MATHEMATICAL SYSTEMS THEORY 10, 169–180 (1977)

Some Bilinear Forms Whose Multiplicative Complexity Depends on the Field of Constants

by

S. WINOGRAD

IBM Thomas J. Watson Research Center
Yorktown Heights, New York

ABSTRACT

In this paper we consider the system of bilinear forms which are defined by a product of two polynomials modulo a third P. We show that the number of multiplications depend on how the field of constants used in the algorithm splits P. If $P = \prod_{i=1}^{k} P_i^{l_i}$ then $2 \cdot \deg(P) - k$ multiplications are needed. (We assume that P_i is irreducible.)

I. Introduction

The framework for many of the results on the number of multiplications necessary to compute algebraic functions is as follows: We start with a field G, called the field of constants, and then consider the functions to be computed as elements of $F = G(x_1, x_2, \ldots, x_n)$—the extension of G by the indeterminates $x_1, \ldots, x_n$. The lower bounds which are then derived on the number of multiplications needed to compute the functions are valid even if multiplications by a fixed element $g \in G$ is not counted as a multiplication. (See, for example, [1] and [2].)

This assumption, that a multiplication by a $g \in G$ is not counted, is valid if g is an integer, for then this multiplication may be replaced by several additions. In many applications the assumption may still be valid if g is a rational number, but if $G = Q(\sqrt{2})$, why assume that multiplication by $\sqrt{2}$ is not counted?

Many of the results in the literature are insensitive to the exact nature of G. The results of [1] and [2], for example, are of this nature, but as we will see in the next section the minimum number of multiplications may depend on the choice of G. We will give an example which requires 3 multiplications if $G = Q$, the rationals, but only 2 if $G = \mathbb{C}$, the complex number. We will then use the algorithm for $G = \mathbb{C}$ to construct an efficient algorithm to solve a related problem for the case $G = Q$.

In the following section we will analyze the dependence of the number of multiplications on the field G for a certain class of systems of bilinear forms. Fiduccia and Zalcstein [3] obtained the result of Theorem 3 for the case $l = 1$. They also obtained the result of the first half of Corollary 1 when the field G splits P and P has no repeated roots.

II. Examples

Consider the following system of bilinear forms:

$$\begin{aligned} \psi_1 &= x_1y_1 - x_2y_2 \\ \psi_2 &= x_2y_1 + x_1y_2. \end{aligned} \tag{1}$$

This system is the real and imaginary part of the product of two complex numbers. It can be computed using 3 multiplications, for example:

$$\begin{gathered} m_1 = x_1(y_1+y_2) \qquad m_2 = (x_1+x_2)y_2 \qquad m_3 = (-x_1+x_2)y_1 \\ \psi_1 = m_1 - m_2 \qquad \psi_2 = m_1 + m_3. \end{gathered} \tag{2}$$

It is known [4] that 3 multiplications is minimal if we take the field of constants to be Q. However, if we take $G = Q(i)$ then we have the following algorithm, which uses only 2 multiplications:

$$\begin{aligned} P_1 &= \frac{x_1+ix_2}{2}(y_1+iy_2) & P_2 &= \frac{x_1-ix_2}{2}(y_1-iy_2) \\ \psi_1 &= P_1+P_2 & \psi_2 &= -iP_1+iP_2. \end{aligned} \tag{3}$$

The next example will illustrate how the second algorithm can be used to derive an efficient algorithm when $G = Q$.

Consider the system of bilinear forms

$$\begin{pmatrix} \psi_1 \\ \psi_2 \\ \psi_3 \\ \psi_4 \end{pmatrix} = \begin{pmatrix} x_1 & -x_2 & -x_3 & x_4 \\ x_2 & x_1 & -x_4 & -x_3 \\ x_3 & -x_4 & x_1 & -x_2 \\ x_4 & x_3 & x_2 & x_1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \\ y_4 \end{pmatrix}. \tag{4}$$

This system is easily recognizable as the direct product of the complex algebra with itself, that is, if we denote:

$$X_1 = (x_1+ix_2), \quad X_2 = (x_3+ix_4), \quad Y_1 = (y_1+iy_2), \quad Y_2 = (y_3+iy_4)$$

then:

$$\begin{aligned} \psi_1 &= \mathrm{Re}(X_1Y_1 - X_2Y_2) \\ \psi_2 &= \mathrm{Im}(X_1Y_1 - X_2Y_2) \\ \psi_3 &= \mathrm{Re}(X_2Y_1 + X_1Y_2) \\ \psi_3 &= \mathrm{Im}(X_2Y_1 + X_1Y_2). \end{aligned} \tag{5}$$

It may be seen that $9 = 3^2$ multiplications are necessary to compute (4) when $G = Q$, however, using algorithm (3) we can obtain an algorithm for computing (4) using only 6 multiplications. Using algorithm (3) we define

$$\begin{aligned} P_1 &= \frac{X_1+iX_2}{2}(Y_1+iY_2) = \frac{(x_1-x_4)+i(x_2+x_3)}{2}((y_1-y_4)+i(y_2+y_3)) \\ P_2 &= \frac{X_1-iX_2}{2}(Y_1-iY_2) = \frac{(x_1+x_4)+i(x_2-x_3)}{2}((y_1+y_4)+i(y_2-y_3)) \end{aligned} \tag{6}$$

$$\begin{aligned} X_1Y_1-X_2Y_2 &= P_1+P_2 \\ X_2Y_1+X_1Y_2 &= -iP_1+iP_2, \end{aligned}$$

and therefore:

$$\begin{aligned} \psi_1 &= \mathrm{Re}(P_1)+\mathrm{Re}(P_2) \\ \psi_2 &= \mathrm{Im}(P_1)+\mathrm{Im}(P_2) \\ \psi_3 &= \mathrm{Im}(P_1)-\mathrm{Im}(P_2) \\ \psi_4 &= -\mathrm{Re}(P_1)+\mathrm{Re}(P_2). \end{aligned} \tag{7}$$

Using algorithm (2) twice we can compute $\mathrm{Re}(P_1)$, $\mathrm{Im}(P_1)$, $\mathrm{Re}(P_2)$, $\mathrm{Im}(P_2)$ in 6 multiplications, that is:

$$\begin{aligned} m_1 &= \frac{x_1-x_4}{2}(y_1-y_4+y_2+y_3) & m_2 &= \frac{x_1-x_4+x_2+y_3}{2}(y_2+y_3) \\ m_3 &= \frac{-x_1+x_4+x_2+x_3}{2}(y_1-y_4) & m_4 &= \frac{x_1+x_4}{2}(y_1+y_4+y_2-y_3) \\ m_5 &= \frac{x_1+x_4+x_2-x_3}{2}(y_2-y_3) & m_6 &= \frac{-x_1-x_4+x_2-x_3}{2}(y_1+y_4) \end{aligned} \tag{8}$$

$$\begin{aligned} \mathrm{Re}(P_1) &= m_1-m_2 & \mathrm{Im}(P_1) &= m_1+m_3 \\ \mathrm{Re}(P_2) &= m_4-m_5 & \mathrm{Im}(P_2) &= m_4+m_6. \end{aligned}$$

Substituting (8) into (7) we obtain:

$$\begin{aligned} \psi_1 &= m_1-m_2+m_4-m_5 & \psi_2 &= m_1+m_4+m_3+m_6 \\ \psi_3 &= m_1+m_3-m_4-m_6 & \psi_4 &= -m_1+m_2+m_4-m_5. \end{aligned} \tag{9}$$

In the next section we will see that 6 multiplications is minimal for the system (4).

It should be clear that the construction used above is quite general. Using this construction one can show, for example, that if there is an algorithm for computing two $n_0 \times n_0$ matrices in k multiplications using any field $G \leq \mathbb{C}$, then it is possible to multiply two $n \times n$ in $An^{\log_{n_0} k}$ operations.

III. Results

In this paper we will write a system of bilinear forms as $A(\underline{x})\underline{y}$ where $A(\underline{x})$ is a

$t \times m$ matrix whose entries are linear forms (over G) of the indeterminates $\{x_1, x_2, \ldots, x_n\}$, and $\underline{y}$ is the (column) vector $(y_1, y_2, \ldots, y_m)^T$. We will need the following two results from [2]:

THEOREM 1: *Let $A(\underline{x})\underline{y}$ be a system of bilinear forms. If $A(x)$ has at least s columns such that no non-trivial linear combination of them (with coefficients in G) yields the column $\underline{0}$ then any algorithm for computing $A(\underline{x})\underline{y}$ requires at least s multiplications.*

THEOREM 2: *Let $A(\underline{x})\underline{y}$ be a system of bilinear forms, and let s be the minimum number of multiplications needed to compute $A(\underline{x})\underline{y}$, then there exists 2s linear forms (of x's and y's with coefficients in G) $L_1, L_2, \ldots, L_s, L_1', L_2', \ldots, L_s'$ such that $A(\underline{x})\underline{y} = U\underline{m}$ where U is a matrix with entries in G, m is the (column) vector $(m_1, m_2, \ldots, m_s)^T$ and $m_i = L_i \cdot L_i'$ $i = 1, 2, \ldots, s$.*

Let $R(z) = \sum_{i=0}^{a} x_i z^i$ and $S(z) = \sum_{i=0}^{b} y_i z^i$ be two polynomials with indeterminates as coefficients, and let $T(z) = R(z) \cdot S(z)$. The $a+b+1$ coefficients of T are a system of bilinear forms, denoted by $\tilde{T}$. It is known [3] that the minimum number of coefficients needed to compute $\tilde{T}$ is $a+b+1$.

One way of computing $\tilde{T}$ using $a+b+1$ multiplications starts by choosing $a+b+1$ distinct elements of G, $\alpha_0, \alpha_1, \ldots, a_{a+b}$. Since $\deg(T) = a+b$ we have

$$R(z) \cdot S(z) = R(z) \cdot S(z) \bmod \prod_{i=0}^{a+b} (z-\alpha_i). \tag{10}$$

By the Chinese Remainder Theorem $R(z) \cdot S(z) \bmod \prod_{i=0}^{a+b} (z-\alpha_i)$ can be obtained by computing $R(z) \cdot S(z) \bmod (u-\alpha_i) = R(\alpha_i) \cdot S(\alpha_i)$ for $i = 0, 1, \ldots, a+b$, and then using only multiplications by elements of G we obtain $R(z) \cdot S(z) \bmod \prod_{i=0}^{a+b} (z-\alpha_i)$. The $a+b+1$ multiplications are $R(\alpha_i) \cdot S(\alpha_i)$ $i = 0, 1, \ldots, a+b$. This method is essentially the one described in [6].

A second method starts by choosing $a+b$ distinct elements of G, $\beta_1, \beta_2, \ldots, \beta_{a+b}$, and uses the identity

$$R(z) \cdot S(z) = R(z) \cdot S(z) \bmod \prod_{i=1}^{a+b} (z-\beta_i) + x_a y_b \prod_{i=1}^{a+b} (z-\beta_i). \tag{11}$$

As before $R(z) \cdot S(z) \bmod \prod_{i=1}^{a+b} (z-\beta_i)$ is computed by using the Chinese Remainder Theorem using $a+b$ multiplications, and the $(a+b+1)^{\text{st}}$ multiplication is $x_a \cdot y_b$.

Of course we could replace the product $R(\alpha_i) \cdot S(\alpha_i)$ by the product $(g \cdot R(\alpha_i)) \cdot (h \cdot S(\alpha_i))$ for any $g, h \in G$ $(g, h \neq 0)$. If we agree to call two algorithms *essentially the same* if they differ only by this kind of changes then we obtain:

THEOREM 3: *Any algorithm for computing $\tilde{T}$ in $a+b+1$ multiplications is essentially the same as either the one derived from* (10) *or the one derived from* (11).

Proof: Let $m_0, m_1, \ldots, m_{a+b}$ be the $a+b+1$ multiplications. Since

$$\tilde{T} \equiv \begin{pmatrix} x_0 & 0 & \cdots & 0 \\ x_1 & x_0 & \cdots & \cdot \\ \cdot & x_1 & & 0 \\ \cdot & & & \\ \cdot & \cdot & & \\ x_a & \cdot & & x_0 \\ 0 & x_a & & x_1 \\ \cdot & 0 & & \cdot \\ \cdot & \cdot & & \cdot \\ \cdot & \cdot & & \cdot \\ 0 & 0 & & x_a \end{pmatrix} \begin{pmatrix} y_0 \\ y_1 \\ \cdot \\ \cdot \\ \cdot \\ \cdot \\ y_b \end{pmatrix} \equiv Xy \tag{12}$$

we obtain that there exists an $(a+b+1) \times (a+b+1)$ matrix U with entries from G such that

$$X\underline{y} = U\begin{pmatrix} m_0 \\ m \\ m_{a+b} \end{pmatrix} \tag{13}$$

Since all the rows of X are linearly independent (over G) we obtain that U is nonsingular. Let $W = U\ ^{1}$. Consequently,

$$(WX)\underline{y} = \begin{pmatrix} m_0 \\ m_1 \\ m_{a+b} \end{pmatrix} \tag{14}$$

Let $(w_0^i, w_1^i, \ldots, w_{a+b}^i)$ denote the i^{th} row of W, then from (14) we obtain

$$\left(\sum_{j=0}^{a} w_j^i x_j, \sum_{j=0}^{a} w_{j+1}^i x_j, \ldots, \sum_{j=0}^{a} w_{j+b}^i x_j\right) \begin{pmatrix} y_0 \\ y_1 \\ y_b \end{pmatrix} = m_i, \tag{15}$$

that is the bilinear form (15) can be computed in only one multiplication, and by Theorem 1 all of the forms $\sum_{j=0}^{a} w_{j+b}^i x_j$ $k = 0, 1, \ldots, b$ are multiples of one of them. That is the matrix

$$\begin{pmatrix} w_0^i & w_1^i \; \ldots \; w_a^i \\ w_1^i & w_2^i \; \ldots \; w_{a+1}^i \\ & \\ w_b^i & w_{b+1}^i \; \ldots \; w_{a+b}^i \end{pmatrix} \tag{16}$$

has rank 1. It is easily verified that this can happen under only two situations:

either $0 = w_0^i = w_1^i = w_2^i = \dots = w_{a+b-1}^i$ and $w_{a+b}^i \neq 0$, or there exists α_i such that $w_j^i = (\alpha_i)^j w_0^i$ $j = 0, 1, \dots, a+b$. Since W is non-singular at most one row can be of the second type, and if two rows are of the first kind their α's are different.

If W has no row of the second type, the algorithm is essentially the same as (10), and otherwise it is essentially the same as (11). This proves the theorem.

In the rest of the paper we will assume $a = b = n-1$.

Let $P = z^n + \sum_{i=0}^{n-1} a_i z^i$ be a polynomial with coefficients in a field F. Let $R = \sum_{i=0}^{n-1} x_i z^i$ and $S = \sum_{i=0}^{n-1} y_i z^i$ be two polynomials with indeterminates as coefficients. The coefficients of the polynomial $T(z) = R(z) \cdot S(z) \bmod P$ are a system of bilinear forms, denoted by $\tilde{T}_p$. For example, if $P = z^2 + 1$, the system $\tilde{T}_p$ is

$$(17) \qquad \begin{array}{c} x_0 y_0 - x_1 y_1 \\ x_1 y_0 + x_0 y_1, \end{array}$$

that is, the same as (1).

The results in this section will describe the minimum number of multiplications needed to compute $\tilde{T}_p$, and its dependence on G.

THEOREM 4: *Let $P = \bar{P}^l$ where $\bar{P}$ is irreducible (over G), and let $n = deg(P)$. The minimum number of multiplications needed to compute $\tilde{T}_p$ is $2n-1$.*

Proof. Let C_p be the companion matrix of P, and let $V_p = \{v \in G^n \mid \exists$ polynomial $q \neq 0$, $\deg(q) < n$ and $vq(C_p) = 0\}$. Since $\bar{P}$ is irreducible, $q(C_p)$ is non-singular whenever $\bar{P} \nmid q$. If $v \in V_p$ then $vq(C_p) = 0$ then $q = \bar{P}^r \cdot \bar{q}$ for some $1 > r > 0$ and $\bar{q}$ relatively prime to $\bar{P}$. Therefore $0 = vq(C_p) = v\bar{P}^r(C_p)\bar{q}(C_p)$, and since $\bar{q}(C_p)$ is non-singular $v\bar{P}^r(C_p) = 0$ and consequently $v\bar{P}^{l-1}(C_p) = 0$. So $V_p = \{v \in G^n \mid v\bar{P}^{l-1}(C_p) = 0\}$. We thus deduce that V_p is a subspace of G^n and $\dim(\bar{V}_p) < n$.

Let $\tilde{T}p = A(\underline{x})\underline{y}$ then $A(\underline{x})$ is

$$(18) \qquad A(\underline{x}) = (\underline{x} \mid C_p \underline{x} \mid C_p^2 \underline{x} \mid \dots \mid C_p^{n-1} \underline{x})$$

where $\underline{x}$ is the (column) vector $(x_0, x_1, \dots, x_{n-1})^T$. (This follows from the observation that the coefficients of the polynomial $z \sum_{i=0}^{n-1} t_i z^i \bmod P$ are $C_p \cdot t$ where t^T is the vector $(t_0, t_1, \dots, t_{n-1})$). Let t be the minimum number of multiplications needed to compute $\tilde{T}_p$, then by Theorem 2, $A(\underline{x})\underline{y} = U\underline{m}$ where U is an $n \times t$ matrix with entries in G and $\underline{m} = (m_1, m_2, \dots m_t)^T$. Since for all non-zero (row) vectors $w \in G^n \mid wA(\underline{x}) \neq 0$ we obtain that rank $(U) = n$, and therefore U has n linearly independent columns. Assume with no loss of generality that the first n columns of U are linearly independent (otherwise we can permute the columns of U and the m_i's). There exists, therefore, an $n \times n$ non-singular matrix W such that $WU = (I \mid U')$. Since W is non-singular its rows span G^n and therefore there exists a row of W which is not in V_p. Assume with no loss of generality that it is the first row, and denote it by w. Since $WA(\dot{\underline{x}})\underline{y} = (I \mid U')\underline{m}$, we obtain $wA(\underline{x})\underline{y} = (1, 0, \overset{n}{\dots}, 0, u_1', u_2', \dots, u_{t-n}')\underline{m}$, i.e., the bilinear form $wA(\underline{x})\underline{y}$ can be computed using $t-n+1$ multiplications. We claim that no non-trivial linear combination of the columns of $wA(\underline{x})$ is 0. Assume

$$0 = \sum_{i=0}^{n-1} wC_p^i \underline{x} \cdot \alpha_i = w\left(\sum_{i=0}^{n-1} \alpha_i C_p^i\right)\underline{x} \text{ then } w \sum_{i=0}^{n-1} \alpha_i C_p^i = 0,$$

but $w \notin V_p$ and therefore $\alpha_i = 0 \; i = 0, 1, \ldots, n-1$. By Theorem 1 at least n multiplications are needed to compute $wA(\underline{x})\underline{y}$, that is, $t-n+1 \geq n$, and $t \geq 2n-1$ which proves the theorem. (Note that since $\tilde{T}$ can be computed in $2n-1$ multiplications so can $\tilde{T}_p$.)

Let $P = P_1^{l_1} \cdot P_2^{l_2}$ where P_1, P_2 are irreducible and $(P_1, P_2) = 1$. By the Chinese Remainder Theorem the system $\tilde{T}_p$ can be computed by computing $\tilde{T}_{p^{l}_1}$ and $\tilde{T}_{p_2{}^{l_2}}$ and then combining the results using only additions and multiplications by elements of G.

Definition: Let $A(\underline{x})\underline{y}$ and $B(\underline{\xi})\underline{\eta}$ be two systems of bilinear forms on disjoint sets of indeterminates. The *disjoint sum of A and B*, denoted by $A+B$, is the system

$$\begin{pmatrix} A(x) & 0 \\ 0 & B(\underline{\xi}) \end{pmatrix} \begin{pmatrix} \underline{y} \\ \underline{\eta} \end{pmatrix}.$$

An *algorithm for computing $A \oplus B$ is said to be disjoint* if its matrix U is

$$U = \begin{pmatrix} U_1 & 0 \\ 0 & U_2 \end{pmatrix},$$

that is, if it can be viewed as computing $A(\underline{x})\underline{y}$ and $B(\underline{\xi})\underline{\eta}$ separately.

Conjecture: The minimum number of multiplications needed to compute $A \oplus B$ is $m(A) + m(B)$ where $m(A)$ denotes the minimum number of multiplications needed to compute $A(\underline{x})\underline{y}$, and similarly for $m(B)$. Moreover, every algorithm which computes $A \oplus B$ in the minimum number of multiplications is disjoint.

We cannot prove the conjecture in general but the next theorem proves it in a special case.

THEOREM 5: *Let $P_i = \bar{P}_i^{l_1}$ $i = 1, 2, \ldots, k$, where $\bar{P}_i$ is irreducible and $deg(P_i) = n_i$, and let $n = \sum_{i=1}^{k} n_i$. The minimum number of multiplications required to compute $\tilde{T} = \tilde{T}_{p_1} \oplus \tilde{T}_{p_2} \oplus \ldots \oplus \tilde{T}_{p_k}$ is $2n-k$. Moreover, every algorithm for computing this system in $2n-k$ multiplications is disjoint.*

Proof: Let $\tilde{T}_{p_i}$ be $A_i(\underline{x}^i)\underline{y}^i$ and $\tilde{T}$ be $A(\underline{x})\underline{y}$ where

$$A(\underline{x}) = \begin{pmatrix} A_1(\underline{x}^1) & & 0 \\ & A_2(\underline{x}^2) & \\ 0 & & A_k(\underline{x}^k) \end{pmatrix} \quad y = \begin{pmatrix} y^1 \\ y^2 \\ \\ y^k \end{pmatrix} \tag{19}$$

Let $A(\underline{x})\underline{y} = U_{n \times t}\underline{m}$, (where t denotes the number of multiplications), then since all the rows of $A(\underline{x})$ are linearly independent, the rank of U is n. Therefore there exists an $n \times n$ non-singular matrix W such that $WU = (I \,|\, U')$. Partition W as $W = (W^1 \,|\, W^2 \,|\, \ldots \,|\, W^k)$ where W^1 is the first n_1 columns of W, W^2 the next n_2 columns of W, etc. Since W is non-singular $\text{rank}(W^i) = n_i$ $i = 1, 2, \ldots, k$. Therefore each W^i has a row which is not in V_{p_i}. Let w_j^i denote the j^{th} row of W^i, and let $p(j)$ denote the cardinality of the set $\{i | w_j^i \notin V_{P_i}\}$.

LEMMA 1: *If for some j, $p(j) = s$ then $t \geq 2n-k+s-1$.*

Proof: Assume with no loss of generality that $p(1) = s$ and that $w_1^i \notin V_{P_i}$ $i = 1, 2, \ldots, s$. Let $j_{s+1}, j_{s+2}, \ldots, j_k$ be such that $w_{j_r}^r \notin V_{P_{j_r}}$ $r = s+1, s+2, \ldots, k$, then there exists a row vector β with non-zero coefficients only in positions $1, j_{s+1}, j_{s+2}, \ldots, j_k$ such that if $\gamma = \beta W = (\gamma_1\gamma_2 \ldots \gamma_k)$ then $\gamma_i \notin V_{P_i}$ $i = 1, 2, \ldots, k$. Consider the bilinear form $\beta W A(\underline{x})\underline{y} = \beta(I\ \ U')\underline{m}$. We claim that at least n multiplications are needed to compute it. Consider any nontrivial linear combinations of the columns of $\beta W A(\underline{x}) = \gamma A(\underline{x})$. Substituting $C_{P_i}^j \underline{x}^i$ for the j^{th} column of $A_i(\underline{x}^i)$ we obtain that this linear combination is

$$\sum_{i=1}^{k} \gamma_i \left(\sum_{j=0}^{n_j-1} \alpha_{i,j} C_{P_i}^j \right) \underline{x}^i.$$

This linear combination vanishes if and only if $\gamma_i \sum_{j=0}^{n_i-1} \alpha_{i,j} C_{P_i}^j = 0$ for $i = 1, 2, \ldots, k$. But $\gamma_i \notin V_{P_i}$ and therefore $\alpha_{i,j} = 0$ for all i and j. This establishes the claim. By Theorem 1 at least n multiplications are needed to compute $\gamma A(\underline{x})\underline{y}$, but $\beta(I\ \ U')$ has at most $k-s+1+t-n$ non-zero coefficients, and therefore $k-s+1+t-n \geq n$ or $t \geq 2n-k+s-1$. This proves the lemma.

Since $s \geq 1$ we have also proved that every algorithm for computing $\tilde{T}$ requires at least $2n-k$ multiplications. Since it can be trivially computed in $2n-k$ multiplications, this proves the first half of the theorem.

To prove the second half of the theorem, consider an algorithm for computing $\tilde{T}$ in $2n-k$ multiplications, and write it as $\tilde{T} = Um$. Let W be as before, then as a consequence of Lemma 1 we obtain $p(j) \leq 1$ for $j = 1, 2, \ldots, n$ i.e., we can partition the rows of W into $k+1$ disjoint sets $N_0, N_1, N_2, \ldots N_k$ such that if $j \in N_0$ $w_j^i \in V_{P_i}$ for $i = 1, 2, \ldots, k$, and if $j \in N_r$ $(r \neq 0)$ then $w_j^r \notin V_{P_r}$ and $w_j^i \in V_{P_i}$ for $i \neq r$. With no loss of generality we may assume that $N_1 = \{1, 2, \ldots, m_1\}$, $N_2 = \{m_1+1, m_1+2, \ldots, m_1+m_2\}$, etc. and that $N_0 = \{\sum_{i=1}^k m_i+1, \sum_{i=1}^k m_i+2, \ldots, n\}$. (If this is not the case we can permute the rows of W, to bring it to this form.) As before we have $WU = (I\ \ U')$ and denote the i, j entry of U' by $u'_{i,j}$.

LEMMA 2: *If $i_1 \in N_{j_1}$ and $i_2 \in N_{j_2}$ $j_1 \neq j_2$ $(j_1, j_2 \neq 0)$ then for all j, $u'_{i_1,j} \cdot u'_{i_2,j}$* $= 0$.

Proof: Assume $u'_{i_1,j} \neq 0$ and $u'_{i_2,j} \neq 0$. Assume with no loss of generality, that $j_1 = 1$, $i_1 = 1$, $j_2 = 2$, $i_2 = m_1+1$, and $j = 1$. Let M be the matrix

$$M = \begin{pmatrix} 1/u'_{1,1} & 0 & 0 & \ldots & 0 \\ -\dfrac{u'_{2,1}}{u'_{1,1}} & 1 & 0 & & 0 \\ -\dfrac{u'_{3,1}}{u'_{1,1}} & 0 & 1 & & 0 \\ -\dfrac{u'_{n,1}}{u'_{1,1}} & 0 & 0 & & 1 \end{pmatrix} \tag{20}$$

Then $MWA(\underline{x})\underline{y} = \bar{W}^{A(\underline{x})}\underline{y} = M(I \,\vert\, U')\underline{m} = (I \,\vert\, \bar{U})\underline{m}'$ where $\underline{m}'$ is $\underline{m}$ with the first and $(n+1)^{\text{st}}$ entries exchanged, and $(I \mid \bar{U}) = M(I \mid U')$ with the first and $(n+1)^{\text{st}}$ columns exchanged. The $(m_1+1)^{\text{st}}$ row of $\bar{W}$ is

$$\left(w^1_{m_1+1} - \frac{u'_{m+1,1}}{u'_{1,1}} w_1{}' \;\middle|\; w^2_{m_1+1} - \frac{u'_{m+1,1}}{u'_{1,1}} w^2_1 \;\middle|\; \dots \;\middle|\; w^k_{m+1} - \frac{u'_{m+1,1}}{u'_{1,1}} w^k_1 \right).$$

By construction $w^1_{m_1+1} \in V_{P_1}$ and $w^1_1 \notin V_{P_1}$ and therefore

$$w^1_{m_1+1} - \frac{u'_{m+1,1}}{u'_{1,1}} w^1_1 \notin V_{P_1},$$

similarly

$$w^2_{m_1+1} - \frac{u'_{m+1,1}}{u'_{1,1}} w^2_1 \notin V_{P_2},$$

and by Lemma 1 the algorithm uses at least $2n-k+1$ multiplications. Contradiction!

Lemma 2 states that the $n-k$ columns of U' can be partitioned into $k+1$ disjoint sets $M_0, M_1, \dots, M_k$ such that if $i \in N_{j_1}$ $(j_1 \neq 0)$ and $j \in M_{j_2}$ $(j_2 \neq j_1)$ then $u'_{i,j} = 0$. Schematically then U' can be written as

$$(21) \qquad U' = \begin{array}{c} \\ N_1 \\ \\ N_2 \\ \\ \\ N_k \\ N_0 \end{array} \left(\begin{array}{c|c|c|c|c} M_1 & M_2 & \cdots\cdots & M_k & M_0 \\ U_1' & 0 & \dots\dots & 0 & \\ \hline 0 & U_2' & \dots\dots & 0 & \\ \hline \vdots & \vdots & \vdots & \vdots & \\ 0 & 0 & \dots\dots & U_k' & \\ \hline & & U_0' & & \end{array}\right)$$

LEMMA 3: (1) *For each ś the cardinality of $M_{ś}$ is $n_{ś} - 1$ (and therefore $M_0 = \emptyset$).*

(2) *If $i \in N_r$ and $j \in M_r$ $(r \neq 0)$ then $u'_{i,j} \neq 0$.*

(3) *If $i \in N_r$ then $w^j_i = 0$ for $j \neq r$.*

Proof: Let i be in $N_r (r \neq 0)$ then since $WA(\underline{x})\underline{y} = (I \mid U')\underline{m}$ we obtain that the bilinear form $(w^1_i, w^2_i, \dots, w^k_i)A(\underline{x})y = (0, 0, \cdot\, 0, \overset{i}{1}, 0, \dots \overset{n}{0}, 0 \dots 0, \overset{M_r}{u'_{r,i}}\, 0, \dots, 0)\,\underline{m} = u_i m$. Since $w^r_i \notin V_{P_r}$ we obtain from Theorem 1 as in the proof of Theorem 4, that at least n_r multiplications are needed to compute it, and that therefore u_j has at least n_r non-zero entries. But that means that the cardinality of M_r is at least $n_r - 1$. Since U' has $n - k = \sum_{s=1}^{k} (n_s - 1)$ columns the cardinality of

M_r is exactly $n_r - 1$, and u^j has exactly n_r non-zero entries. To prove the third part of the lemma, observe that if $w_i^j \neq 0$ for $j \neq r$ then $(w_i^1 \mid w_i^2 \mid \ldots \mid w_i^k)A(\underline{x})$ has at least $n_r + 1$ linearly independent columns, namely the n_r columns $\sum_{a=1}^{r-1} n_a + 1, \sum_{a=1}^{r-1} n_a + 2, \ldots, \sum_{a=1}^{r} n_a$ (which are linearly independent since $w_i^r \notin V_{P_r}$) and without loss of generality, the column $\sum_{a=1}^{j-1} n_a + 1$ which is not zero since $w_i^j \neq 0$ and cannot depend on the other n_r columns since it has the indeterminates $\{x^j\}$ while the other n_r columns are linear combinations of the indeterminates $\{x^r\}$. But u_i has exactly n_r non-zero entries, contradicting Theorem 1.

LEMMA 4: *Let $i \in N_0$ and $j \in M_r$, and assume $u'_{i,j} \neq 0$, then:*
(1) *If $s \notin M_r$ then $u'_{i,s} = 0$.*
(2) *If $a \neq r$ then $w_i^a = 0$.*

Proof: Assume with no loss of generality that $j = 1 \in M_1$. Let M be as in the proof of Lemma 2 (that is, M as in (20)). Note that by Lemma 3, $u'_{1,1} \neq 0$. Let $\bar{W} = MW$ and let $M(I\ U')\underline{m} = (I\ \bar{U})\underline{m}'$ as in the proof of Lemma 2. Let $\bar{N}_0, \bar{N}_1, \ldots, \bar{N}_k$ be the partitioning of the rows of $\bar{W}$, then $i \in \bar{N}_1$, since

$$\bar{w}_i^1 = w_i^1 - \frac{u'_{i,1}}{u'_{1,1}} w_1^1 \notin V_{P_1}.$$

But by Lemma 2, if $s \notin M_r$ then $\bar{u}_{i,s} = u'_{i,s}$, and applying Lemma 2 again, we obtain $0 = \bar{u}_{i,s}$. This proves the first part of the lemma. By Lemma 3 (third part) $\bar{w}_i^s = w_i^s$, and again applying Lemma 3 we obtain $\bar{w}_i^s = 0$. This proves the lemma.

Lemma 4 states that the rows of W can be partitioned into k disjoint sets $\Pi_1, \Pi_2, \ldots, \Pi_k$, where $i \in \Pi_r$ if and only if $w_i^r \neq 0$. Since W is non-singular, the cardinality of Π_r is n_r, i.e.,

$$W = \begin{array}{cc} \begin{array}{c} \Pi_1 \\ \Pi_2 \\ \\ \\ \Pi_k \end{array} & \left(\begin{array}{c|c|c|c} W_1 & 0 & \cdots\cdots & 0 \\ \hline 0 & W_2 & \cdots\cdots & 0 \\ \hline & & \ddots & \\ & & & \\ \hline 0 & 0 & \cdots\cdots & W_k \end{array}\right) \end{array} \tag{22}$$

and similarly

$$U' = \begin{array}{cc} & \begin{array}{cccc} M_1 & M_2 & \cdots & M_k \end{array} \\ \begin{array}{c} \Pi_1 \\ \Pi_2 \\ \\ \\ \Pi_k \end{array} & \left(\begin{array}{c|c|c|c} U'_1 & 0 & \cdots & 0 \\ \hline 0 & U'_2 & \cdots & 0 \\ \hline & & \ddots & \\ & & & \\ \hline 0 & 0 & \cdots & U'_k \end{array}\right) \end{array} \tag{23}$$

and therefore the columns of $(I \mid U')$ can be permuted by a permutation P such that

$$(24) \qquad (I\ U')P = \begin{pmatrix} \tilde{U}_1 & 0 & \dots & 0 \\ 0 & \tilde{U}_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \\ 0 & 0 & \ddots & U_k \end{pmatrix}.$$

But $WA(\underline{x})\underline{y} = ((I \mid U')P)P^{-1}\underline{m}$ and therefore $A(\underline{x})\underline{y} = ((W^{-1}(I \mid U')P)P^{-1}\underline{m}$, that is, the columns of the matrix U could be permuted such that

$$(25) \qquad U = \begin{pmatrix} U_1 & 0 & \dots & 0 \\ 0 & U_2 & & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & U_k \end{pmatrix}$$

and therefore the algorithm is disjoint, and we have proved the second half of the theorem.

COROLLARY 1: *Let k be the number of irreducible factors of a polynomial P (not counting multiplicity) then the minimum number of multiplications needed to compute $\tilde{T}_p$ is $2 \cdot deg(P) - k$. Moreover, if P has no repeated roots and it is split by G then the minimal algorithms is unique.*

Proof: Let $P = \prod_{i=1}^{k} P_i^{l_i}$, by the Chinese Remainder Theorem multiplication modulo P is the same as multiplication modulo the $P_i^{l_i}$'s. The second part of the corollary follows from the observation that if P is linear the minimal algorithm for computing $\tilde{T}_p$ is unique.

COROLLARY 2: *Let $G = \mathbb{R}$, the reals. The minimal number of multiplications needed to compute the system (4) of bilinear forms is 6.*

Proof: Define $\xi_1 = x_1 + x_4$, $\xi_2 = x_2 - x_3$, $\xi_3 = x_1 - x_4$, $\xi_4 = x_2 + x_3$, $\eta_1 = y_1 + y_4$, $\eta_2 = y_2 - y_3$, $\eta_3 = y_1 - y_4$, $\eta_4 = y_2 + y_3$, then we obtain

$$(26) \qquad \begin{pmatrix} \psi_1 + \psi_4 \\ \psi_2 - \psi_3 \\ \psi_1 - \psi_4 \\ \psi_2 + \psi_3 \end{pmatrix} = \begin{pmatrix} \xi_1 & -\xi_2 & 0 & 0 \\ \xi_2 & \xi_1 & 0 & 0 \\ 0 & 0 & \xi_3 & -\xi_4 \\ 0 & 0 & \xi_4 & \xi_3 \end{pmatrix} \begin{pmatrix} \eta_1 \\ \eta_2 \\ \eta_3 \\ \eta_4 \end{pmatrix}.$$

System (19 is clearly equivalent to (4), and (19) is $\tilde{T}_p \oplus \tilde{T}_p$ where $P = z^2 + 1$.

REFERENCES

[1] PAN, V. YA., Methods of computing values of polynomials, *Russian Mathematical Surveys*, **21** (1966) 105–136.

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

[3] FIDUCCIA, C. M. and Y. ZALCSTEIN, *Algebras having linear multiplicative complexities*, Technical Report 46, Department of Computer Science, State University of New York at Stony Brook, (August 1975).

[4] WINOGRAD, S., On multiplication of 2 × 2 matrices, *Linear Alg. Appl.*, **4** (1971) 381–388.

[5] STRASSEN, V., Vermeidung von Divisionen, *J. für reine und angewandte Mathematik*, **264** (1973), 184–202.

[6] TOOM, A. L., The Complexity of a Scheme of Functional Elements, Soviet Mathematics, Translations of Doklady Akademie, *Nauk. S.S.S.R.*, **4**, (June 1963), 714–717.

Received December 3, 1975 and in revised form
April 8, 1976 and June 16, 1976