

4. Applications

Objektyp: **Chapter**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **26 (1980)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **25.09.2024**

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.

Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.

Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

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. Abbreviating $x = x_1, \dots, x_n$, $y = y_1, \dots, y_k$, consider $\Omega = \overline{F(x, y)}$, $K = \overline{F(x)}$, $E = \overline{F(y)}$. Then E and K are linearly disjoint over \overline{F} (see e.g. [1], p. 203).

Taking $k = 1$, $e_i = y_1^i$, $1 \leq i \leq n$, we see that any computation of $f(y_1) = x_1 y_1 + \dots + x_n y_1^n$ in $(\Omega, E \cup K)$ requires $\lceil \frac{n}{2} \rceil M/D$ that count even if we disregard a M/D by an element $g \in \overline{F}$. Thus any preprocessing using algebraic functions α_1, \dots in x and algebraic functions β_1, \dots in y , cannot save more than $\frac{n}{2} M/D$.

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

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

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

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

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

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

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

$$(8) \quad x_1 v_1 + \dots + x_n v_n = w.$$

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

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

Hence, from (8),

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

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

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

Because v_1, \dots, v_n are linearly independent mod F^m over F , we have that w_1, \dots, w_n are linearly independent over F . Consider the sum $Z_1 w_1 + \dots + Z_n w_n$, where Z_1, \dots, 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

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

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

We claim that among the $L_{ij}(Z)$, $1 \leq i \leq m, 1 \leq j \leq p$, 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 $h_1, \dots, h_n \in F$, not all 0, so that the substitution $Z_1 = h_1, \dots, Z_n = h_n$ yields $L_{ij}(h) = 0, 1 \leq i \leq m, 1 \leq j \leq p$. By (9) we now have $h_1 w_1 + \dots + h_n w_n = 0$, contradicting the linear independence of w_1, \dots, w_n over F .

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

$$L_{i_e j_e}(Z_1, \dots, Z_n) = d_{i_e j_e}, \quad 1 \leq e \leq n.$$

Thus, finally

$$(10) \quad x_1 w_1 + \dots + x_n w_n = [d_{i_1 j_1} e_1 + \dots + d_{i_p j_p} e_p]_{1 \leq i \leq m}$$

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

For the next application let x_1, \dots, x_n be algebraically independent over F and put $\Omega = \overline{F(x_1, \dots, x_n)}, E = \overline{F}, K = F(x_1, \dots, x_n)$. 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

$$(11) \quad \omega x_1 + \dots + \omega^n x_n$$

in $(\Omega, E \cup K)$ requires at least $\lceil \frac{n}{2} \rceil M/D$. 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, \dots, 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, \dots, x_n by algebraic functions involve just a finite number of such functions, we essentially conclude that algebraic preprocessing of x_1, \dots, 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 $\lceil \frac{n}{2} \rceil$. Specifically

THEOREM 3. *Let*

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

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

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

$$\begin{array}{ccc} \overline{\mathbf{Q}(x_1, \dots, x_n)} & & \\ \cup & \cup & \\ \bar{\mathbf{Q}} & & K \\ \cup & \cup & \\ F_1 = \bar{\mathbf{Q}} \cap K & & \\ \cup & & \\ F = \mathbf{Q} & & \end{array}$$

Notice that $\bar{\mathbf{Q}} = \bar{F}_1$ and $\bar{F}_1 \cap K = F_1$. This implies that $\bar{\mathbf{Q}}$ and K are linearly disjoint over F_1 . Namely let $e_1, \dots, e_q \in \bar{F}_1$ be independent over F_1 . Choose a primitive element $e \in \bar{F}_1$, of degree m over F say, such that $e_1, \dots, e_q \in F_1(e)$, 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 $1, e, \dots, e^{m-1}$ are linearly independent over K . By linear algebra it follows that e_1, \dots, e_q are linearly independent over K .

The degree $[F_1 : \mathbf{Q}]$ is at most $[K : \mathbf{Q}(x_1, \dots, x_n)]$ hence finite. This implies that for any n there exists an algebraic number $\omega \in \bar{\mathbf{Q}}$ 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.