On the Maximal Multiplicative Complexity of a Family of Bilinear Forms

M. D. Atkinson and N. M. Stephens
Department of Computing Mathematics
University College
Cardiff, U.K.

Submitted by F. Robert

ABSTRACT

The number of nonscalar multiplications required to evaluate a general family of bilinear forms is investigated. An upper bound is obtained which is about half that obtained from naive arguments. In certain cases the best possible upper bound is obtained.

0. INTRODUCTION

In this paper we study a well-known problem in the theory of algebraic computational complexity: the computation of a family of bilinear forms

$$\sum_{i,j} \alpha_{ijk} x_i y_j, \qquad k = 1,2,\ldots,p, \tag{1}$$

in noncommuting variables $x_1,\ldots,x_m,y_1,\ldots,y_n$. This problem has been much studied recently, partly perhaps because the model of computation which is usually taken is simpler than such models often are. In this model the only operations which are counted are those multiplications in which neither of the factors is a constant (i.e., independent of $x_1,\ldots,x_m,y_1,\ldots,y_n$). We refer the reader to [4, 7, 9] for the defence of this model and some extensive background material, and recall only that the problem and the model were originally suggested by the Strassen matrix multiplication algorithm.

The simplicity of the model has allowed some elegant characterizations of the minimal cost ν associated with the computation of (1). One such [8, 10] is that ν is the minimal number such that there exist constants a_{is}, b_{js}, c_{ks} with $\alpha_{ijk} = \sum_{s=1}^{\nu} a_{is} b_{js} c_{ks}$ for all relevant i,j,k. Because of an analogy with

 0024-3795/79/050001+8$01.75

matrices, ν is called the rank of the tensor (α_{ijk}). From this characterization follows the well-known principle of duality: that the families of bilinear forms defined by permuting the roles of the suffices i,j,k in (1) all have the same minimal cost.

Another interpretation [4, 9] is that ν is the minimal number of rank 1 matrices whose span contains the $m \times n$ matrices $A_1,\ldots,A_p$, where by definition the (i,j) entry of A_k is α_{ijk}. Although duality is hidden in this formulation, it is more convenient for our purposes. Accordingly, throughout this paper we shall consider families of bilinear forms to be specified by $m \times n$ matrices $A_1,\ldots,A_p$, and we shall be concerned with finding a set of rank 1 matrices whose span contains $A_1,\ldots,A_p$. We shall work over the field $\mathbf{C}$ of complex numbers, although many of our techniques carry over to other fields. It is evident (and well known) that $\nu = \nu(A_1,\ldots,A_p)$ is unaltered if $A_1,\ldots,A_p$ are replaced by another spanning set for $\langle A_1,\ldots,A_p\rangle$. Also well known is that ν is unaltered if row and column operations are simultaneously performed on $A_1,\ldots,A_p$, and we shall make frequent use of these two facts without much further comment.

Of course, for fixed m,n,p, $\nu(A_1,\ldots,A_p)$ depends on $A_1,\ldots,A_p$, and it is natural therefore to define (following Dobkin in [6]) $r(m,n,p)$ as the maximal value of $\nu(A_1,\ldots,A_p)$ over all families of p $m \times n$ matrices. In other words $r(m,n,p)$ is the maximum rank attainable by an $m \times n \times p$ tensor. It is with $r(m,n,p)$ that this paper is concerned. Some known properties of $r(m,n,p)$ which put our own results into perspective are:

(i) $r(m,n,p)$ is symmetric in m,n,p [6],
(ii) $r(m,n,p) \leqslant \min(mn,np,pm)$ [4],
(iii) if $p \geqslant mn$, then $r(m,n,p) = mn$ [6],
(iv) $r(m,n,1) = \min(m,n)$ (trivial),
(v) $r(m,n,2) = \min(2m, 2n, m + \lfloor n/2 \rfloor, n + \lfloor m/2 \rfloor)$ [1],
(vi) $r(n,n,3) \leqslant 2n$ [5],
(vii) $r(m,n,p) \geqslant mnp/(m+n+p-2)$ [3].

Our first result is

THEOREM 1. *If $m \leqslant n$, then $r(m,n,p) \leqslant m + \lfloor p/2 \rfloor n$.*

We note first that this implies (vi). However, it is more instructive to compare it with (ii) and (vii) in the case that $m = n = p$. Clearly (ii) yields $r(n,n,n) \leqslant n^2$, whilst our theorem and (vii) give

$$n^2/3 \leqslant r(n,n,n) \leqslant n^2/2 + O(n).$$

It is an intriguing and apparently difficult problem to tighten either of these bounds significantly.

A negative aspect of the theorem is that it is useless for values m,n,p in which $m \leqslant p/2$, since (ii) then provides a better bound. Of course for much larger values of p, $p \geqslant mn$, (iii) determines the exact value of $r(m,n,p)$. This suggests the study of values p which are just less than mn, and that is the topic of our second theorem.

THEOREM 2. *If* $k \leqslant \min(m,n)$, *then* $r(m,n,mn-k) = mn - k^2 + r(k,k,k^2 - k)$.

This result suggests that the values of $r(k,k,k^2-k)$ should be investigated. It is trivial that $r(1,1,0)=0$, and quite well known that $r(2,2,2)=3$. We have proved [2], by calculations which would take us too far afield to reproduce here, that $r(3,3,6)=7$ and $r(4,4,12)=14$. Thus, as consequences of Theorem 2, we have

1. $r(m,n,mn-1) = mn-1$ if $m,n \geqslant 1$,
2. $r(m,n,mn-2) = mn-1$ if $m,n \geqslant 2$,
3. $r(m,n,mn-3) = mn-2$ if $m,n \geqslant 3$,
4. $r(m,n,mn-4) = mn-2$ if $m,n \geqslant 4$.

These results encourage one to believe that $r(m,n,mn-k) = mn - \lceil k/2 \rceil$ if $m,n \geqslant k$. We have not been able to prove this, although Mrs. S. Lloyd (unpublished) has shown that $r(m,n,mn-k) \geqslant mn - \lceil k/2 \rceil$. So far as we know it had not previously been observed that $p < mn$ implies $r(m,n,p) < mn$ —i.e., in (iii) above the condition $p \geqslant mn$ cannot be weakened.

1. PROOF OF THEOREM 1

Throughout this section we shall assume that $m \leqslant n$.

LEMMA 1. *If* $p(\lambda), q(\lambda)$ *are polynomials in* λ *with complex coefficients and if, for all values of* x, *the polynomial* $p(\lambda) + xq(\lambda)$ *has a repeated factor, then* $q(\lambda)$ *also has a repeated factor.*

Proof. We let F be the field of rational functions in an indeterminate x over $\mathbf{C}$ and consider $f(\lambda) = p(\lambda) + xq(\lambda)$ to be a polynomial with coefficients in F.

We prove first that f and $df/d\lambda$ are not coprime as polynomials in $F[\lambda]$. If they were, we could write

$$af + b\frac{df}{d\lambda} = 1$$

for some polynomials $a, b \in F[\lambda]$. Then we could substitute some value x_0 for x which was not a pole of any coefficient of a or b, and we could deduce that $p(\lambda) + x_0 q(\lambda)$ was coprime to its derivative and so did not have a repeated factor—a contradiction.

Thus we may deduce that $f(\lambda) = r(\lambda)^2 s(\lambda)$ for some polynomials $r(\lambda)$, $s(\lambda)$ in $F[\lambda]$, with $r(\lambda)$ nontrivial. But now, differentiating with respect to x, we have that $r(\lambda)$ divides $q(\lambda)$ and so has coefficients in $\mathbf{C}$. It is now easy to see that $r(\lambda)^2$ divides $q(\lambda)$, completing the proof. ■

LEMMA 2. *Let* $S = \{1, 2, \ldots, m\}$, $m \geqslant 0$, *and let* $\{a_I(\lambda)\}$ *be a family of* 2^m *polynomials with complex coefficients indexed by the subsets* I *of* S. *Let* $f(x_1, \ldots, x_m, \lambda) = \sum_I a_I(\lambda) \prod_{i \in I} x_i$, *and assume that* $a_S(\lambda)$, *the coefficient of* $x_1 x_2 \cdots x_m$, *has no repeated roots. Then there exist values for* $x_1, \ldots, x_m$ *such that* $f(x_1, \ldots, x_m, \lambda)$ *has no repeated roots.*

Proof. We use induction on the size m of S, the case $m = 0$ being trivial. So assume that $m > 0$ and that the lemma has been established for smaller values than m. Let $S' = S - \{x_m\}$, and write

$$f(x_1, \ldots, x_m, \lambda) = \sum_{I \subseteq S'} a_I(\lambda) \prod_{i \in I} x_i + x_m \sum_{\substack{I \subseteq S \\ m \in I}} a_I(\lambda) \prod_{i \in I - \{x_m\}} x_i$$

$$= p(\lambda) + x_m q(\lambda), \quad \text{say,}$$

where

$$q(\lambda) = \sum_{\substack{I \subseteq S \\ m \in I}} a_I(\lambda) \prod_{i \in I - \{x_m\}} x_i.$$

Now $q(\lambda)$ has the same general form as $f(x_1, \ldots, x_m, \lambda)$ except that it only involves $x_1, \ldots, x_{m-1}$; moreover the coefficient of $x_1 x_2 \ldots x_{m-1}$ is $a_S(\lambda)$, which has no repeated roots. The inductive hypothesis now allows us to choose values for $x_1, \ldots, x_{m-1}$ so that $q(\lambda)$ has no repeated roots. Then Lemma 1 allows x_m to be chosen so that $p(\lambda) + x_m q(\lambda) = f(x_1, \ldots, x_m, \lambda)$ has no repeated roots. ■

LEMMA 3. *If X, Y are any two $m \times m$ matrices, then there exist two diagonal matrices J, K such that*

(i) *$X+J$ is nonsingular,*
(ii) *$|\lambda(X+J)-(Y+K)|$ has m distinct roots as a polynomial in λ.*

(Here and in the sequel the notation $|A|$ denotes the determinant of the matrix A.)

Proof. To satisfy (i) we simply take $J = -\alpha I$, where α is not an eigenvalue of X. To satisfy (ii), consider an arbitrary diagonal matrix K with diagonal entries $x_1, \ldots, x_m$ and expand the determinant $|\lambda(X+J)-(Y+K)|$. This gives a polynomial of degree m in λ which has the form which featured in Lemma 2; moreover, the coefficient of $x_1 x_2 \cdots x_m$ is 1, a polynomial without repeated roots. Consequently Lemma 2 guarantees a choice of values for $x_1, \ldots, x_m$ such that K satisfies (ii). ∎

LEMMA 4. *If X, Y are $m \times m$ matrices such that*

(i) *X is nonsingular,*
(ii) *the polynomial $|\lambda X - Y|$ has m distinct roots,*

then, for any $m \times (n-m)$ matrices U, V, the multiplicative complexity $\nu(A,B)$ of the two $m \times n$ matrices $A = (X\ U)$, $B = (Y\ V)$ is at most n.

Proof.

$$\begin{aligned}
\nu(A,B) &= \nu(X^{-1}A, X^{-1}B), \quad \text{since row operations do not affect } \nu \\
&= \nu((I\ S),(X^{-1}Y\ T)), \quad \text{where } S = X^{-1}U,\ T = X^{-1}V \\
&= \nu((I\ 0),(X^{-1}Y\ R)) \quad \text{by column operations which reduce } S \text{ to } 0 \\
&\leqslant \nu(I, X^{-1}Y) + \nu(0,R) \\
&\leqslant m + (n-m), \quad \text{since, by (ii), } X^{-1}Y \text{ is diagonalizable.}
\end{aligned}$$

∎

Completion of proof. Consider any family of p $m \times n$ matrices. If p is odd, we shall assume that one of the matrices, C say, has been brought, by row and column operations, to a form in which the only nonzero entries are on the first main diagonal. We then consider the remaining matrices in $(p-1)/2$ pairs, whilst if p is even we consider the p matrices in $p/2$ pairs.

Let $M_1, \ldots, M_m$ be the $m \times n$ rank 1 matrices $E_{11}, E_{22}, \ldots, E_{mm}$, so that, in the case that p is odd, $C \in \langle M_1, \ldots, M_m \rangle$. We shall show that for each A, B, a typical one of the $\lfloor p/2 \rfloor$ pairs, it suffices to take along with $M_1, \ldots, M_m$ only n further rank 1 matrices to obtain a set whose span contains A, B. The theorem follows immediately from this.

Let $A=(X\ U)$, $B=(Y\ V)$, where X, Y are $m\times m$ matrices. According to Lemma 3 there exist two $m\times m$ diagonal matrices J, K such that

$$(X\ U)+(J\ 0) \quad \text{and} \quad (Y\ V)+(K\ 0)$$

satisfy the conditions of Lemma 4. These two matrices are therefore in the span of n rank 1 matrices $N_1,\ldots,N_n$, and since $(J\ 0),(K\ 0)\in\langle M_1,\ldots,M_m\rangle$, we have that A, B are in the span of $M_1,\ldots,M_m,N_1,\ldots,N_n$, as required. ■

By similar arguments to those above it can be shown that $r(n,n,3)\leqslant 2n-1$ and $r(n,n+1,3)\leqslant 2n$. The precise value of $r(n,n,3)$ seems difficult to determine, although it is known that $\lfloor 7n/4\rfloor \leqslant r(n,n,3)$, a result which determines $r(n,n,3)$ for $n\leqslant 4$. These facts, together with the consequences of Theorem 2 and some small calculations, are sufficient to specify all the values of $r(3,3,p)$ except for $p=5$:

p	1	2	3	4	6	7	8	9
$r(3,3,p)$	3	4	5	6	7	8	8	9

It seems surprisingly hard to decide whether $r(3,3,5)=6$ or 7.

2. PROOF OF THEOREM 2

LEMMA 5. *Let $Y_1,\ldots,Y_s$ be subspaces, with the same dimension, of a vector space V. Then there exists a subspace Z such that $V=Y_i\oplus Z$, $i=1,2,\ldots,s$.*

Proof. We prove first that V is not the union of a finite number of proper subspaces. For suppose that $M_1,\ldots,M_t$ are proper subspaces of V and that $V=\bigcup_i M_i$. We may assume that this union is irredundant and choose $x\in M_1$ with $x\notin\bigcup_{i>1}M_i$. We also choose $y\notin M_1$. Then none of $x+y$, $2x+y, 3x+y,\ldots$ are in M_1, and so all belong to $\bigcup_{i>1}M_i$; but then two of them must belong to some M_k, $k>1$, and so $x\in M_k$, a contradiction.

We now argue by induction on the (common) codimension of the Y_i. The lemma is clearly true if all $Y_i=V$. As inductive hypotheses we assume that the Y_i are proper subspaces and that the lemma has been established for subspaces of smaller codimension than the Y_i. Since $\bigcup_i Y_i\neq V$, there exists some vector v which is not in any Y_i. Then the subspaces $Y_i\oplus\langle v\rangle$ all have equal codimension smaller than the Y_i, and the result now follows from the inductive hypotheses. ■

We obtain Theorem 2 as a consequence of the following slightly more general result.

PROPOSITION. *If* $k \leqslant n$, *then* $r(m,n,mn-k) = m(n-k) + r(m,k,mk-k)$.

Proof. To show that $r(m,n,mn-k) \leqslant m(n-k)+r(m,k,mk-k)$, consider an arbitrary set of $mn-k$ $m\times n$ matrices, and let $\mathfrak{X}$ be the space they generate. Clearly, there is no loss in generality in assuming that $\mathfrak{X}$ has dimension $mn-k$. For each $i=1,2,\ldots,m$ let $\mathfrak{Y}_i$ be the space of all $m\times n$ matrices whose only entries are in the ith row. Since

$$\dim(\mathfrak{X}\cap\mathfrak{Y}_i) = \dim(\mathfrak{X}) + \dim(\mathfrak{Y}_i) - \dim(\mathfrak{X}+\mathfrak{Y}_i)$$

$$\geqslant mn-k+n-mn = n-k,$$

it follows that $\mathfrak{X}\cap\mathfrak{Y}_i$ contains $n-k$ linearly independent matrices $B_1^{(i)},\ldots,B_{n-k}^{(i)}$ where each $B_j^{(i)}$ has nonzero entries only in its ith row, a row vector $b_j^{(i)}$.

Clearly $\{B_j^{(i)} | i=1,\ldots,m,\ j=1,\ldots,n-k\}$ is a set of linearly independent rank 1 matrices. We choose $mn-k-m(n-k)=mk-k$ matrices $Z_1,Z_2,\ldots$ which complete this set to a basis of $\mathfrak{X}$.

For each $i=1,2,\ldots,m$ let V_i be the subspace of n-dimensional row space V generated by $b_1^{(i)},\ldots,b_{n-k}^{(i)}$. By Lemma 5 there exist vectors $u_1,\ldots,u_k$ such that $U=\langle u_1,\ldots,u_k\rangle$ is a direct complement in V for each of the subspaces $V_1,\ldots,V_m$. Hence, for any row vector v and any fixed i, there is a linear combination of the form $v+\sum_j \alpha_j b_j^{(i)}$ which belongs to U. Consequently, for each matrix Z_r there is some matrix Z_r^* of the form $Z_r^* = Z_r + \sum_{i,j}\beta_{ijr}B_j^{(i)}$, all of whose rows are in U. These $mk-k$ matrices Z_r^* also complete the set $\{B_j^{(i)}\}_{i,j}$ to a basis of $\mathfrak{X}$.

Now let G be some nonsingular $n\times n$ matrix whose last $n-k$ columns are a basis for the orthogonal complement of U. Then

$$\nu(Z_1^*,\ldots,Z_{mk-k}^*) = \nu(Z_1^*G,\ldots,Z_{mk-k}^*G) \leqslant r(m,k,mk-k),$$

since each Z_r^*G is an $m\times n$ matrix whose last $n-k$ columns are zero. It follows that there exist $m(n-k)+r(m,k,mk-k)$ rank 1 matrices whose span contains $\mathfrak{X}$, and this completes the first half of the proof.

Finally we show that $r(m,n,mn-k)\geqslant m(n-k)+r(m,k,mk-k)$. Let $A_1,\ldots,A_{mk-k}$ be a system of $m\times k$ matrices of maximal complexity $r(m,k,mk-k)$. Then it follows from [4] that the set

$$\{(A_i 0)\}_{i=1}^{mk-k} \cup \{E_{ij} | i=1,\ldots,m,\ j=k+1,\ldots,n\}$$

is a family of $mn-k$ $m\times n$ matrices of complexity $m(n-k)+r(m,k,mk-k)$. ∎

With this proposition the derivation of Theorem 2 [with $k \leqslant \min(m,n)$] is as follows:

$$\begin{aligned} r(m,n,mn-k) &= m(n-k) + r(m,k,mk-k) \\ &= m(n-k) + r(k,m,mk-k) \\ &= m(n-k) + k(m-k) + r(k,k,k^2-k) \\ &= mn - k^2 + r(k,k,k^2-k). \end{aligned}$$

REFERENCES

1 M. D. Atkinson and N. M. Stephens, The multiplicative complexity of two bilinear forms, in preparation.

2 M. D. Atkinson and N. M. Stephens, On the maximal rank of some special three-tensors, unpublished, Cardiff Univ., 1977.

3 R. W. Brockett, On the generic degree of a 3-tensor, unpublished typescript, Harvard Univ., 1976.

4 R. W. Brockett and D. Dobkin, On the optimal evaluation of a set of bilinear forms, in *Proceedings of the 5th Annual ACM Symposium on the Theory of Computing*, 1973, pp. 88–95.

5 D. Dobkin, On the complexity of a class of arithmetic computations, Ph.D. Thesis, Harvard Univ., Sept. 1973.

6 D. Dobkin, On the optimal evaluation of a set of n-linear forms, in *Conference Record, 14th Annual Symposium on Switching and Automata Theory*, Iowa City, 1973, pp. 92–102.

7 C. M. Fiduccia and Y. Zalcstein, Algebras having linear multiplicative complexities, *J. Assoc. Comput. Mach.* 24:311–331 (1977).

8 N. Gastinel, Le rang tensoriel d'un ensemble de matrices, Seminaire d'Analyse Numerique de l'Universite de Grenoble, No. 159, 1972.

9 J. C. Lafon, Optimum computation of p bilinear forms, *Linear Algebra and Appl.* 10:225–260 (1975).

10 V. Strassen, Vermeidung von Divisionen, *J. Reine Angew. Math.* 264:184–202 (1973).

Received March 1978