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: 2. Basic concepts and the Main Theorem

DOI: https://doi.org/10.5169/seals-51078

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

$$
\begin{array}{lccc}
 & & \Omega & \\
 & \cup\!| & & |\!\cup \\
(3) \qquad & E & & K \\
 & |\!\cup & & \cup\!| \\
 & & F &
\end{array}
$$

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*

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

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 pre-processing 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

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

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 $e_1, \ldots, e_p \in K$ are linearly independent mod F over F and similarly for $d_1, \ldots, d_p \in K$, 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 $1, x, \ldots, x^{n-1}$ of E remains linearly independent over K. Hence, by linear algebra, E and K are linearly disjoint over F. Consider the element

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

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