Zeitschrift: L'Enseignement Mathématique
Herausgeber: Commission Internationale de l'Enseignement Mathématique
Band: 26 (1980)
Heft: 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

Artikel: LINEAR DISJOINTNESS AND ALGEBRAIC COMPLEXITY
Autor: Baur, Walter / Rabin, Michael O.
Kapitel: 4. Applications
DOI: https://doi.org/10.5169/seals-51078

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 $A = (a_{ij})_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}}$ 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* $\lceil \frac{r}{2} \rceil$ 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 $r < j \leqslant n$

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

Hence, from (8),

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

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

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

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

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

Thus, finally

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

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 **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*

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

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

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

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 $e_1, \ldots, e_q \in \bar{F}_1$ be independent over F_1. Choose a primitive element $e \in \bar{F}_1$, of degree m over F say, such that $e_1, \ldots, e_q \in F_1(e)$, 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 $1, e, \ldots, e^{m-1}$ are linearly independent over K. By linear algebra it follows that $e_1, \ldots, e_q$ are linearly independent over K.

The degree $[F_1 : \mathbf{Q}]$ is at most $[K : \mathbf{Q}(x_1, \ldots, x_n)]$ 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.