimes compact the straight-line programs if we are not interested in all individual steps.

For mathematical convenience we shall regard multiplications by elements of k for free and only count the multiplications in which both operands depend on x's or y's. Thus like OSTROWSKI [18] already did we shall actually assume that after the ith step in a straight-line program we possess the entire module generated by $s_1,\ldots,s_i$ and only count a multiplication s_{i+1} when the module properly extends (see also FIDUCCIA [7]).

It is no restriction to assume from now on that
$R = k[x_1,\ldots,x_n,y_1,\ldots,y_m]$.

The tasks considered in this paper are all of the following type:

$$\text{compute } B\underline{x} + \underline{u} \quad \text{modulo } k \cup \{x_1,\ldots,x_n,y_1,\ldots,y_m\}$$

where B is a matrix whose entries are linear functions in the y's, $x = [x_1,\ldots,x_n]^T$, and $\underline{u}$ is a columnvector whose coordinates are polynomials in the x's or in the y's exclusively (that is, x's and y's do not occur simultaneously in $\underline{u}$ and it is entirely used as an "x-residu" or as a "y-residu").

The rank-concepts which are normally applied to B are based on the notion of independence modulo k (see e.g. WINOGRAD [22] or AHO-HOPCROFT-ULLMAN [1]). A collection of vectors is called independent modulo k if there exists no non-trivial k-linear combination of the vectors such that in the resulting sum all indeterminates have disappeared.

If the results of distinct multiplication steps in some algorithm to compute a task of the given type are denoted by $s_1,\ldots,s_l$ then one can automatically obtain from such an algorithm an equality of the form

$$B\underline{x} + \underline{u} = A\underline{s} + \underline{v}$$

where $\underline{s} = [s_1,\ldots,s_l]^T$, A a matrix over k (thus effectuating a suitable k-linear combination of the multiplications), and $\underline{v}$ is a column-vector whose entries are linear functions in the x's and the y's (accomodating for the contributions of straight additions and scalar multiplications).

In order to reduce the complexity of the problem it would be nice if one could be more specific about the products $s_1,\ldots,s_l$ and conclude for instance that both operands in each multiplication are linear homogeneous expressions in the x's and the y's. WINOGRAD [23] needed a tedious argument to show that for computing a set of bilinear forms this may indeed be assumed without loss of generality. A much easier way to obtain this conclusion is to reduce both the task and the algorithm modulo the ideal I spanned by the third order terms in x's and y's, i.e.

$$I = (\ldots, x_i x_j x_k, \ldots, x_i x_j y_k, \ldots, x_i y_j y_k, \ldots, y_i y_j y_k, \ldots)$$

It is easy to see that constant terms where-ever they occur in an operand of a multiplication can be eliminated at the cost of inserting a few extra additive steps following each multiplication. Furthermore, in computing modulo I it makes no sense to multiply a linear term with a term of higher order since their product is a member of I. Therefore the operands in each multiplication may be assumed to be both homogeneously linear.

Note that in reducing the task $B.\underline{x} + \underline{u}$ modulo I no contribution from the product $B.\underline{x}$ vanishes since this is a homogeneous bilinear product. The same holds for $\underline{u}$ unless $\underline{u}$ contains terms of order ≥ 3.

PROPOSITION 2.1. *Each straight-line algorithm for computing the task* $B.\underline{x} + \underline{u}$ *over* $k \cup \{x_1,\ldots,x_n,y_1,\ldots,y_m\}$ *in* R/I *reduces to an equation*

$$B.\underline{x} + \underline{u} = A.\underline{s} + \underline{v} \qquad (\text{mod } I)$$

where $\underline{s}$ *is a column of products whose operands are homogeneously linear in* x's *and* y's, *where the entries in* A *belong to* k, *and where* $\underline{v}$ *consists of linear functions in* x's *and* y's.

The relevance of studying tasks and algorithms in R/I is clear from the following special case of the Sikulationssatz of STRASSEN [18].

LEMMA 2.2. *The minimal number of multiplications needed to compute* $B\underline{x} + \underline{u}$ *in* R *is* $\geq$ *the minimal number of multiplications needed to compute* $B\underline{x} + \underline{u}$ *in* R/I.

PROOF. Each algorithm in R is an algorithm in R/I. □

Since we need it later we give the following generalization of FIDUCCIA's row-rank lowerbound:

PROPOSITION 2.3. *Let* $\underline{u}$ *be a vector whose entries are polynomials in the* x's. *Then the minimal number of multiplications to compute* $B.\underline{x} + \underline{u}$ *over* $k \cup \{x_1,\ldots,x_n,y_1,\ldots,y_m\}$ *in* R/I *is* $\geq$ *the row rank of* B.

PROOF. Let the row rank of B equal q. We can assume wlog. that B contains exactly q rows. Assume that a straight-line algorithm for $B.\underline{x} + \underline{u}$ uses ℓ multiplications $s_1,\ldots,s_\ell$ where $\ell < q$. Then there exists an equation

$$B.\underline{x} + \underline{u} = A.\underline{s} + \underline{v} \qquad (\mathrm{mod}\ I).$$

Now A is an q by ℓ matrix with coefficients in k, and since $q > \ell$ there must be a q-vector $\underline{a} \neq \underline{0}$ with coefficients in k such that ${}^{t}\underline{a}.A = \underline{0}$. Hence:

$${}^{t}\underline{a}.B.\underline{x} + {}^{t}\underline{a}.\underline{u} = {}^{t}\underline{a}A.\underline{s} + {}^{t}\underline{a}.\underline{v} = {}^{t}\underline{a}.\underline{v}. \qquad (\mathrm{mod}\ I) \qquad (*).$$

Since rank (B) $\geq q > \ell$, the vector ${}^{t}\underline{a}.B$ contains some y's with non-zero coefficients. Consequently the left hand side of (*) must contain a contribution $y_i x_j$ which does not occur on the right hand side and which is also not absorbed in the ideal.
Contradiction. □

3. Consider the computation of a finite set of bilinear forms in R over $k \cup \{x_1,\ldots,x_n\} \cup \{y_1,\ldots,y_m\}$, formulated as a matrix-vector product

$$\begin{bmatrix} & & \\ & B & \\ & & \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

where the entries in B are linear in the y's.

A set of indeterminates $\{y_{i_1},\ldots,y_{i_r}\}$ is called *firm* in B when

- each y_{i_j} occurs in B
- replacing any set Γ of y_{i_j}'s by a k-linear combination of remaining y's cannot make any of the $\{y_{i_1},\ldots,y_{i_r}\} - \Gamma$ disappear entirely in B.

Then we give

DEFINITION. A matrix B is called *d-immune in* $\{y_{i_1},\ldots,y_{i_r}\}$ when the following conditions hold:

- $\{y_{i_1},\dots,y_{i_r}\}$ is firm in B
- the row-rank of B is always ≥ d independent of replacing all indeterminates $y_{i_1},\dots,y_{i_r}$ by an arbitrary k-linear combination of the remaining indeterminates in $\{y_1,\dots,y_m\}$.

The following matrix for example is 3-immune in $\{y_1\}$, but only 2-immune in $\{y_2\}$:

$$\begin{bmatrix} y_2 & 0 \\ y_3 & y_1 \\ 0 & y_2 - y_3 \end{bmatrix}$$

When B is d-immune for a set of indeterminates, then necessarily rank (B) ≥ d.

Our main theorem is based on the following crucial result:

<u>LEMMA 3.1</u>. *Let* B *be d-immune in* $\{y_{i_1},\dots,y_{i_r}\}$, *and let* $\underline{u}$ *be a vector consisting of polynomials in the* x's. *Then the minimal number of multiplications required in any straight-line program to compute* $B\underline{x} + \underline{u}$ *over* $k \cup \{x_1,\dots,x_n,y_1,\dots,y_m\}$ *in* R/I *is* ≥ d + r.

<u>PROOF</u>. The proof is based on induction in r.

For r = 0 the definition of immunity implies that rank (B) ≥ d and the result follows immediately from Fiduccia's criterion (proposition 2.3).

For r > 0 we are going to use the fact that in algorithms modulo I all operands in a multiplication are linear homogeneous expressions (proposition 2.1) Consider the indeterminate y_{i_r}. Since y_{i_r} occurs non-trivially in a product with some x in $B\underline{x} + \underline{u}$ there must be multiplication in the straight-line program for this task in which at least one of the operands contains y_{i_r} with non-zero coefficient:

$$(\alpha y_{i_r} + f + g) * h$$

where f, g, and h are linear homogeneous expressions in x's, in y's unequal to y_{i_r}, and in x's and y's respectively.

If we now make the substitution

$$y_{i_r} = -\frac{1}{\alpha} f - \frac{1}{\alpha} g$$

the operand is made 0, thus eliminating at least one multiplication from the program. It is not hard to verify that the form of the ideal I is left invariant under such a substitution, and consistently eliminating y_{i_r} a new straight-line program is obtained computing the task

$$B'\underline{x} + \underline{u}$$

still modulo I, where B' results from B by replacing y_{i_r} throughout by $-\frac{1}{\alpha} f - \frac{1}{\alpha} g$. Note that $\underline{u}$ has not changed since it is made from $\underline{x}$-expressions exclusively.

Collecting the x's and y's in B' in separate terms one can write

$$B'\underline{x} + \underline{u} = B''\underline{x} + B'''\underline{x} + \underline{u}$$

where the entries of B" are linear in the y's and the entries in B"' are linear in the x's exclusively (with B'=B"+B"').

It follows that we may write the new task as

$$B''\underline{x} + \underline{u}'$$

where B" is effectively obtained from the original matrix B by substituting $y_{i_r} = -\frac{1}{\alpha} g$ (that is, some linear combination of y's eliminating y_{i_r}) and $\underline{u}' = B'''\underline{x} + \underline{u}$ is some new residu consisting entirely of x-terms.

Now observe that by the assumptions on B the matrix B" must be d-immune in $\{y_{i_1},\ldots,y_{i_{r-1}}\}$. By induction hypothesis the minimal number of multiplications needed for $B''.\underline{x} + u'$ in R'/I' is $\geq d + (r-1)$, and therefore the original number of multiplications for $B.\underline{x} + \underline{u}$ in R/I cannot be less than $d + (r-1) + 1 = d + r$. □

The given proof is similar in spirit to WINOGRAD's proof [22] of the column-rank lowerbound. However his vector $\underline{u}$ consists of polynomials in the y's, and his elimination steps substitute for x's. Clearly if one substitutes for an x occurring in $\underline{u}$ the vector $\underline{u}$ may get filled with the mixed products which one tried to compute. This indicates why it is impossible to use the column-rank lowerbound at the basis of our induction argument.

One can show however that the mixed-rank lowerbound of FIDUCCIA [7] can be obtained in a similar fashion as lemma 3.1 by starting with his row-rank argument, and eliminating x's, using a vector $\underline{u}$ of polynomials in y's. (This is the reverse order of arguments as is used in [7]).

From 3.1, we immediately obtain

THEOREM 3.2. *The minimal number of multiplications needed to compute* $B\underline{x}$ *is greater than or equal to the maximal number of the form* $d + r$ *where* B *can be* d-*immune in* r y-*indeterminates.*

In the further sections of this paper we shall illustrate the use of 3.2 and its ease of application in a large number of usually wellknown examples.

We conclude this section by explaining the deeper meaning of performing a linear substitution $y_i = f$ where f is a homogeneous linear form in the x's and the remaining y's. From an algebraic point of view performing such a substitution means replacing the ring R by the ring $R/(y_i-f)$, respectively replacing the ring R/I by the ring $R/(I+(y_i-f))$. There exists however a natural isomorphism between $R/(y_i-f)$ and the ring $R' = k[x_1,\ldots,x_n,y_1,\ldots,y_{i-1},y_{i+1},\ldots,y_m]$ which is obtained after replacing y_i throughout by the expression f. If, moreover, I' is the image of $I/(y_i-f)$ under this isomorphism then $R/(I+(x_i-f))$ and R'/I' are again isomorphic. In our case, where I is the ideal spanned by the third order homogeneous terms, I' is the analogous ideal in R'; this shows that the shape of the ideal I is left invariant by the elimination. However if J is some ill-choosen ideal like e.g. $(\ldots,x_ix_j,\ldots,y_iy_j,\ldots)$ then J' may contain some mixed terms, showing that in general the form of an ideal is changed by an elimination step.

4. A first example of the use of rank-immunity concerns the task of

computing the product of two complex numbers $x_1 + x_2 i$ and $y_1 + y_2 i$. It is well-known that 3 multiplications suffice in computing the product.

PROPOSITION 4.1. (WINOGRAD [21]). *Computing the product of two complex numbers over a real field in* 3 *multiplications is optimal.*

PROOF. The task can be equivalently formulated as the computation of

$$\begin{bmatrix} y_1 & -y_2 \\ y_2 & y_1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \end{bmatrix} .$$

The matrix shown is easily seen to be 2-immune in $\{y_2\}$ since after replacing y_2 by some k-linear combination in the remaining variable we get

$$\underline{\text{rank}} \begin{bmatrix} y_1 & -\alpha y_1 \\ \alpha y_1 & y_1 \end{bmatrix} = \underline{\text{rank}} \begin{bmatrix} y_1 & 0 \\ \alpha y_1 & (1+\alpha^2) y_1 \end{bmatrix} = 2$$

for any $\alpha \in k$.

The product of two general quaternions $x_1 + x_2 i + x_3 j + x_4 k$ and $y_1 + y_2 i + y_3 j + y_4 k$ (see e.g. KUROSH [15]) is defined to be the quaternion $z_1 + z_2 i + z_3 j + z_4 k$ with

$$\begin{aligned} z_1 &= x_1y_1 - x_2y_2 - x_3y_3 - x_4y_4 \\ z_2 &= x_1y_2 + x_2y_1 + x_3y_4 - x_4y_3 \\ z_3 &= x_1y_3 - x_2y_4 + x_3y_1 + x_4y_2 \\ z_4 &= x_1y_4 + x_2y_3 - x_3y_2 + x_4y_1 \end{aligned}$$

It is known already for some time that one may do in less than 16 multiplications to compute the product. FIDUCCIA [8] showed that the task can be computed in only 10 multiplications, and LAFON [16] further reduced it to 9. Recently FISCHER, DE GROOTE & SCHÖNHAGE [9] and independently the present authors found a method that needs only 8 multiplications (but the method was in fact already contained in DOBKIN [5]).

Determine

$$\begin{aligned}
\mathrm{I} &= (x_1+x_2+x_3+x_4)(y_1+y_2+y_3+y_4)\\
\mathrm{II} &= (-x_1+x_2-x_3+x_4)(y_1-y_2+y_3-y_4)\\
\mathrm{III} &= (x_1+x_2-x_3-x_4)(y_1+y_2-y_3-y_4)\\
\mathrm{IV} &= (-x_1+x_2+x_3-x_4)(y_1-y_2-y_3+y_4)\\
\mathrm{V} &= x_1y_1\\
\mathrm{VI} &= x_2y_4\\
\mathrm{VII} &= x_3y_2\\
\mathrm{VIII} &= x_4y_3
\end{aligned}$$

A little bit of calculation shows that

$$\begin{aligned}
\mathrm{I} &= -z_1+z_2+z_3+z_4+2(\mathrm{V}+\mathrm{VI}+\mathrm{VII}+\mathrm{VIII})\\
\mathrm{II} &= z_1+z_2-z_3+z_4+2(-\mathrm{V}-\mathrm{VI}+\mathrm{VII}+\mathrm{VIII})\\
\mathrm{III} &= -z_1+z_2-z_3-z_4+2(\mathrm{V}-\mathrm{VI}-\mathrm{VII}+\mathrm{VIII})\\
\mathrm{IV} &= z_1+z_2+z_3-z_4+2(-\mathrm{V}+\mathrm{VI}-\mathrm{VII}+\mathrm{VIII})
\end{aligned}$$

and thus

$$\begin{bmatrix} -1 & 1 & 1 & 1\\ 1 & 1 & -1 & 1\\ -1 & 1 & -1 & -1\\ 1 & 1 & 1 & -1 \end{bmatrix} \begin{bmatrix} z_1\\ z_2\\ z_3\\ z_4 \end{bmatrix}$$

is obtained in only 8 multiplications. After inverting the (orthogonal) matrix involved each z_i is indeed expressed as rational combination of I,..., VIII and we achieved the task. A related algebraic principle shows that for instance Cayley-numbers (octaves) may be computed in only 30 real multiplications and there is a generalisation in arbitrary linear associative algebras.

With the help of 3.3 we can easily derive a lowerbound and obtain the following result due to FIDUCCIA [7], DOBKIN [5], and LAFON [16].

PROPOSITION 4.2. *The product of two quaternions over a real field requires at least 7 multiplications.*

PROOF. Formulate the task as a computation of

$$\begin{bmatrix} y_1 & -y_2 & -y_3 & -y_4 \\ y_2 & y_1 & y_4 & -y_3 \\ y_3 & -y_4 & y_1 & y_2 \\ y_4 & y_3 & -y_2 & y_1 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_3 \\ x_4 \end{bmatrix}$$

Since the determinant of

$$\begin{bmatrix} 1 & -\alpha & -\beta & -\gamma \\ \alpha & 1 & \gamma & -\beta \\ \beta & -\gamma & 1 & \alpha \\ \gamma & \beta & -\alpha & 1 \end{bmatrix}$$

is just the square of the norm of the quaternion $1 + \alpha i + \beta j + \gamma k$ $(\alpha,\beta,\gamma\epsilon k)$ and therefore never equal to 0, it follows that the matrix shown in the task is 4-immune in $\{y_2,y_3,y_4\}$ and thus we obtain from 3.3 indeed a lowerbound of 4 + 3 = 7 multiplications over a real field. □

In the same way one can derive a lowerbound of 15 multiplications for computing the product of two Cayley-numbers. DE GROOTE [3] and LAFON [17] have recently improved 4.2 to 8 multiplications and thus the given algorithm is in fact optimal.

In section 6 we shall prove an ultimate generalisation of 4.1 and 4.2 which applies to arbitrary finite dimensional algebras.

5. An n × n matrix A is called a Toeplitz-matrix when for all $2 \leq i, j \leq n$: $A[i,j] = A[i-1,j-1]$.

PROPOSITION 5.1. (AHO-HOPCROFT-ULLMAN [1], ex.12.6) *Computing the product of an* n × n *Toeplitz matrix and a vector requires at least* 2n - 1 *multiplications.*

PROOF. The task is to compute

$$B\underline{x}$$

where B is the matrix:

$$\begin{bmatrix} y_1 & y_{n+1} & \cdots & y_{2n-1} \\ y_2 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & y_{n+1} \\ y_n & & y_2 & y_1 \end{bmatrix}$$

B is obviously n-immune in $\{y_{n+1},\ldots,y_{2n-1}\}$, and therefore $B\underline{x}$ requires $n + (n-1) = 2n-1$ multiplications. □

To multiply a symmetric, tridiagonal n × n-matrix and a vector in the normal way requires 3n - 2 multiplications:

$$\begin{bmatrix} y_1 & z_1 & & & \\ z_1 & y_2 & z_2 & & \\ & z_2 & y_3 & \ddots & \\ & & \ddots & \ddots & z_{n-1} \\ & & & z_{n-1} & y_n \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

This bound can not be optimal since for n = 2 already one can do in 3 (rather than in 4) multiplications:

$$x_1y_1 + x_2z_1 = \tfrac{1}{2}(x_1+x_2)(y_1+z_1) + \tfrac{1}{2}(x_1-x_2)(y_1-z_1)$$
$$x_1z_1 + x_2y_2 = \tfrac{1}{2}(x_1+x_2)(y_1+z_1) - \tfrac{1}{2}(x_1-x_2)(y_1-z_1) - x_2(y_1-y_2)$$

For $n > 2$ once may distinguish appropriately located 2×2 sub-matrices along the main diagonal and show in a straightforward way that one can compute the present matrix-vector product in only $[\frac{5}{2} n] - 2$ multiplications.

With the help of 3.3 we can prove a general lowerbound which shows at least that the given method in the 2×2-case must be optimal.

PROPOSITION 5.2. *The product of a symmetric, tridiagonal* $n \times n$-*matrix and a vector requires at least* $2n - 1$ *multiplications.*

PROOF. It is a straightforward verification that the matrix of the task shown above is n-immune in $\{z_1,\ldots,z_{n-1}\}$. □

To get 5.2 from the theorems of Winograd and Fiduccia needs a transformation first. With exactly the same argument one can show that computing

$$\begin{bmatrix} y_1 & -z_1 & & & \\ z_1 & y_2 & -z_2 & & \\ & z_2 & y_3 & \ddots & \\ & & \ddots & \ddots & -z_{n-1} \\ & & & z_{n-1} & y_n \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ \vdots \\ x_n \end{bmatrix}$$

requires at least 2n - 1 multiplications.

PROPOSITION 5.3. *Computing the product of two* n × n *matrices requires at least* $2n^2 - n$ *multiplications.*

PROOF. The task of computing $[y_{ij}] * [x_{ij}]$ can be equivalently formulated as the task of computing

$$\left[\begin{array}{ccc:ccc:c:ccc} y_{11} & \cdots & y_{1n} & & & & & & & \\ \vdots & & & & & & & & & \\ y_{n1} & \cdots & y_{nn} & & & & & & & \\ \hdashline & & & y_{11} & \cdots & & & & & \\ & & & \vdots & & & & & & \\ & & & y_{n1} & \cdots & & & & & \\ \hdashline & & & & & & \ddots & & & \\ \hdashline & & & & & & & y_{11} & \cdots & y_{1n} \\ & & & & & & & \vdots & & \vdots \\ & & & & & & & y_{n1} & \cdots & y_{nn} \end{array}\right] \begin{bmatrix} x_{11} \\ x_{21} \\ \vdots \\ x_{n1} \\ x_{12} \\ \vdots \\ x_{n2} \\ \vdots \\ x_{1n} \\ \vdots \\ x_{nn} \end{bmatrix}$$

The matrix shown is easily seen to be n^2-immune in $\{y_{12},\ldots,y_{1n},y_{22},\ldots,y_{2n},\ldots,y_{n2},\ldots,y_{nn}\}$ (which are n^2-n indeterminates). The result then follows from 3.2. □

The criteria in for instance FIDUCCIA [7] do not give a better bound than n^2, and thus 3.3 really enables us to do more. By an analogous argument it can be shown that the product of $k \times \ell$ and $\ell \times m$ matrices requires at least $\max\{k(\ell+m-1),\ell(k+m-1),m(k+\ell-1)\}$ thereby using the symmetry-theorem of STRASSEN [21] and HOPCROFT & MUSINSKI [14].

In 5.3 is also clear that the argument based on an embedding in R/I is not as powerful as the estimates based on tensor-rank. Even in the case of 2 × 2 matrices 5.3 gives a lowerbound of 6 multiplications instead of 7. In fact, the proof-technique of 5.3 simplifies Winograd's argument for optimality of 7 multiplications [23], but one has to apply some transformations first before the arguments apply.

We conclude this section with three more examples of a somewhat more special form.

PROPOSITION 5.4. *Computing the product of two* 2 × 2 *matrices one of which is triangular in* 6 *multiplications is optimal.*

PROOF. Since

$$\begin{bmatrix} y_1 & y_3 \\ y_2 & y_4 \end{bmatrix} \begin{bmatrix} x_1 & 0 \\ x_2 & x_4 \end{bmatrix} = \begin{bmatrix} x_1y_1 + x_2y_3 & x_4y_3 \\ x_1y_2 + x_2y_4 & x_4y_4 \end{bmatrix}$$

6 multiplications suffice.

Formulate the task as a computation of

$$\begin{bmatrix} y_1 & y_3 & 0 \\ y_2 & y_4 & 0 \\ 0 & 0 & y_3 \\ 0 & 0 & y_4 \end{bmatrix} \begin{bmatrix} x_1 \\ x_2 \\ x_4 \end{bmatrix},$$

and observe that the matrix shown is 4-immune in $\{y_1,y_2\}$. Thus 6 multiplications are also minimally required. □

PROPOSITION 5.5. *A computation of* x_1y_1 *and* $x_1y_i + x_iy_1$ *for* $1 < i \leq k$ *in* $2k - 1$ *multiplications is optimal.*

PROOF. It is straightforward to see that $2k - 1$ multiplications suffice. To conclude optimality we first formulate the task as a computation of

$$\begin{bmatrix} y_1 & & & \\ y_2 & y_1 & & \\ \vdots & & \ddots & \\ y_k & & & y_1 \end{bmatrix} \qquad \begin{bmatrix} x_1 \\ \vdots \\ x_k \end{bmatrix}$$

The matrix shown is k-immune in $\{y_2,\ldots,y_k\}$ and it follows that $k + (k-1) = 2k - 1$ indeed also is a lowerbound on the number of multiplications required. □

As a last example we prove that 3.2 immediately yields a lemma of HOPCROFT & KERR [13], appearing as a ★-exercise in AHO-HOPCROFT-ULLMAN [1].

PROPOSITION 5.6. *A computation of* x_iy_i *and* $u_ix_i + v_iy_i$ *for* $1 \leq i \leq k$ *in* $3k$ *multiplications is optimal.*

PROOF. The task is to compute

$$\left[\begin{array}{ccc|ccc} y_1 & & & & & \\ & \ddots & & & & \\ & & y_k & & & \\ \hline u_1 & & & y_1 & & \\ & \ddots & & & \ddots & \\ & & u_k & & & y_k \end{array}\right] \left[\begin{array}{c} x_1 \\ \vdots \\ x_k \\ \hline v_1 \\ \vdots \\ v_k \end{array}\right]$$

The matrix shown is 2k-immune in $\{u_1,\ldots,u_k\}$, and the result follows. □

(In HOPCROFT & KERR [13] only the non-commutative version of 5.5 was shown).

6. In [7] FIDUCCIA considers linear algebras which are not necessarily commutative or associative. Such an algebra is a finite dimensional vector space on which a bilinear multiplication is defined. Selecting a base $e_1,\ldots,e_n$ the multiplication is described by the so-called structural constants γ_{ijk} satisfying $e_i.e_j = \sum \gamma_{ijk}.e_k$.

In the matrix-times-vector terminology the task of multiplying two elements in the algebra is described by $B.\underline{x}$ where

$$B = \begin{array}{r c} & k \\ i- & \left[\begin{array}{c} \vdots \\ \cdots\sum_j \gamma_{ijk} y_j \cdots \\ \vdots \end{array}\right] \end{array} \quad \text{and} \quad \underline{x} = \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

According to STRASSEN [21] the multiplication-complexity of this algebra equals the minimal rank of a third order tensor which is the sum of the tensor formed by the structural constants, and a tensor of the same size which is anti-symmetric in i and j.

FIDUCCIA [7] conjectured that in the case that the algebra is zero-divisor free at least 2n-1 multiplications are required. This conjecture has been verified for the complex numbers, the quaternions and the octaves. Together with the reals themselves this list exhaust all possible examples of alternative zero-divisor free real algebras, as follows from a theorem of FROBENIUS [11], and its generalization [see 15]. Therefore the conjecture only makes sense for rather uncommon algebras.

<u>PROPOSITION 6.1</u>. *Multiplication of two elements in an* n*-dimensional zero-divisor free algebra takes at least* 2n-1 *multiplications.*

<u>PROOF</u>. We claim that the matrix

$$B = \begin{bmatrix} \vdots \\ \cdots\sum_j \gamma_{ijk} y_j \cdots \\ \vdots \end{bmatrix}$$

is n-immune in $\{y_1,\ldots,y_n\}\backslash\{y_\ell\}$ for each ℓ. Indeed substituting linear multiples of y_ℓ for the y_i with $i \neq \ell$ one obtains a matrix B' consisting of entries of the form $\sum_j \gamma_{ijk}\lambda_j y_\ell$ where $\lambda_\ell = \ell$.

Suppose that this matrix has row-rank < n. Then there exists a non-zero row-vector $(\alpha_1,\ldots,\alpha_n)$ such that in $(\alpha_1,\ldots,\alpha_n)$ B' y_ℓ does no longer occur. This implies that:

$$\sum_i \alpha_i \sum_j \lambda_j \gamma_{ijk} = 0 \qquad \text{for each } k \text{ and therefore}$$

$$\sum_k \sum_i \alpha_i \cdot \sum_j \lambda_j \gamma_{ijk} \cdot e_k = \sum_i \alpha_i \cdot \sum_j \lambda_j \sum_k \gamma_{ijk} \cdot e_k =$$

$$\sum_i \alpha_i \sum \lambda_j \cdot (e_i \cdot e_j) = (\sum_i \alpha_i e_i) \cdot (\sum \lambda_j e_j) = 0.$$

This contradicts the fact that the algebra is zero-divisor free.

Note that we have not checked that the set $\{y_1,\ldots,y_n\}\backslash\{y_\ell\}$ is firm in the matrix. However assuming that an y_i can be made to vanish by a linear substitution for other indeterminates, then the above immunity argument must fail for the set $\{y_1,\ldots,y_n\}\backslash\{y_i\}$, since the substitution $y_j = 0$ for $j \neq i$ would make the complete matrix disappear. □

REFERENCES

[1] AHO, A.V., J.E. HOPCROFT, & J.D. ULLMAN, *The design and analysis of computer algorithms*, Addison, Wesley, Reading, Mass. (1974).

[2] BROCKETT, R.W., & D. DOBKIN, *On the optimal evaluation of a set of bilinear forms*, Proc. 5th Ann. ACM Symp. Theory of Computing, Austin (1973), 88-95.

[3] DE GROOTE, H.F., *The computational complexity of quaternion-multiplication*, Math. Inst. der Universität Tübingen (1975), (submitted to SIAM J. Computing).

[4] DOBKIN, D., *On the optimal evaluation of a set of N-linear forms*, Conference Record 14th Ann. Symp. on Switching & Automata Theory, Iowa City (1973), 92-102.

[5] DOBKIN, D., *On the complexity of a class of arithmetic computations*, Ph.D. thesis, Harvard Univ. (1973).

[6] DOBKIN, D.; *Private communication*, Kaiserslautern (1975).

[7] FIDUCCIA, C.M., *On the algebraic complexity of matrix multiplication*, Ph.D. thesis, Brown Univ. (1973).

[8] FIDUCCIA, C.M., *On obtaining upper-bounds on the complexity of matrix multiplication, in:* R. Miller & J.W. Thatcher (ed.), *Complexity of computer computations*, Plenum Press, New York (1972).

[9] FISCHER, M.J., H.F. DE GROOTE, & A. SCHÖNHAGE, *On quaternion-multiplication*, preprint (1975).

[10] FISCHER, M.J., *Private communication*, Kaiserslautern (1975).

[11] FROBENIUS, F.G., *Über lineaire Substitutionen und bilineare Formen.* J. Reine Angew. Math. 84 (1878) 1-63. Also in J.P. Serve (ed.), *Gesamelte Abhandlungen, Vol. 1*, pp. 343-405, Springer Berlin 1968.

[12] HENRICI, P., *Applied and computational complex analysis* (I), Wiley-Interscience, New York (1974).

[13] HOPCROFT, J.E., & L.R. KERR, *On minimizing the number of multiplications necessary for matrix multiplication*, SIAM J. Appl. Math. 20 (1971), 30-36.

[14] HOPCROFT, J.E. & J. MUSINSKI, *Duality applied to the complexity of matrix multiplication and other bilinear forms*, Proc. 5th Ann. ACM Symp. Theory of Computing, Austin (1973), 73-87.

[15] KUROSH, A.G., *Lectures on general algebra*, Chelsea Publ. Cy., New York (1963).

[16] LAFON, J.C., *Sur le produit de deux quaternions*, Comptes Rendus Acad. Sci. Paris, Ser. A t 280 (10 Mars 1975), 665-668.

[17] LAFON, J.C., *Complexity of the product of two quaternions*, Université Sc. & Med. de Grenoble, preprint (1975).

[18] OSTROWSKI, A.M., *On two problems in abstract algebra connected with Horner's rule*, in: *Studies in Mathematics and Mechanics presented to R. von Mises*, Acad. Press, New York (1954), 40-48.

[19] STRASSEN, V., *Berechnung und programm* (I), Acta Informatica 1 (1972), 320-335.

[20] STRASSEN, V., *Berechnung und programm* (II), Acta Informatica 2 (1973), 64-79.

[21] STRASSEN, V., *Vermeidung von Divisionen*, J. Reine Angew. Math. 264 (1973), 184-202.

[22] WINOGRAD, S., *On the number of multiplications necessary to compute certain functions*, Comm. Pure Appl. Math 23 (1970), 165-179.

[23] WINOGRAD, S., *On the multiplication of 2 by 2 matrices*, J. Linear Algebra and Appl 4 (1971), 381-388.