TESTING POLYNOMIALS WHICH ARE EASY TO COMPUTE

(Extended Abstract)

J. Heintz and C.P. Schnorr

Fachbereich Mathematik
Universität Frankfurt

Abstract We exploit the fact that the set of all polynomials $P \in \mathbb{K}[x_1,..,x_n]$ of degree $\leq d$ which can be evaluated with $\leq v$ nonscalar steps can be embedded into a Zariski-closed affine set $W(d,n,v)$, $\dim W(d,n,v) \leq (v+1+n)^2$ and $\deg W(d,n,v) \leq (2vd)^{(v+1+n)^2}$. As a consequence we prove that for $u := 2v(d+1)^2$ and $s := 6(v+1+n)^2$ there exist $\underline{a}^1,..,\underline{a}^s \in [u]^n = \{1,2,..,u\}^n$ such that for all polynomials $P \in W(d,n,v): P(\underline{a}^1) = P(\underline{a}^2) = \ldots = P(\underline{a}^s) = 0$ implies $P \equiv 0$. This means that $\underline{a}^1,\ldots,\underline{a}^s$ is a correct test sequence for a zero test on all polynomials in $W(d,n,v)$. Moreover, "almost every" sequence $\underline{a}^1,..,\underline{a}^s \in [u]^n$ is such a correct test sequence for $W(d,n,v)$. The existence of correct test sequences $\underline{a}^1,..,\underline{a}^s \in [u]^n$ is established by a counting argument without constructing a correct test sequence. We even show that it is beyond the known methods to establish (i.e. to construct and to prove correctness) of such a short correct test sequence for $W(d,n,v)$. We prove that given such a short, correct test sequence for $W(d,n,v)$ we can efficiently construct a multivariate polynomial $P \in \mathbb{K}[x_1,..,x_n]$ with $\deg(P) = d$ and small integer coefficients such that $P \notin W(d,n,v)$. For $v > n \log d$ lower bounds of this type are beyond our present methods in algebraic complexity theory.

1. Introduction and Preliminaries

There is already a respectable list of applications of Bezout's theorem in complexity theory. Straßen (1972) proved that the evaluation of all elementary symmetrical functions of n variables requires $\Omega(n \log n)$ nonscalar steps. Straßen's method has been extended by Schnorr (1979) to single multivariate polynomials, e.g. $L_{ns}(\Sigma_{i=1}^n x_i^d y_i) \geq \frac{1}{2} n \log d$ provided $n \leq \sqrt{d}$. Heintz and Sieveking (1978) established new lower bounds on the complexity of univariate polynomials with algebraic coefficients, e.g. $L_{ns}(\Sigma_{j=1}^d 2^{1/j} x^j) = \Omega(\sqrt{\frac{d}{\log d}})$, see von zur Gathen and Straßen (1979) for additional examples. Mignotte and Morgenstern (1979) observed $L_{ns}(\Sigma_{j=1}^d \sqrt{p_j} x^j) = \Omega(\sqrt{\frac{d}{\log d}})$ for pairwise distinct prime numbers p_j. Heintz (1979) proved good upper bounds on the number of solutions of first order formulae in the theory of algebraic closed fields. In this paper we establish a connection between lower bound proofs for the complexity of polynomial evaluation and the problem of testing polynomial identities. Indeed the same methods are involved in both problems which shows that the

methods for proving lower bounds might be useful in some other, even more practical context as well.
We give examples of the powerful and elegant counting method which derives from Bezout's theorem. Because of its large and easy applicability and its concise formulation Bezout's inequality might be useful even for non experts in algebraic geometry. Indeed for our applications of Bezout's theorem we only need some very basic facts of the highly developed machinery of modern algebraic geometry.

For a multivariate polynomial $P \in \mathbb{K}[x_1,..,x_n]$ let $L_{ns}(P)$ be the minimal number of nonscalar steps which are necessary to evaluate P. By the methods of Schnorr (1978) and Heintz and Sieveking (1978) the set

$$\{P \in \mathbb{K}[x_1,..,x_n] \mid \deg P \leq d, L_{ns}(P) \leq v\}$$

can be embedded into a (Zariski-)closed set W(d,n,v) such that (1) W(d,n,v) is definable over $\mathbb{Q}$, (2) $\dim W(d,n,v) \leq (v+1+n)^2$, $\deg W(d,n,v) \leq (2vd)^{(v+1+n)^2}$. Using this <u>basic theorem</u> and Bezout's inequality one obtains lower bounds on polynomials with algebraic coefficients. We also derive a rather elegant proof for

$$\max\{L_{ns}(\Sigma_{i=0}^{d} a_i x^i) \mid a_i \in \{0,1\}\} \geq \sqrt{\tfrac{2}{3}d/\log d} - 1$$

which avoids the lengthy calculations used in Schnorr (1978). Moreover, this proof shows that the bound $\sqrt{\frac{2}{3}d/\log d}-1$ is achieved for "almost all" $(a_0,..,a_d) \in \{0,1\}^{d+1}$.

Another application of the basic theorem concerns the following problem: given a short computation for $P \in \mathbb{K}[x_1,..,x_n]$, decide whether $P \equiv 0$. Suppose $\deg P \leq d$ then it can easily be seen that for every $A \subset \mathbb{K}$, A finite:

$$\#\{\underline{x} \in A^n \mid P(\underline{x}) = 0\} \leq d(\#A)^{n-1} \text{ provided } P \not\equiv 0$$

This gives raise to a random decision procedure for $P \equiv 0$ since

$$\text{prob}\{\underline{x} \in A^n \mid P(\underline{x}) = 0\} \leq d/\#A \quad \text{provided } P \not\equiv 0$$

with respect to the uniform distribution on A^n, see Schwarz (1979). It is an interesting open problem whether in this case there is an efficient deterministic algorithm that tests $P \equiv 0$. Lovász (1979) gave a particularly interesting example of this situation showing that the (linearly represented) matroid parity problem can be solved by deciding whether a given determinant with polynomial entries is identical zero. The basic theorem implies that given any $u \geq 2v(d+1)^2$ and $s \geq 6(v+1+n)^2$ there exist $\underline{a}^1,..,\underline{a}^s \in [u]^n$, $[u] := \{1,2,..,u\}$ such that for all $P \in W(d,n,v)$: $P(\underline{a}^1) = P(\underline{a}^2) = \ldots = P(\underline{a}^s) = 0$ implies $P \equiv 0$. This means that $\underline{a}^1,..,\underline{a}^s$ is a <u>correct test sequence</u> for zero testing all polynomials in W(d,n,v). Moreover, "almost every" sequence $\underline{a}^1,..,\underline{a}^s \in [u]^n$ forms such a correct sequence of test points for W(d,n,v). This statement sounds much like Adleman's (1978) observation that every problem which is decidable in random polynomial time has polynomially bounded network size. However, in our situation Adleman's argument is not applicable since W(d,n,v) is not finite but $\dim W(d,n,v) = \Omega(v+n)^2$. Observe that in our computations arbitrary constants in $\mathbb{K}$ are given for free. Of course Adleman's argument can be applied if we restrict the computations such that only a fixed finite set of constants is given for free and if we count all arithmetical operations. In this case the number of polynomials computable with $\leq v$ scalar + nonscalar operations is at most $2^{O(v \log v)}$.

On the other hand we give evidence that it is beyond our present proof methods to establish for given d,n,v a specific correct test sequence $\underline{a}^1,..,\underline{a}^s \in [u]^n$ for W(d,n,v) with s,u polynomially bounded in d+n+v. We prove that given such a correct test sequence for W(d,n,v) we can efficiently construct a multivariate polynomial $P \in \mathbb{K}[x_1,..,x_n]$ with deg $P \leq d$ such that P has only small integer coefficients (P even has $\leq s+1$ coefficients $\neq 0$) and $P \notin W(d,n,v)$. Lower bound proofs of this type are beyond our present methods in algebraic complexity theory. The best we can prove so far are lower bounds for polynomials with rapidly increasing integer coefficients, e.g. $L_{ns}(\Sigma_{i=0}^{d} 2^{2^i} x^i) = \Omega(\sqrt{d/\log d})$ and lower bounds with small integer coefficients which are not much greater than the number of indeterminates, e.g. $L_{ns}(\Sigma_{i=1}^{n} x_i^d y^i) \geq \frac{1}{2} n \log d$ with $n < d^{1/4}$, see Schnorr (1979).

Throughout the paper $\mathbb{K}$ is an algebraic closed field with prime field $\mathbb{Q}$ and let $\mathbb{K}_0 \subset \mathbb{K}$ be some subfield. $x_1,..,x_n,y,y_i,z_i$ are indeterminates over $\mathbb{K}_0$. $\mathbb{K}_0[x_1,..,x_n]$ is the ring of multivariate polynomials in the indeterminates $x_1,..,x_n$ with coefficients in $\mathbb{K}_0$. $\mathbb{K}_0(x_1,..,x_n)$ is the field of rational functions in the indeterminates $x_1,..,x_n$. $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are the sets of natural, integer, rational, real and complex numbers. log n is the logarithm of n to base 2. #A denotes the cardinality of set A. We use $f(n) = \Omega(g(n))$ as an abbreviation for $\exists c \in \mathbb{N}: \forall n: c \cdot f(n) > g(n)$. Tuples are underlined, e.g. $\underline{x} = (x_1,..,x_n)$. We abbreviate $\underline{x}^{\underline{j}} := \Pi_{i=1}^{n} x_i^{j_i}$ and $(\underline{x}-\underline{\eta})^{\underline{j}} = \Pi_{i=1}^{n} (x_i-\eta_i)^{j_i}$, $|\underline{j}| = j_1+j_2+...+j_n$. For $u \in \mathbb{N}$ let $[u] := \{1,2,..,u\}$.

2. A useful bound on the degree of (Zariski)-closed sets

In this section we introduce notions from algebraic geometry. In order to make the paper understandable for readers without prior knowledge in algebraic geometry we present all concepts and facts to be used. For convenience we will work with affine closed sets. Our main tool is the Bezout inequality for the degree of affine closed sets. In proposition 2.3 we establish a bound on the degree of closed sets which lateron will be applied in many situations.

A subset $E \subset \mathbb{K}^n$ is called (Zariski-)closed (over $\mathbb{K}_0$) if it is definable as the set of common zero's of some set of polynomials $B \subset \mathbb{K}_0[x_1,..,x_n]$, i.e.

$$E = \{\underline{a} \in \mathbb{K}^n \mid \forall P \in B: P(\underline{a}) = 0\}.$$

These closed sets are called definable over $\mathbb{K}_0$ since they are defined by polynomials with coefficients in $\mathbb{K}_0$. Note that an arbitrary intersection and a finite union of closed sets is closed. These closed sets define the Zariski-topology of $\mathbb{K}^n$. The closure $\bar{A}$ of a set $A \subset \mathbb{K}^n$ is the intersection of all closed sets E that contain A, or equivalently, $\bar{A}$ is the smallest closed set containing A. A closed set $E \subset \mathbb{K}^n$ is called a hypersurface (hyperplane, resp.) if it is definable by a single polynomial (single linear polynomial, resp.)

A closed set $E \subset \mathbb{K}^n$ is called irreducible (E is then called a variety) if there do not exist closed sets E_1,E_2 such that $E = E_1 \cup E_2$ and $E_1,E_2 \neq E$. The irreducible closed sets $E \subset \mathbb{K}^n$ are exactly those sets $E \subset \mathbb{K}^n$ which are definable as the sets of zero's of a prime ideal $B \subset \mathbb{Z}[x_1,..,x_n]$. Each closed set E is a finite union of irreducible closed sets, $E = \bigcup_i C_i$. This representation of E is unique, if it is not redundant, i.e. if $C_i \not\subseteq C_j$ for $i \neq j$. Therefore the C_i appearing in this representation of E are called components of E. The dimension dim E of a closed set $E \subset \mathbb{K}^n, E \neq \emptyset$ is the maximal integer m such that there exist distinct irreducible closed sets $Z_1,..,Z_m$ such that $\emptyset \neq Z_1 \subset Z_2 \subset .. Z_m \subset E$. Every closed set

$E \neq \emptyset$ has a finite dimension. We have dim $\mathbb{K}^n = n$. The zero dimensional closed subsets of $\mathbb{K}^n$ are finite. The dimension of a hypersurface $H \subset \mathbb{K}^n$ is n-1. This definition immediately implies

Fact 2.1 Let E,D be closed sets, E irreducible and $E \not\subset D$, then $\dim(E \cap D) < \dim E$.

The degree deg E of an irreducible closed set $E \subset \mathbb{K}^n$ is the maximal cardinality of a finite set which is obtained by intersecting E with a linear affine subspace

$$\deg E := \max\{\#(E \cap L) < \infty \mid L \subset \mathbb{K}^n \text{ affine linear subspace}\}$$

Following Heintz (1979) we extend this definition to reducible closed sets as

$$\deg E := \sum_{C \text{ component of } E} \deg C$$

Every closed set $E \neq \emptyset$ has a finite degree.

Our main tool in applying algebraic geometry is Bezout's inequality for the degree of affine varieties. The corresponding Bezout equality with respect to projective varieties can be found in Kendig p.207 and Van der Waerden p.177. The Bezout inequality for affine varieties follows from Bezout's equality for projective varieties, as is shown in the appendix of Schnorr (1979), [10]. Heintz (1979) has given a direct proof, based on commutative algebra. Our formulation of Bezout's inequality avoids the quite complicated notion of intersection multiplicity. We hope that this will facilitate applications by non experts.

Bezout's inequality

Let $E, D \subset \mathbb{K}^n$ be closed sets, then $\deg(E \cap D) \leq \deg E \cdot \deg D$.

We shall also use the theorem on the dimension of fibres:

Theorem 2.2 (Schafarewitch, p.69)

Let E,D be closed sets, E irreducible and let $f: E \to D$ be a regular map, dim E=n, dim D=m, $n \geq m$. Then for all $y \in f(E)$: $\dim f^{-1}(y) \geq n-m$.

Proposition 2.3 Let $E_i \subset \mathbb{K}^n$ i=1,..,r

be closed sets, then $\deg \bigcap_{i \leq r} E_i \leq \deg E_1 (\max_{i>1} \deg E_i)^{\dim E_1}$.

Proof We proceed by induction on r. The case r=1 is trivial, we introduce $E_2 := \mathbb{K}^n$, thus $\max_{i>1} \deg E_i = 1$. Now let C_ν $\nu \in J$ be the components of E_1. It suffices to prove under the induction hypothesis for r-1 that

$$\deg(C_\nu \cap \bigcap_{1<i\leq r} E_i) \leq \deg C_\nu (\max_{i>1} \deg E_i)^{\dim C_\nu} \quad \text{for } \nu \in J.$$

In the case $C_\nu \subset E_2$, the intersection with E_2 has no effect and we are already in the case r-1. In the case $C_\nu \not\subset E_2$ we apply the induction hypothesis to $E_1' := C_\nu \cap E_2$. Since $\dim(C_\nu \cap E_2) < \dim C_\nu$ Bezout's inequality and the induction hypothesis yield

$$\deg(C_\nu \cap \bigcap_{1<i\leq r} E_i) \leq \deg(C_\nu \cap E_2) \max_{i>2}(\deg E_i)^{\dim C_\nu - 1} \leq \deg C_\nu \cdot (\max_{i>1} \deg E_i)^{\dim C_\nu}.$$ ∎

3. The closed sets of all polynomials which are easy to compute

Following the methods of Schnorr (1978) and Heintz and Sieveking (1978) we can embed the set of all polynomials $P \in \mathbb{K}[x_1,..,x_n]$ with deg $P \leq d$ and computable with $\leq v$ nonscalar steps into a closed set $W(d,n,v)$ with small dimension and small degree. We reformulate this basic theorem and give some illuminating examples for its application.

A straight-line computation over $\mathbb{K} \cup \{x_1,..,x_n\}$ is a sequence of rational functions $R_1,..,R_w \in \mathbb{K}(x_1,..,x_n)$ such that for $i=1,..,w$ either (1) $R_i \in \mathbb{K} \cup \{x_1,..,x_n\}$ or (2) $R_i = R_j \circ R_k$ with $j,k<i$ and $\circ \in \{+,-,*,/\}$. $R_1,..,R_w$ are the results of the computation. A "computation step" $R_i = R_j \circ R_k$ is called nonscalar provided (1) $\circ$ is * and $R_j, R_k \notin \mathbb{K}$ or (2) $\circ$ is / and $R_k \notin \mathbb{K}$. For $P \in \mathbb{K}(x_1,..,x_n)$ let $L_{ns}(P)$ be the minimal number of nonscalar steps in any computation of P over $\mathbb{K} \cup \{x_1,..,x_n\}$.

The following is a straightforward extension of theorem 2.1 in Schnorr (1978) from one indeterminate x to n indeterminates $x_1,..,x_n$. The theorem means that the coefficients $a_{\underline{j}}$ of all polynomials $P \in \mathbb{K}[x_1,..,x_n]$ with $L_{ns}(P) \leq v$ can be represented as the values of polynomials $Q^v_{\underline{j}}$ with small degree and depending on $O(v^2)$ indeterminates in total.

Theorem 3.1 (Schnorr 1978, theorem 2.1)
For every $v \in \mathbb{N}$ there exist polynomials $Q^v_{\underline{j}} \in \mathbb{Z}[z_1,..,z_m]$ for $\underline{j} \in \mathbb{N}^n$ with $m = (v+1+n)^2-1$ deg $Q^v_{\underline{j}} \leq 2^{|\underline{j}|} v$ such that for every $P \in \mathbb{K}(x_1,..,x_n)$ with $L_{ns}(P) \leq v$ there exists a hypersurface $H \subset \mathbb{K}^n$ such that for all $\underline{\eta} \in \mathbb{K}^n - H$ there exist $a_{\underline{j}}(\underline{\eta}) \in \mathbb{K}$ with

$$P \equiv \sum_{\underline{j} \in \mathbb{N}^n} a_{\underline{j}}(\underline{\eta}) (\underline{x}-\underline{\eta})^{\underline{j}} \quad \text{and} \quad (a_{\underline{j}}(\underline{\eta}) : |\underline{j}|>0) \in \mathrm{Im}(Q^v_{\underline{j}} : |\underline{j}|>0).$$

Here $\mathrm{Im}(Q^v_{\underline{j}}:|\underline{j}|>0)$ is the image of the map on $\mathbb{K}^m$ defined by the $Q^v_{\underline{j}}, |\underline{j}|>0$.

Following Heintz and Sieveking (1978) this rather complicated theorem gives raise to a concise statement in terms of Zariski-closed sets. We identify a polynomial $P \in \mathbb{K}[x_1,..,x_n]$ with deg $P \leq d$ with its coefficient vector in $\mathbb{K}^t$, $t := \binom{n+d}{n}$.

Basic theorem 3.2 (Heintz, Sieveking 1978)
For every $d,n,v \in \mathbb{N}$ there exists a closed set $W(d,n,v) \subset \mathbb{K}^t$, definable over $\mathbb{Q}$, $t = \binom{n+d}{d}$ such that
(1) $W(d,n,v)$ contains all $P \in \mathbb{K}[x_1,..,x_n]$ with deg $P \leq d$ and $L_{ns}(P) \leq v$
(2) $\dim W(d,n,v) \leq (v+1+n)^2$ deg $W(d,n,v) \leq (2vd)^{(v+1+n)^2}$

Proof Take the polynomials $Q^v_{\underline{j}}$ of the above theorem and set $Q^v_{\underline{0}} = z_o$ (let $\underline{0} = (0,..,0) \in \mathbb{N}^n$) with an additional variable z_o. Then define

$$W(d,n,v) := \overline{\mathrm{Im}(Q^v_{\underline{j}}:|\underline{j}| \leq d)}$$

i.e. $W(d,n,v)$ is the closure of the image of the $Q^v_{\underline{j}}$. Theorem 3.1 immediately implies that (1) holds. Observe that the restriction on the point of development $\underline{\eta}$ in theorem 3.1 has been eliminated in theorem 3.2 by reasons of continuity. We can always choose $\underline{\eta}=\underline{0}$ since $W(d,n,v) \subset \mathbb{K}^t$ is closed. Obviously $\dim W(d,n,v) \leq (v+1+n)^2$ since the $Q^v_{\underline{j}}$ with $|\underline{j}| \leq d$ only depend on $(v+1+n)^2$ indeterminates. Thus the crucial point is to prove the degree bound on $W(d,n,v)$. We refer the reader to the Lemma in Heintz and Sieveking (1978). ∎

Next we consider the maximal nonscalar complexity of univariate polynomials of degree $\leq d$ with 0,1-coefficients:

$C^{ns}_{0,1}(d) := \max\{L_{ns}(\Sigma_{i=0}^{d} a_i x^i) \mid (a_0,..,a_d) \in \{0,1\}^{d+1}\}$

By rather lengthy calculations we obtained lower bounds

$C^{ns}_{0,1}(d) \geq \sqrt{d}/(4 \log d)$ (Schnorr 1978) and

$C^{ns}_{0,1}(d) \geq \frac{1}{4}\sqrt{d/\log(2d)}-3$ (Schnorr, Van de Wiele 1978).

We now give an elegant proof for a better result.

Corollary 3.3

(1) $\#\{(a_0,..,a_d) \in \{0,1\}^{d+1} \mid L_{ns}(\Sigma_{i=0}^{d} a_i x^i) \leq \sqrt{\frac{2}{3}\frac{d}{\log d}} - 2\} \leq 2^{d-\sqrt{\frac{2}{3} d \log d}}$

(2) $C^{ns}_{0,1}(d) \geq \sqrt{\frac{2}{3}\frac{d}{\log d}} - 1$

Proof We use proposition 2.3 and theorem 3.2 to bound $\#(W(d,1,v) \cap \{0,1\}^{d+1})$. $\{0,1\}^{d+1}$ is the intersection of hypersurfaces H_i which are defined by $z_i(z_i-1) = 0$ for $i=1,..,d+1$. Applying proposition 2.3 to $E_1 := W(d,1,v)$ and $E_{1+i} := H_i$ $i=1,..,d+1$ we obtain

$\#(W(d,1,v) \cap \{0,1\}^{d+1}) \leq \deg W(d,1,v) \cdot 2^{\dim W(d,1,v)} \leq (2vd)^{(v+1)(v+2)} 2^{(v+1)(v+2)} = (4vd)^{(v+1)(v+2)}$

In order to prove (1) it is sufficient to verify:

$$v \leq \sqrt{\frac{2}{3}\frac{d}{\log d}} - 2 \text{ and } d \geq 2 \text{ imply } (v+1)(v+2)\log(4vd) \leq d - \sqrt{\tfrac{2}{3} d \log d}. \qquad \blacksquare$$

It turns out that the lower bounds on specific polynomials with algebraic coefficients in Heintz and Sieveking (1978) and von zur Gathen and Straßen (1979) can be obtained in the same way. Following Mignotte and Morgenstern we obtain:

Corollary 3.4 $L_{ns}(\Sigma_{j=0}^{d} \sqrt{p_j} x^j) \geq \sqrt{\frac{2}{3}\frac{d}{\log d}} - 1$,

for any choice of pairwise distinct primes p_j.

The proof is similar to the proof of Corollary 3.3. In this case we intersect $W(d,1,v)$ with $V := (\sqrt{p_0},.., \sqrt{p_d})$ which consists of all conjugates of $(\sqrt{p_0},.., \sqrt{p_d})$. V is defined by the equations $p_i - z_i^2 = 0$ $i = 0,..,d$ and the points in V define equally hard polynomials.

In the same way one proves $L_{ns}(\Sigma_{i=0}^{d} p_i^{1/d} x^i) \geq \sqrt{d/2.5}-2$

for pairwise distinct primes p_i. This lower bound is sharp up to a constant factor. The corresponding upper bound is known from Paterson, Stockmeyer (1973).

The above methods apply to other complexity measures as well. For instance they can be used (1) if we count additions/subtractions no matter how many multiplications/divisions are used (2) if we separately count additions/subtractions and nonscalar steps (3) if we count the total number of arithmetical operations. This is a consequence of the representations of the polynomials which are easy to compute given in Schnorr and Van de Wiele (1978).

Another extension of these results concerns the approximate evaluation of polynomials. Let ϱ be the Cartesian distance on $\mathbb{K}^{d+1}$, $\mathbb{K} := \mathbb{C}$. Since $W(d,n,v)$ is topologically closed

with respect to ρ it follows that $W(d,n,v)$ contains all polynomials which can be approximately evaluated with $\leq v$ nonscalar steps, i.e. for n=1:

$$\{P \in \mathbb{C}^{d+1} \mid \forall \varepsilon>0: \exists P_\varepsilon \in W(d,1,v): \rho(P,P_\varepsilon)<\varepsilon\} \subset W(d,1,v)$$

Hence there exists $\varepsilon>0$ such that every approximate evaluation of $\sum_{i=0}^{d} p_i^{1/d} x^i$ which for all $a \in \mathbb{C}$ with $|a| \leq 1$ has an error $<\varepsilon$, requires $\sqrt{d/2.5}-2$ nonscalar steps.

4. On the verification of polynomial identities

We consider the following problem: given a short computation for a polynomial $P \in \mathbb{K}[x_1,..,x_n]$, decide whether $P \equiv 0$.
Schwartz (1979) suggested a probabilistic algorithm in the spirit of the Rabin, Solovay, Straßen primality test: choose random values $\underline{a}^i \in \mathbb{K}^n$ i=1,..,s and check whether $P(\underline{a}^i) = 0$ for i=1,..,s. Of course we like to draw the $\underline{a}^i$ out of a domain where P can be evaluated efficiently and where P has not too many zero's provided $P \not\equiv 0$. The following Lemma may be helpful.

Lemma 4.1 Suppose $P \in \mathbb{K}[x_1,..,x_n]$, deg $P \leq d$ and let $E_i \subset \mathbb{K}^n$ i=1,..,r be closed sets, deg $E_i \leq m$ and let $E := \bigcap_{i \leq r} E_i$ be finite. Then $\#\{\underline{x} \in E \mid P(\underline{x}) = 0\} \leq dm^{n-1}$ provided $P \not\equiv 0$.

Proof If $P \not\equiv 0$ then P defines a hypersurface $H_P \subset \mathbb{K}^n$ over $\mathbb{K}$ with dim $H_P = n-1$, deg $H_P \leq d$. Then by proposition 2.3 we have $\#\{\underline{x} \in E \mid P(\underline{x}) = 0\} = \deg(H_P \cap \bigcap_{i \leq r} E_i) \leq dm^{n-1}$. ■

In particular the bound of Lemma 4.1 applies to direct products $E = I_1 \times I_2 \times .. \times I_n$ with $\#I_i \leq m$. In this case E is the intersection of hypersurfaces $H_i \subset \mathbb{K}^n$ defined by

$$\prod_{a \in I_i} (x_i - a) = 0 \quad \text{for} \quad i=1,\ldots,n.$$

However, in this special case, Lemma 4.1 can be proved by elementary induction, see Schwartz (1979).

We shall discuss whether the probabilistic choice of test points $\underline{a}^1,\ldots,\underline{a}^s \in \mathbb{K}^n$ is appropriate or whether we can find a universal set of test points for a correct 0-test over large classes of polynomials. We call $\underline{a}^1,..,\underline{a}^s \in \mathbb{K}^n$ a correct test sequence for $U \subset \mathbb{K}[x_1,\ldots,x_n]$ iff $\forall P \in U$: $P(\underline{a}^1) = \ldots = P(\underline{a}^s) = 0$ implies $P \equiv 0$.
Kroneckers method yields a correct single test point for polynomials $P \in \mathbb{Z}[x_1,..,x_n]$ with bounded weight and bounded degree. The weight w(P) is the sum of the absolute values of the coefficients of P.

Lemma 4.2 (Kronecker) Let $P \in \mathbb{Z}[x_1,..,x_n]$, $w(P) \leq m$, deg $P \leq d$ then

$P(2m,(2m)^d,(2m)^{d^2},\ldots,(2m)^{d^{n-1}}) = 0$ implies $P \equiv 0$. ■

Unfortunately a test point $(2m,(2m)^d,\ldots,(2m)^{d^{n-1}})$ as in Lemma 4.2 is impractical since this test point has exponentially binary length $d^{n-1}\log(2m)$ and we do not know any efficient method for verifying $P(2m,(2m)^d,..,(2m)^{d^{n-1}}) = 0$. However this can efficiently be verified by a random algorithm which randomly choosed small prime numbers $p_1,..,p_s$ and checks whether $P(2m,..,(2m)^{d^{n-1}}) \equiv 0 \bmod p_i$ for i=1,..,s. Surprisingly we can establish nice test points with algebraic coefficients which are correct for all polynomials $P \in \mathbb{Q}[x_1,..,x_n]$ with bounded degree:

Lemma 4.3 Let $U(d,n) := \{P \in \mathbb{Q}[x_1,..,x_n] \mid \deg P \leq d\}$.
Then every choice of pairwise distinct primes $p_1,..,p_n \in \mathbb{N}$ yields a correct test point $(p_1^{1/(d+1)},..,p_n^{1/(d+1)})$ for $U(d,n)$.

Proof by contradiction. Suppose $P \neq 0$ and $P(p_1^{1/(d+1)},..,p_n^{1/(d+1)}) = 0$.

Let $V := \overline{(p_1^{1/(d+1)},..,p_n^{1/(d+1)})}$ be the closure of $(p_1^{1/(d+1)},..,p_n^{1/(d+1)})$ with respect to the closed sets definable over $\mathbb{Q}$. V consists of all conjugates of $(p_1^{1/(d+1)},..,p_n^{1/(d+1)})$. Clearly $\#V = (d+1)^n$ and V is contained in the intersection of the hypersurfaces $H_i \subset \mathbb{K}^n$ which are defined by $p_i - x_i^{d+1} = 0$ for $i=1,..,n$. Let H_P be the hypersurface defined by P, then $\dim H_P = n-1, \deg H_P \leq d$.

Hence $V \subset H_P \cap \bigcap_{i=1}^{n} H_i$ and Proposition 2.3 implies $\#V \leq \deg H_P \cdot (d+1)^{n-1} < (d+1)^n$ which yields a contradiction to $\#V = (d+1)^n$. ∎∎

Presumably the test point of Lemma 4.3 is impractical, too. We do not know an efficient method for verifying whether $P(p_1^{1/(d+1)},..,p_n^{1/(d+1)}) = 0$. Thus the question remains whether there exist "practical" correct test points. There cannot exist "practical" test sequences $\underline{a}^1,..,\underline{a}^d \in \mathbb{Q}^n$ of length d which are correct for all $P \in \mathbb{K}[x_1,..,x_n], \deg P \leq d$ which are easy to compute. Observe that such a test sequence is falsified by the simple polynomial $\prod_{i=1}^{d}(x_1 - a_1^i)$. Nevertheless we shall establish the existence of short, practical and correct test sequences for all polynomials which are easy to compute, i.e. test sequences which are correct for the classes $W(d,n,v)$.

Theorem 4.4 For every $v,d \in \mathbb{N}$ and for $u := 2v(d+1)^2$ and $s := 6(v+1+n)^2$ the number of correct test sequences $(\underline{a}^1,..,\underline{a}^s) \in [u]^{ns}$ for $W(d,n,v)$ is at least $u^{ns}(1-u^{-s/6})$.

Proof Let $t := \binom{n+d}{d}$ and for all $P \in \mathbb{K}[x_1,..,x_n]$ with $\deg P \leq d$ identify P with its coefficient vector in $\mathbb{K}^t$. Then

$$V(d,n,v,s) := \left\{ (\underline{a}^1,..,\underline{a}^s,P) \in \mathbb{K}^{ns+t} \;\middle|\; \begin{array}{l} P \in W(d,n,v) \\ \forall \nu \leq s : P(\underline{a}^\nu) = 0 \end{array} \right\}$$

is a closed set definable over $\mathbb{Q}$. Let $x_{i,\nu}$ $i=1,..,n, \nu=1,..,s$ and $z_{\underline{\mu}}, |\underline{\mu}| \leq d$ be the coordinates of $\mathbb{K}^{ns+t}$. Then $V(d,n,v,s)$ is defined by the polynomial equations defining $W(d,n,v)$ together with the following equations of degree d+1:

$$\sum_{|\underline{\mu}| \leq d} z_{\underline{\mu}} \prod_{i=1}^{n} x_{i,\nu}^{\mu_i} = 0 \qquad \nu = 1,\ldots,s$$

By Bezout's inequality and Theorem 3.2 we have

$$\deg V(d,n,v,s) \leq \deg W(d,n,v)\,(d+1)^s \leq (2vd)^{s/6}(d+1)^s.$$

Let $\pi_1 : V(d,n,v,s) \to \mathbb{K}^{ns}$ and $\pi_2 : V(d,n,v,s) \to W(d,n,v) \subset \mathbb{K}^t$ be the projections. Let C_j $j \in J$ be all those components of $V(d,n,v,s)$ such that $\pi_2(C_j)$ contains some polynomial $P \neq 0$. Clearly $\pi_1(\bigcup_{j \in J} C_j) \subset \mathbb{K}^{ns}$ contains all incorrect test sequences for $W(d,n,v)$. In order to bound the cardinality of $\pi_1(\bigcup_{j \in J} C_j) \cap [u]^{ns}$ we need the following

Fact $\dim C_j \leq (n-1)s + s/6$ for all $j \in J$.

Proof Let $P \in \pi_2(C_j)$, $P \neq 0$. Then clearly $\dim \pi_2^{-1}(P) = (n-1)s$, since $\pi_2^{-1}(P) = \{(\underline{a}^1,..,\underline{a}^s) \mid \forall \nu \leq s : P(\underline{a}^\nu) = 0\}$.

Applying theorem 2.2 to $E := C_j$, $D := W(d,n,v)$ yields

$$\dim \pi_2^{-1}(P) \geq \dim C_j - \dim W(d,n,v).$$

Hence $\dim C_j \leq (n-1)s+s/6$.

Let $H_{i,\nu} \subset \mathbb{K}^{ns+t}$ be the hypersurface defined by

$$(x_{i,\nu}-1)(x_{i,\nu}-2)\ldots(x_{i,\nu}-u) = 0 \text{ for } i=1,..,n, \nu=1,..,s.$$

Then $\pi_1(\bigcup_{j\in J} C_j) \cap [u]^{ns} = \pi_1(\bigcup_{j\in J} C_j \cap \bigcap_{i,\nu} H_{i,\nu})$

Therefore $\#(\pi_1(\bigcup_{j\in J} C_j) \cap [u]^{ns})$

$$= \#\pi_1(\bigcup_{j\in J} C_j \cap \bigcap_{i,\nu} H_{i,\nu})$$

$$\leq \deg(\bigcup_{j\in J} C_j \cap \bigcap_{i,\nu} H_{i,\nu})$$

applying proposition 2.3 to $E_1 := \bigcup_{j\in J} C_j$, $\dim E_1 \leq (n-1)s+s/6$ yields

$$\leq \deg(\bigcup_{j\in J} C_j)\, u^{(n-1)s+s/6}$$

$$\leq (2vd)^{s/6}(d+1)^s\, u^{(n-1)s+s/6}$$

$$= u^{ns}\, u^{-s/6}(2vd)^{s/6}(d+1)^s\, u^{-\frac{2s}{3}}$$

$$\leq u^{ns}\, u^{-s/6} \quad \text{since } u \geq 2v(d+1)^2.$$

Hence at most $u^{ns}\, u^{-s/6}$ sequences in $[u]^{ns}$ are incorrect test sequences for $W(d,n,v)$. This proves the theorem. ∎

It is an interesting observation that so far the provably correct test sequences for $W(d,n,v)$ and the coefficient vectors of multivariate polynomials which are provably not in $W(d,n,v)$ both are of the following three types:

(1) integer vectors with doubly exponentially increasing components, e.g.: $(m, m^d, m^{d^2}, \ldots, m^{d^{k-1}})$

(2) vectors $(a_1,..,a_k)$ with <u>algebraic</u> coefficients that generate a large closure $\overline{(a_1,..,a_k)} \subset \mathbb{K}^k$ with respect to closed sets definable over $\mathbb{Q}$.

(3) for sufficiently large $u \in \mathbb{N}$ almost all $(a_1,..,a_k) \in [u]^k$.

Indeed so far our methods for proving substantial lower bound on the arithmetical complexity of polynomials and the methods for establishing a correct test sequence for $W(d,n,v)$ are essentially the same. This does not happen accidentally. Indeed we can reduce the problem of establishing multivariate polynomials not in $W(d,n,v)$ to the problem of constructing a correct test sequence for $W(d,n,v)$.

For a sequence $(\underline{a}^1,..,\underline{a}^s) \in \mathbb{Z}^{ns}$ with $\underline{a}^\nu = (a_1^\nu,..,a_n^\nu) \in \mathbb{Z}^n$ we define the <u>weight</u> as $w(\underline{a}^1,..,\underline{a}^s) := \Sigma_{i,\nu}|a_i^\nu|$. As before we identify a polynomial $P \in \mathbb{K}[x_1,..,x_n]$, $\deg P \leq d$ with its coefficient vector in $\mathbb{K}^t$, $t := \binom{n+d}{d}$. Moreover, we fix an arbitrary ordering of the coefficients of P and for $r<t$ we identify $\mathbb{K}^r$ with the set of all polynomials that have non zeros only within the first r coefficients and all other coefficients being zero.

Theorem 4.5

Given a correct test sequence $\underline{a}^1,..,\underline{a}^s \in \mathbb{Z}^n$ for W(d,n,v) we can construct a polynomial $P \in \mathbb{Z}^{s+1}$ (i.e. the polynomial P has non zeros only within the first s+1 coefficients), deg P $\leq$ d, $P \notin W(d,n,v)$ and the construction time is polynomial in s d log $w(\underline{a}^1,..,\underline{a}^s)$. In particular log w(P) = $O(s^2 d \log s \log w(\underline{a}^1,..,\underline{a}^s))$.

Given a correct test sequence $\underline{a}^1,..,\underline{a}^s$ for W(d,n,v) then the construction of a polynomial $P \notin W(d,n,v)$ deg P$\leq$d isparticularly easy if d is sufficiently large, i.e. d$\geq$s:

Lemma 4.6 Let $\underline{a}^1,..,\underline{a}^s \in \mathbb{Q}^{ns}$ be a correct test sequence for W(d,n,v) and d$\geq$s. Then $L_{ns}(\prod_{i=1}^{s}(x_\nu - a_\nu^i)) \geq \nu$ for $\nu = 1,..,n$.

Proof Every polynomial $\prod_{i=1}^{s}(x_\nu - a_\nu^i)$ falsifies the test sequence $(\underline{a}^1,..,\underline{a}^s)$. Since s$\leq$d this implies $L_{ns}(\prod_{i=1}^{s}(x_\nu - a_\nu^i)) \geq \nu$. ∎

Acknowledgement Our interest in this subject was greatly stimulated by several conversations with Steve Cook and by the talk of M. Mignotte at the occasion of the 1979 Oberwolfach Conference on Complexity Theory.

References

1. Adleman, L.: TWO THEOREMS ON RANDOM POLYNOMIAL TIME. Proceedings of 19th Symposium on Foundations of Computer Science, Ann Arbor, 1978, pp. 75-83

2. von zur Gathen, J. and Straßen, V.: SOME POLYNOMIALS THAT ARE HARD TO COMPUTE. Preprint Universität Zürich, 1979

3. Heintz, J.: DEFINABILITY BOUNDS OF FIRST ORDER THEORIES OF ALGEBRAICALLY CLOSED FIELDS. Extended abstract in the Proceedings of the FCT Conference, Berlin/Wendisch Rietz 1979, Ed. L. Budach. Berlin: Akademie-Verlag 1979, pp. 160-166

4. Heintz, J. and Sieveking, M.: LOWER BOUNDS FOR POLYNOMIALS WITH ALGEBRAIC COEFFICIENTS. Preprint Universität Frankfurt/Main 1978, to appear in Theoretical Computer Science

5. Kendig, K.: ELEMENTARY ALGEBRAIC GEOMETRY. New York: Springer-Verlag 1977

6. Lovász, L.: ON DETERMINANTS, MATCHINGS AND RANDOM ALGORITHMS. Proceedings of the FCT-Conference, Berlin/Wendisch-Rietz 1979, Ed. L. Budach, Berlin: Akademie-Verlag 1979, pp. 565-574

7. Mignotte, M. and Morgenstern, J.: personal communication at the 1979 Oberwolfach Conference on Complexity Theory

8. Paterson, M.S. and Stockmeyer, L.J.: ON THE NUMBER OF NONSCALAR MULTIPLICATIONS NECESSARY TO EVALUATE POLYNOMIALS. SIAM J. Comput.2, 1973, 60-66

9. Schnorr, C.P.: IMPROVED LOWER BOUNDS ON THE NUMBER OF MULTIPLICATIONS/DIVISIONS WHICH ARE NECESSARY TO EVALUATE POLYNOMIALS. Theoretical Computer Science 7, 1978 pp. 251-261

10. Schnorr, C.P.: AN EXTENSION OF STRASSENS'S DEGREE BOUND. Preprint in the Proceedings of the FCT Conference Berlin/Wendisch-Rietz 1979, Ed. L. Budach, Berlin: Akademie-Verlag 1979, pp. 404-416 . Full version to appear in SIAM J.of Comp.

11. Schnorr, C.P.: HOW MANY POLYNOMIALS CAN BE FASTER APPROXIMATED THAN THEY CAN BE EVALUATED? Preprint Universität Frankfurt/Main 1979

12. Schnorr, C.P. and Van de Wiele, J.P.: ON THE ADDITIVE COMPLEXITY OF POLYNOMIALS. Theoretical Computer Science 10, 1980, 1-18

13. Schafarewitch, I.R.: GRUNDLAGEN DER ALGEBRAISCHEN GEOMETRY. Berlin: VEB Deutscher Verlag der Wissenschaften 1972

14. Schwartz, J.T.: PROBABILISTIC ALGORITHMS FOR VERIFICATION OF POLYNOMIAL IDENTITIES. Proceedings of the Eurosam Symposium Marseille 1979, Lecture Notes in Computer Science 72, Ed. E.W.Ng. Berlin-New York: Springer-Verlag 1979, pp. 216-226

15. Stoß, H.J.: UNTERE SCHRANKEN FÜR DIE ZAHL DER OPERATIONEN BEI DER BERECHNUNG VON POLYNOMEN. Preprint Universität Konstanz, 1979

16. Straßen, V.: DIE BERECHNUNGSKOMPLEXITÄT DER ELEMENTARSYMMETRISCHEN FUNKTIONEN UND VON INTERPOLATIONSKOEFFIZIENTEN. Numerische Mathematik 20, 1972, pp. 238-251

17. Straßen, V.: POLYNOMIALS WITH RATIONAL COEFFICIENTS WHICH ARE HARD TO COMPUTE. SIAM J. Computing 3, 1974, pp. 128-149

18. Van der Waerden, B.L.: EINFÜHRUNG IN DIE ALGEBRAISCHE GEOMETRIE (zweite Auflage), New York: Springer-Verlag, 1973