LINEAR DISJOINTNESS AND ALGEBRAIC COMPLEXITY

by Walter BAUR and Michael O. RABIN

Dedicated to Ernst Specker on the occasion of his 60th birthday.

1. INTRODUCTION

It is well known that any algorithm for the evaluation of a polynomial

$$f(y) = x_0 + x_1 y + \dots + x_n y^n, \tag{1}$$

or of an inner product of two vectors

$$(x, y) = x_1 y_1 + \dots + x_n y_n, \tag{2}$$

requires, under certain natural assumptions such as that $y, x_1, \dots, x_n$ are algebraically independent over some ground-field F, at least n multiplications. This number of multiplications can of course be achieved by an appropriate algorithm.

Motzkin [3] has introduced the idea of preprocessing the coefficients of a polynomial. In certain situations, for example when we have to evaluate f for many values $y = c_1, y = c_2, \dots$ of the argument, though these values are not given in advance, it makes sense to compute once and for all certain functions $\alpha_1(x_1, \dots, x_n), \dots, \alpha_n(x_1, \dots, x_n)$ of the coefficients and use these $\alpha_1, \dots, \alpha_n$ later on in an algorithm for the calculation of the $f(c_i)$, i.e. $f(y)$. The $\alpha_1, \dots, \alpha_n$ and the algorithm should be so chosen that the evaluation of $f(y)$ now requires fewer than n multiplications. The cost of this "preprocessing" of the coefficients $x_1, \dots, x_n$ is then absorbed in the saving in the computations $f(c_1), f(c_2), \dots$.

Motzkin has shown that preprocessing of the coefficients can lead to evaluation of $f(y)$ in $\left\lceil \frac{n}{2} \right\rceil + 2$ multiplications and $n + 2$ additions. From now on we shall concentrate our attention on the number of multiplications or divisions used in an algorithm. The notation $n\ M/D$ means n multiplications or divisions. We must take into account divisions as well as multiplications because a product xy can be computed by doing two divisions.

Winograd [6] has noted that if in (2) we allow preprocessing on both the x and y then $\left\lceil \frac{n}{2} \right\rceil M$ are sufficient. Namely, assume n even and define

$$w(x) = x_1 x_2 + x_3 x_4 + .. + x_{n-1} x_n .$$

If $w(x)$ and $w(y)$ have been precomputed then

$$(x, y) = (x_1 + y_2)(x_2 + y_1) + \ldots + (x_{n-1} + y_n)(x_n + y_{n-1}) - w(x) - w(y)$$

computes (2) with $\frac{n}{2} M$. There are situations, involving many vectors $x, y, z, \ldots$, and many scalar products, say, $(x, y), (y, z), (x, z), \ldots$, where this idea makes computational sense.

Can the upper bound $\frac{n}{2}$ in the algorithms for $f(y)$ and (x, y) with preprocessing be improved. Can we get lower bound results for these and more general computational problems. We have, of course, to be careful about the preprocessing that we permit. For example, if we permit to form products $x_i y_i$ then no multiplications will later be needed in computing (x, y). Thus preprocessing for (2) should not involve multiplications "mixing" the $x_1, \ldots, x_n$ with the $y_1, \ldots, y_n$, or with y in the case of $f(y)$. It will be seen later that the crux of this paper is a precise determination of the sort of "mixing" that should be avoided so as to yield a good lower-bound result.

In [3] (see also [4]) it is shown that if $F \subseteq K \subseteq K(y)$ and if $x_1, \ldots, x_n \in K$ are algebraically independent over F, then any computation of $f(y)$ which allows the use of any $\alpha_1, \alpha_2, \ldots \in K$ must involve $\frac{n}{2} M/D$, even if a multiplication step $a \cdot b$ is not counted if $a \in F$ or $b \in F$, and a step a/b is not counted when $b \in F$. Similar results hold for polynomials in several variables $y_1, y_2, \ldots$.

Winograd [6] has introduced another lower bound theorem for the case of computations with preprocessing. His theorem involves restrictions on the fields in question, and the conditions (involving topology) for the theorem to hold are difficult to interpret or check in specific cases. The proof in [6] employs topological methods.

In the present paper we observe that the concept of linear disjointness of two fields over a common subfield provides a proper framework for a very general result, Theorem 1, on lower bounds for the number of M/D operations in computations with preprocessing. The result and its simple proof are expressed in purely algebraic terms. In section 4 we apply Theorem 1 to obtain the known results on lower bounds, as well as new results which do not fall within the scope of previous methods.

2. Basic concepts and the Main Theorem

Let Ω be a field and S a subset of its elements. Following [5, 6], a (straight-line) algorithm or computation in (Ω, S) is a sequence π: $\pi(1), \ldots, \pi(l)$ where for each $1 \leqslant k \leqslant l$ we have $\pi(k) \in S$, or for some $i, j < k$, $\pi(k) = (+, i, j)$ or $(-, i, j)$ or $(\cdot, i, j)$ or $(/, i, j)$.

With π we associate the sequence $r(1), \ldots, r(l)$ of the results of the computation π. The $r(k)$ are all elements of $\Omega \cup \{u\}$. Define $r(1) = \pi(1) \in S$. Inductively, if $r(1), \ldots, r(k-1)$ are already defined we set $r(k) = \pi(k)$ if $\pi(k) \in S$, $r(k) = r(i) + r(j)$ if $\pi(k) = (+, i, j)$, etc. By convention, $r/0 = u + r = u \cdot r = \ldots = u$ for $r \in \Omega \cup \{u\}$.

We say that π computes the elements $a_1, \ldots, a_m \in \Omega$ if there exist $1 \leqslant i_j \leqslant l$, $1 \leqslant j \leqslant m$, so that for the results of π we have $r(i_j) = a_j$, $1 \leqslant j \leqslant m$.

In the sequel we shall be interested in fields $F \subseteq \Omega$ and two intermediate fields E, K. Thus

$$(3) \qquad \begin{array}{ccccc} & & \Omega & & \\ & \cup\!\!\!/ & & \backslash\!\!\cup & \\ & E & & K & \\ & \backslash\!\!\cup & & \cup\!\!\!/ & \\ & & F & & \end{array}$$

The following concept comes from the theory of fields and from algebraic geometry, see [1, 2].

Definition. The fields E and K are linearly disjoint over F if any $e_1, \ldots, e_m \in E$ which are linearly independent over F are also linearly independent over K, i.e. $\Sigma\, a_i e_i = 0$, $a_i \in K$, only if $a_i = 0$, $1 \leqslant i \leqslant m$.

As the definition stands, the fields E and K play different roles. It is however easy to see that the above definition implies the analogous statement with the roles of E and K interchanged. (See e.g. [1].)

Our theorem will be about computations π in $(\Omega, E \cup K)$. The fact that we permit using any $\alpha \in E \cup K$ at no computational cost captures, in an algebraic form, the idea of preprocessing.

We shall strengthen the contents of our lower bound results by disregarding those M/D used in a computation π where one of the factors or the denominator is a $g \in F$. An M/D-operation $\pi(k) = (\sigma, i, j)$ *counts* if $r(k) \neq u$ and either $\sigma = \cdot$ and $r(i), r(j) \notin F$, or $\sigma = /$ and $r(j) \notin F$.

Given $e_1, \ldots, e_p \in E$, we say that they are *independent mod F* over F if $\Sigma g_i e_i \in F$ and $g_i \in F$, $1 \leqslant i \leqslant p$, implies $g_i = 0$, $1 \leqslant i \leqslant p$.

With these concepts we can state our main result.

THEOREM 1. *Assume that* E *and* K *in* (3) *are linearly disjoint over* F. *Let* $d_{ij} \in K$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant p$, *be such that the degree of transcendence of* $D = \{d_{ij} \mid 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant p\}$ *over* F *is* t. *Let* $e_1, \ldots, e_p \in E$ *be linearly independent* mod F *over* F. *If* π *is any algorithm in* $(\Omega, E \cup K)$ *which computes all the* m *elements*

$$
\begin{array}{c}
d_{11}e_1 + \ldots + d_{1p}e_p \\
\cdot \\
\cdot \\
\cdot \\
d_{m1}e_1 + \ldots + d_{mp}e_p
\end{array}
\tag{4}
$$

then π *has at least* $\left\lceil \frac{t}{2} \right\rceil$ M/D *that count.*

The proof will be given in section 3. Let us consider some preliminary examples.

In (3), let $\Omega = F(x_1, \ldots, x_n, y_1, \ldots, y_n)$ where $x_1, \ldots, y_n$ are algebraically independent over F, and let $E = F(y_1, \ldots, y_n)$, $K = F(x_1, \ldots, x_n)$. Then E and K are linearly disjoint over F. This can be seen as follows: Assume $\Sigma r_i(x) s_i(y) = 0$ is a nontrivial dependence relation, $r_i(x) \in K$, $s_i(y) \in E$. Multiplying by some $r(x) \in F[x_1, \ldots, x_n]$ we may assume that all $r_i(x) \in F[x_1, \ldots, x_n]$. Let m be a monomial in $x_1, \ldots, x_n$ occurring in at least one $r_i(x)$ and let $g_i \in F$ be the coefficient of m in $r_i(x)$. Then $\Sigma g_i s_i(y)$ is a nontrival dependence relation with coefficients from F.

So the conditions of Theorem 1 hold for the inner product $(x, y) = x_1 y_1 + \ldots + x_n y_n$ with $t = n$ (and $m = 1$). Hence no algorithm π computing (x, y), even when allowed to use at no cost any rational functions $r(x_1, \ldots, x_n) \in K$, $s(y_1, \ldots, y_n) \in E$ can have fewer than $\left\lceil \frac{n}{2} \right\rceil$ M/D that count. Much stronger results on (x, y) will be given later, but we mention this fact now as an illustration of the concepts and because Winograd's preprocessing is of the kind covered by this remark.

The need for the condition that the e_i are linearly independent mod F is clear. Otherwise if, say, $m = 1$ and $e_i = g_i e_1 + h_i, g_i, h_i \in F, 2 \leqslant i \leqslant p$ then

$$d_1 e_1 + \dots + d_p e_p = (d_1 + g_2 d_2 + \dots + g_p d_p) e_1 + h_2 d_2 + \dots + h_p d_p .$$

Thus there is only one multiplication that counts.

It is not sufficient to require in Theorem 1 that $E \cap K = F$, even though this might seem to prevent a computation in $(\Omega, E \cup K)$ from "mixing" without cost elements from E with elements from K: Let Ω be the quotient field of the integral domain $F[x_1, x_2, x_3, y_1, y_2, y_3]/(x_1 y_1 + x_2 y_2 + x_3 y_3)$, and put $E = F(x_1, x_2, x_3) \subseteq \Omega, K = F(y_1, y_2, y_3) \subseteq \Omega$. In Ω, the elements x_1, x_2, x_3 are still algebraically independent over F, and similarly for y_1, y_2, y_3. Also $E \cap K = F$. So the conditions of Theorem 1, with $E \cap K = F$ instead of linear disjointness, hold for $x_1 y_1 + x_2 y_2 + x_3 y_3 = 0$. But the computation of this sum requires no operation instead of $2\ M/D$.

One might think that the condition of linear disjointness on E and K in Theorem 1 is already so strong that we could replace the degree of transcendence t by just the linear dimension. Thus if $e_1, \dots, e_p \in K$ are linearly independent mod F over F and similarly for $d_1, \dots, d_p \in K$, and E and K are linearly disjoint over F, does $\Sigma\, d_i e_i$ require at least $\left\lceil \frac{p}{2} \right\rceil M/D$ that count. The next example refutes this conjecture.

Denoting the algebraic closure of a field H by $\overline{H}$, let $\Omega = \overline{G(x, y)}$ where x, y are algebraically independent over G. Let $n > 1$ and put $F = G(x^n, y^n), E = F(x), K = F(y)$. Clearly the F-base $1, x, \dots, x^{n-1}$ of E remains linearly independent over K. Hence, by linear algebra, E and K are linearly disjoint over F. Consider the element

$$\frac{1 - x^n y^n}{1 - xy} - 1 = xy + x^2 y^2 + \dots + x^{n-1} y^{n-1} .$$

Obviously this element can be computed in $(\Omega, E \cup K)$ with $2\ M/D$.

3. Proof of Theorem

Put $e_o = 1$ and let $(e_i)_{i<\kappa}$ (κ some cardinal) be an extension of $e_0, e_1, ..., e_p$ to an F-base of E. By linear disjointness, $(e_i)_{i<\kappa}$ is also a K-base of the K-algebra $K[E]$. Since for $i, j < \kappa$ $e_i e_j = \sum_k g_{ijk} e_k$ for suitable $g_{ijk} \in F$ we have:

(5) If $(\Sigma a_i e_i)(\Sigma b_j e_j) = \Sigma c_k e_k$ where $a_i, b_j, c_k \in K$
(and the sums are finite of course) then

$$c_k = \sum_{i,j} a_i b_j g_{ijk} \in F[\{a_i\} \cup \{b_j\}],$$

Any element $r \in KE$, the quotient field of $K[E]$, can be written in the form

$$r = \frac{\Sigma a_i e_i}{\Sigma b_j e_j} + c$$

where $a_i, b_j, c \in K$, not all $b_j = 0$. Such a representation of r will be called a canonical representation, and the a_i's and b_j's are the coefficients of the given representation. Note that the canonical representation is not unique.

Lemma. *If $r_1, ..., r_n$ is the sequence of results of some computation in $(\Omega, E \cup K)$ using s M/D that count then there are $2s$ elements $\alpha_1, ..., \alpha_{2s} \in K$ such that each $r_\nu \neq u$, $1 \leqslant \nu \leqslant n$, has a canonical representation all of whose coefficients are in $F[\alpha_1, ..., \alpha_{2s}]$.*

The proof is by induction on n. The case $n = 0$ being trivial assume $n > 0$.

If $r_n \in E \cup K$ then obviously r_n has a canonical representation with coefficients in F, so the claim follows from the induction hypothesis. The same applies if $r_n = u$.

Next assume that $r_n \in \Omega$ is the result of a non-counting operation, i.e. $r_n = r_\mu \pm r_\nu$ for some $\mu, \nu < n$ or r_n is the result of a M/D where one of the factors or the denominator is a $g \in F$. Let us consider the case $r_n = r_\mu + r_\nu$, the other cases are similar. Choose $\alpha_1, ..., \alpha_{2s} \in K$ and canonical representations

$$r_\mu = \frac{A}{B} + c, \qquad r_\nu = \frac{A'}{B'} + c'$$

according to the induction hypothesis. Then, by (5), the coefficients of the canonical representation

$$r_n = \frac{AB' + A'B}{BB'} + (c + c')$$

also lie in $F[\alpha_1, \ldots, \alpha_{2s}]$.

Finally let $r_n = r_\mu \cdot r_\nu$ ($r_n = r_\mu / r_\nu$ resp.), $r_n \in \Omega$. Then, again by (5), the coefficients of the representation

$$r_n = \frac{(A + cB)(A' + c'B')}{BB'} \qquad \left(r_n = \frac{(A + cB)\, B'}{(A' + cB')B} \text{ resp.} \right)$$

lie in $F[\alpha_1, \ldots, \alpha_{2s-2}, c, c']$ where $\alpha_1, \ldots, \alpha_{2s-2} \in K$ are provided by induction hypothesis. Putting $\alpha_{2s-1} = c$, $\alpha_{2s} = c'$ completes the induction.

Proof of Theorem 1. Assume that π computes the elements $\sum_{j=1}^{p} d_{ij} e_j$, $1 \leqslant i \leqslant m$, in $(\Omega, E \cup K)$ with s counting M/D. By the Lemma there exist $\alpha_1, \ldots, \alpha_{2s} \in K$ and canonical representations

$$\sum_{j=1}^{p} d_{ij} e_j = \frac{\sum_k a_{ik} e_k}{\sum_q b_{iq} e_q} + c_i\,, \quad 1 \leqslant i \leqslant m\,, \tag{6}$$

with coefficients $a_{ik}, b_{iq} \in F[\alpha_1, \ldots, \alpha_{2s}]$. Now fix i. Multiplying (6) by the denominator gives

$$\Big(\sum_q b_{iq} e_q\Big)\Big(-c_i e_0 + \sum_j d_{ij} e_j\Big) = \sum_k a_{ik} e_k\,. \tag{7}$$

Multiplying out the left hand side and comparing the coefficients of each e_k on both sides (recall that $e_0, e_1, \ldots$, are independent over K) we obtain, by using (5), a system $\mathscr{S}$ of linear equations for the d_{ij}'s and c_i whose coefficients are F-linear forms of the b_{iq}'s. Now the equation (7) clearly determines the element $-c_i e_0 + \sum_j d_{ij} e_j$ uniquely. Since the e_j are K-linear independent it follows that $\mathscr{S}$ has a unique solution, and hence d_{ij}, $c_i \in F(\alpha_1, \ldots, \alpha_{2s})$, by linear algebra. Since D has degree of transcendence t over F we obtain $2s \geqslant t$, i.e. $s \geqslant \left\lceil \frac{t}{2} \right\rceil$.

Remark. The method for handling divisions was proposed by Volker Strassen and we kindly thank him for this.

4. Applications

Let us start by deriving some results which could also be obtained from the theorems in [3, 4, 6] mentioned in the introduction. Abreviating $x = x_1, \ldots, x_n$, $y = y_1, \ldots, y_k$, consider $\Omega = \overline{F(x, y)}$, $K = \overline{F(x)}$, $E = \overline{F(y)}$. Then E and K are linearly disjoint over $\bar{F}$ (see e.g. [1], p. 203).

Taking $k = 1$, $e_i = y_1^i$, $1 \leqslant i \leqslant n$, we see that any computation of $f(y_1) = x_1 y_1 + \ldots + x_n y_1^n$ in $(\Omega, E \cup K)$ requires $\left\lceil \frac{n}{2} \right\rceil$ M/D that count even if we disregard a M/D by an element $g \in \bar{F}$. Thus any preprocessing using algebraic functions $\alpha_1, \ldots$ in x and algebraic functions $\beta_1, \ldots$ in y, cannot save more than $\frac{n}{2}$ M/D.

Taking $k = n$, we get a similar result for $x_1 y_1 + \ldots + x_n y_n$.

In [6] Winograd has considered the computation of the product Ax where $A = (a_{ij})_{\substack{1 \leqq i \leqq m \\ 1 \leqq j \leqq n}}$ is an $m \times n$ matrix and x is the column vector $x = (x_1, \ldots, x_n)$. Computing Ax means, of course, computing the forms $a_{i1} x_1 + \ldots + a_{in} x_n$, $1 \leqslant i \leqslant m$. In our notations assume that $a_{ij} \in E$, $x_1, \ldots, x_n \in K$. Denote the column vectors of A by $v_1, \ldots, v_n$, thus $v_j \in E^m$.

We say that $\dim_{E^m/F^m}(v_1, \ldots, v_n) = r$, if r is the largest integer such that for some subset $\{i_1, \ldots, i_r\} \subseteq \{1, \ldots, n\}$

$$g_1 v_{i_1} + \ldots + g_r v_{i_r} \in F^m,\ g_i \in F \text{ implies } g_i = 0,\ 1 \leqslant i \leqslant r.$$

Winograd [6] assumes that $\dim_{E^m/F^m}(v_1, \ldots, v_n) = r$, and that $F \subseteq \mathbf{C}$— the field of complex numbers. Furthermore K is a field such that $F(x_1, \ldots, x_n) \subseteq K$ and K is embeddable in a field of continuous (except for isolated points) functions $f(x_1, \ldots, x_n)$ into $\mathbf{C}$ which vanish only at isolated points; similarly $F(y_1, \ldots, y_m) \subseteq E$, and E is embeddable in a field of functions $g(v_1, \ldots, y_m)$ with the above properties. Under these conditions, an algorithm for Ax requires at least $\left\lceil \frac{r}{2} \right\rceil$ M/D that count.

In purely algebraic terms we can state and prove the following theorem.

Theorem 2. *Let $A = (a_{ij})$ be an $m \times n$ matrix with $a_{ij} \in E$ and let $x_1, \ldots, x_n \in K$ be algebraically independent over F. Denote the columns of A by $v_1, \ldots, v_n$. If E and K are linearly disjoint over F, and if*

$\dim_{E^m/F^m}(v_1, \ldots, v_n) = r$, *then any algorithm* π *in* $(\Omega, E \cup K)$ *which computes* Ax *has at least* $\left\lceil \frac{r}{2} \right\rceil$ M/D *that count.*

Proof. Using vector notation, computing Ax means computing all coordinates of the sum

$$x_1 v_1 + \ldots + x_n v_n = w . \tag{8}$$

We may assume that $r = n$. Otherwise let without loss of generality $v_1, \ldots, v_r$, $r < n$, be vectors which are independent mod F^m over F. Then for $r < j \leqslant n$

$$v_j = g_{j1} v_1 + \ldots + g_{jr} v_r + u_j , \; g_{ji} \in F , \; u_j \in F^m .$$

Hence, from (8),

$$\begin{aligned} w &= (x_1 + g_{r+1,1} x_{r+1} + \ldots + g_{n1} x_n) v_1 + \ldots + x_{r+1} u_{r+1} + \ldots + x_n u_n \\ &= z_1 v_1 + \ldots + z_r v_r + u , \end{aligned}$$

where $u \in K^m$. Now the computation in $(\Omega, E \cup K)$ of u costs nothing, and the $z_1, \ldots, z_r \in K$ are algebraically independent over F. So we have the conditions of the theorem with $r = n$.

Assume from now on that $v_1, \ldots, v_n$ are independent mod F^m over F. Let $e_0 = 1, e_1, \ldots, e_p$ be elements in E which are linearly independent over F, such that every a_{ij} (the i-th component of v_j), $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant n$, is a linear combination of $e_0, \ldots, e_p$ with coefficients in F. Each v_j can be split $v_j = u_j + w_j$, where $u_j \in F^m$, and every coordinate of w_j is a linear combination of just $e_1, \ldots, e_p$ with coefficients in F. Thus $w = x_1 w_1 + \ldots + x_n w_n + u$, where $u \in K^m$, and computing $x_1 w_1 + \ldots + x_n w_n$ in $(\Omega, E \cup K)$ takes as many M/D that count as does computing w.

Because $v_1, \ldots, v_n$ are linearly independent mod F^m over F, we have that $w_1, \ldots, w_n$ are linearly independent over F. Consider the sum $Z_1 w_1 + \ldots + Z_n w_n$, where $Z_1, \ldots, Z_n$ are variables ranging over Ω. Writing the i-th coordinate of w_k as a linear combination $\sum_{j=1}^{p} g_{ijk} e_j$ and rearranging, we get

$$Z_1 w_1 + \ldots + Z_n w_n = \left[L_{i1}(Z) e_1 + \ldots + L_{ip}(Z) e_p \right]_{1 \leq i \leq m} \tag{9}$$

where $L_{ij}(Z) = \sum_{k=1}^{n} g_{ijk} Z_k$.

We claim that among the $L_{ij}(Z)$, $1 \leqslant i \leqslant m$, $1 \leqslant j \leqslant p$, there are n forms which are linearly independent. By this we mean that the rows of coefficients of these n forms are linearly independent over F. Otherwise there are $h_1, \ldots, h_n \in F$, not all 0, so that the substitution $Z_1 = h_1, \ldots, Z_n = h_n$ yields $L_{ij}(h) = 0, 1 \leqslant i \leqslant m, 1 \leqslant j \leqslant p$. By (9) we now have $h_1 w_1 + \ldots + h_n w_n = 0$, contradicting the linear independence of $w_1, \ldots, w_n$ over F.

Let $L_{i_1 j_1}(Z), \ldots, L_{i_n j_n}(Z)$ be such a system of n independent forms. Then $d_{i_1 j_1} = L_{i_1 j_1}(x_1, \ldots, x_n), \ldots, d_{i_n j_n} = L_{i_n j_n}(x_1, \ldots, x_n)$ are algebraically independent over F. This is because $x_1, \ldots, x_n$ is the unique solution of the regular system of linear equations

$$L_{i_e j_e}(Z_1, \ldots, Z_n) = d_{i_e j_e}, \qquad 1 \leqslant e \leqslant n .$$

Thus, finally

$$x_1 w_1 + \ldots + x_n w_n = [d_{i1} e_1 + \ldots + d_{ip} e_p]_{1 \leq i \leq m} \tag{10}$$

with $d_{ij} \in K$, and the degree of transcendence of the d_{ij} over F is n. So, by Theorem 1, at least $\left\lceil \frac{n}{2} \right\rceil M/D$ that count are needed to compute (10), and hence to compute (8) in $(\Omega, E \cup K)$.

For the next application let $x_1, \ldots, x_n$ be algebraically independent over F and put $\Omega = \overline{F(x_1, \ldots, x_n)}, E = \bar{F}, K = F(x_1, \ldots, x_n)$. Then, by an argument like the one used in the first example after the statement of Theorem 1, E and K are linearly disjoint over F. Therefore Theorem 1 implies that for any $\omega \in E$ of degree at least $n + 1$ over F the computation of

$$\omega x_1 + \ldots + \omega^n x_n \tag{11}$$

in $(\Omega, E \cup K)$ requires at least $\left\lceil \frac{n}{2} \right\rceil M/D$. Note that now we have a result about substitution of a specific algebraic number in a polynomial. We allow any rational preprocessing of the coefficients and any algebraic preprocessing of the argument ω.

Next we show that no finite number of algebraic functions of $x_1, \ldots, x_n$ simplifies the computation of (11) for all algebraic ω of degree $n + 1$ over the rationals $\mathbf{Q}$. Since any particular preprocessing of $x_1, \ldots, x_n$ by algebraic functions involve just a finite number of such functions, we essentially conclude that algebraic preprocessing of $x_1, \ldots, x_n$ in (11), as well as the ω (ω now depends on the chosen preprocessing of the x_i of course), does not reduce the number of M/D that count below $\left\lceil \frac{n}{2} \right\rceil$. Specifically

THEOREM 3. *Let*

$$G = \mathbf{Q}(x_1, ..., x_n),\ \Omega = \bar{G},\ a_1, ..., a_q \in \Omega,\ K = G(a_1, ..., a_q)$$

and $F = \mathbf{Q}$. *There exists an element* $\omega \in \overline{\mathbf{Q}}$ *of degree* $n + 1$ *over* $\mathbf{Q}$ *such that any computation* π *for* (11) *in* $(\Omega, \overline{\mathbf{Q}} \cup K)$ *must have at least* $\left\lceil \frac{n}{2} \right\rceil$ M/D *that count.*

Proof. Define $F_1 = \overline{\mathbf{Q}} \cap K$. We shall prove slightly more than stated, namely that for a suitable $\omega \in \overline{\mathbf{Q}}$, computation of (11) in $(\Omega, \overline{\mathbf{Q}} \cup K)$ requires at least $\left\lceil \frac{n}{2} \right\rceil$ M/D that count even if we disregard M/D by a $g \in F_1$. The diagram of fields is

$$\begin{array}{ccc} & \overline{\mathbf{Q}(x_1, ..., x_n)} & \\ \cup\!\!/ & & \backslash\!\!\cup \\ \overline{\mathbf{Q}} & & K \\ \backslash\!\!\cup & & \cup\!\!/ \\ & F_1 = \overline{\mathbf{Q}} \cap K & \\ & \cup\!\!| & \\ & F = \mathbf{Q} & \end{array}$$

Notice that $\overline{\mathbf{Q}} = \bar{F}_1$ and $\bar{F}_1 \cap K = F_1$. This implies that $\overline{\mathbf{Q}}$ and K are linearly disjoint over F_1. Namely let $e_1, ..., e_q \in \bar{F}_1$ be independent over F_1. Choose a primitive element $e \in \bar{F}_1$, of degree m over F say, such that $e_1, ..., e_q \in F_1(e)$, and let $f(X) \in F_1[X]$ be the minimal polynomial of e over F_1. Assume $f = f_1 f_2$ in $K[X]$. Since the coefficients of f_1, f_2 are algebraic over F_1 and since $\bar{F}_1 \cap K = F_1$ we obtain $f_1, f_2 \in F_1[X]$. Therefore f is irreducible in $K[X]$ and hence the elements $1, e, ..., e^{m-1}$ are linearly independent over K. By linear algebra it follows that $e_1, ..., e_q$ are linearly independent over K.

The degree $[F_1 : \mathbf{Q}]$ is at most $[K : \mathbf{Q}(x_1, ..., x_n)]$ hence finite. This implies that for any n there exists an algebraic number $\omega \in \overline{\mathbf{Q}}$ of degree $n + 1$ over $\mathbf{Q}$ which retains the degree $n + 1$ over F_1. For this ω the statement in the theorem holds true as a consequence of Theorem 1.

REFERENCES

[1] JACOBSON, N. *Lectures in Abstract Algebra, vol. III.* Graduate Texts in Mathematics, Springer Verlag.

[2] LANG, S. *Introduction to Algebraic Geometry.* New York-London, Interscience, 1958.

[3] MOTZKIN, T. S. Evaluation of polynomials and evaluation of rational functions. *Bull. Amer. Math. Soc. 61* (1955), p. 163.

[4] REINGOLD, E. M. and A. I. STOCKS. Simple proofs of lower bounds for polynomial evaluation. *In: Complexity of Computer Computations*, R. Miller, J. Thatcher (Editors), Plenum Press, New York-London, 1972, pp. 21-30.

[5] STRASSEN, V. Berechnung und Programm I. *Acta Informatica 1* (1972), pp. 320-335.

[6] WINOGRAD, S. On the number of multiplications necessary to compute certain functions. *Communications on pure and appl. Math. 23* (1970), pp. 165-179.

(Reçu le 15 juillet 1980)

Walter Baur

Seminar für Angew. Math.
Universität Zürich
Freiestrasse 36
CH-8032 Zürich

Michael O. Rabin

Dept. of Mathematics
Hebrew University
Jerusalem, Israel