ON LOWER BOUNDS FOR THE COMPLEXITY OF POLYNOMIALS AND THEIR MULTIPLES

Walter Baur and Karin Halupczok

Abstract. We prove a theorem giving arbitrarily long explicit sequences $x_1, \ldots, x_s$ of algebraic numbers such that any nonzero polynomial $f(X)$ satisfying $f(x_1) = \cdots = f(x_s) = 0$ has nonscalar complexity $> C\sqrt{s}$ for some positive constant C independent of s. A similar result is shown for rapidly growing rational sequences.

1. Introduction

Let k be an infinite field. For polynomials $f \in k[X]$ let $L(f)$ be the nonscalar complexity of f, i.e. the minimum number of nonscalar multiplications/divisions necessary to compute f. It is well known that $L(f) \leq 2\sqrt{n}$ where n is the degree of f (Paterson and Stockmeyer [6], see also Bürgisser et al. [4]).

In the following we are concerned with lower bounds for $L(f)$. The first nontrivial lower bounds for specific polynomials were obtained by Strassen [7]. His methods apply to polynomials with sufficiently independent algebraic coefficients like $f = \sum_{i=1}^{n} \sqrt{p_i} X^i$ (p_i the i-th prime), or to polynomials with rapidly growing rational coefficients like $f = \sum_{i=1}^{n} 2^{2^i} X^i$, giving a lower bound of order $\sqrt{\frac{n}{\log n}}$ in both cases.

Heintz and Morgenstern [5] proved a general theorem on the complexity of polynomials given by their roots. For $f = \prod_{i=1}^{n}(X - \sqrt{p_i})$ they obtained again a lower bound of order $\sqrt{\frac{n}{\log n}}$ (see also Baur [3]).

For $f = \prod_{i=1}^{n} \left(X - 2^{2^i}\right)$ a similar result was shown in Aldaz et al. [1].

The aim of this paper is to exhibit specific polynomials f such that a nontrivial lower bound can be proved not just for $L(f)$ but for $\min\{L(fh) : 0 \neq h \in k[X]\}$, i.e. for all nonzero polynomials from the ideal generated by f. An example is the polynomial $f = \prod_{i=1}^{n} \left(X - 2^{2^i}\right)$ from above: We show that for sufficiently large n we have $L(fh) > \frac{1}{3}n^{\frac{1}{3}}$ for all $0 \neq h \in \mathbf{C}[X]$ (Corollary 3.2). Similar results are obtained for polynomials $f = \prod_{i=1}^{n} (X - x_i)$ whose roots x_i are sufficiently independent algebraic numbers of high degree (Corollary 3.1). The polynomial $f = \prod_{i=1}^{n} \left(X - \sqrt{p_i}\right)$ however is out of reach of the present methods. The reason is that there is a multiple $f \cdot \prod_{i=1}^{n} \left(X + \sqrt{p_i}\right) = \prod_{i=1}^{n} (X^2 - p_i)$ of f which is a polynomial of degree $2n$ whose coefficients are integers of moderate size. To our knowledge no nontrivial lower bound for the complexity of a polynomial of this kind has ever been proved.

2. The Theorem.

The main result is the following

Theorem 2.1. *For all sufficiently large positive integers r, s such that $4r^2 \leq s \leq 2^r$ there exists a nonvanishing polynomial $q(X_1, \ldots, X_s)$ of degree $\leq 2^{3r}$ in each indeterminate X_i and with integer coefficients of absolute value ≤ 1 such that for all nonzero polynomials $f \in k[X]$ with $L(f) \leq r$ and all s-tuples $(x_1, \ldots, x_s)$ of zeroes $x_i \in k$ of f we have $q(x_1, \ldots, x_s) = 0$.*

The proof relies on methods introduced by Strassen [7].
Recall that the height $\mathrm{ht}(F)$ of a multivariate polynomial F with integer coefficients is the maximum of the absolute values of its coefficients, and the weight $\mathrm{wt}(F)$ is the sum of the absolute values of its coefficients.

We will use the following version of the representation theorem for polynomials of complexity r. (A proof of a closely related variant of this theorem can be found in Bürgisser et al. [4].)

Representation Theorem 2.2. *For any integer $r \geq 1$ there exists a polynomial $F(\underline{Z}, X) \in \mathbf{Z}[Z_1, \ldots, Z_{(r+2)^2}, X]$ such that*

(i) $\deg_X F \leq 2^r$, $\deg_{\underline{Z}} F \leq 2^{r+1}r$,

(ii) $\operatorname{wt} F \leq 2^{2^{2r^2}}$,

(iii) *for any polynomial $f \in k[X]$ such that $L(f) \leq r$ the following holds: For almost all $\xi \in k$ there exist $\eta_1, \ldots, \eta_{(r+2)^2} \in k$ such that $f(X+\xi) = F(\underline{\eta}, X)$.*

REMARK 2.3. *Any polynomial f such that $L(f) \leq r$ has degree $\leq 2^r$. This is the reason for truncating the "generic power series of complexity r" to a polynomial $F(\underline{Z}, X)$ of degree 2^r in X.*

We will also make use of

SIEGEL'S LEMMA 2.4. (see e.g. [2], p. 13) *Let $l_1, \ldots, l_M \in \mathbf{Z}[X_1, \ldots, X_N]$ be linear forms of weight $\leq w$ for some positive integer w. If $N > M$ then there exists a nontrivial vector $\underline{x} = (x_1, \ldots, x_N) \in \mathbf{Z}^N$ such that $l_1(\underline{x}) = \cdots = l_M(\underline{x}) = 0$ and*

$$|x_i| \leq w^{\frac{M}{N-M}}, \quad 1 \leq i \leq N.$$

We start the proof of the theorem with

LEMMA 2.5. *For all sufficiently large positive integers r, s such that $4r^2 \leq s \leq 2^r$ there exists a nonvanishing polynomial*

$$Q = \sum_{0 \leq j_1, \ldots, j_s < 2^r} q_{\underline{j}}(X_1, \ldots, X_s) Y_1^{j_1} \cdots Y_s^{j_s} \in \mathbf{Z}[\underline{X}, \underline{Y}]$$

in independent indeterminates $\underline{X}$, $\underline{Y}$ such that

(i) $\deg_{X_i} q_{\underline{j}} \leq 2^{3r}$ *for all $i, \underline{j}$,*

(ii) $\operatorname{ht} q_{\underline{j}} \leq 1$ *for all $\underline{j}$,*

(iii) *for all $f \in k[X]$ such that $L(f) \leq r$ we have*

$$Q(X_1, \ldots, X_s, f(X_1), \ldots, f(X_s)) = 0.$$

Proof. Fix r and s according to the hypothesis. Let $F(Z_1, \dots, Z_{(r+2)^2}, X)$ be the polynomial from the Representation Theorem. Replace the indeterminate Y_i in the unknown polynomial Q by $F(\underline{Z}, X_i)$ and consider

$$\sum_{0 \le j_1, \dots, j_s < 2^r} q_{\underline{j}}(\underline{X}) F(\underline{Z}, X_1)^{j_1} \cdots F(\underline{Z}, X_s)^{j_s} = 0 \tag{2.1}$$

as a system $\mathcal{L}$ of homogeneous linear equations for the unknown coefficients of the polynomials $q_{\underline{j}}$. Then the number N of unknowns is

$$N = \left(2^{3r} + 1\right)^s \cdot 2^{rs} \ge 2^{4rs}$$

whereas the number M of linear equations equals the number of monomials in $\underline{Z}$, $\underline{X}$ occurring in (2.1). Therefore, for sufficiently large r, we get

$$\begin{aligned} M &\le \left(\deg_{\underline{Z}} F \cdot 2^r s\right)^{(r+2)^2} \cdot \left(2^{3r} + \deg_X F \cdot 2^r\right)^s \\ &\le 2^{3r^3 + o(r^3)} \cdot \left(2^{3r} + 2^{2r}\right)^s \\ &\le 2^{3r^3 + 3rs + s + o(r^3)}, \end{aligned}$$

since $s \le 2^r$. Hence

$$\begin{aligned} N - M &\ge 2^{4rs} \left(1 - 2^{-rs + 3r^3 + s + o(r^3)}\right) \\ &\ge 2^{4rs - 1} \end{aligned}$$

since $s \ge 4r^2$ and r is large.
This shows $N > M$ and, again using $s \ge 4r^2$,

$$\begin{aligned} \frac{M}{N - M} &\le 2^{3r^3 + 3rs + s - 4rs + o(r^3)} \\ &\le 2^{-(r-1)s + 3r^3 + o(r^3)} \\ &\le 2^{-r^3/2} \end{aligned}$$

if r is large.

The sum of the absolute values of the coefficients of any of the linear equations from $\mathcal{L}$ can be estimated from above by the weight of the polynomial in (2.1) where the coefficients of the $q_{\underline{j}}$ are considered as new indeterminates. Therefore, using subadditivity and submultiplicativity of the weight and the weight bound from the Representation Theorem

$$w \le 2^{rs} \cdot \left(2^{3r} + 1\right)^s \cdot 2^{2^{2r^2} 2^r s} \le 2^{2^{3r^2}}$$

if r is large. Hence

$$w^{\frac{M}{N-M}} \leq 2^{2^{3r^2} \cdot 2^{-r^3/2}} \longrightarrow 1 \tag{2.2}$$

if $r \to \infty$.

Now we apply Siegel's Lemma to the system $\mathcal{L}$. Using $N > M$ and (2.2) we get a nontrivial integer solution whose components are of absolute value ≤ 1, i.e. polynomials $q_{\underline{j}}$ satisfying (i) and (ii).
In order to finish the proof let $f \in k[X]$ be a polynomial with $L(f) \leq r$. Using (2.1) and the Representation Theorem we obtain

$$Q(X_1, \ldots, X_s, f(X_1 + \xi), \ldots, f(X_s + \xi)) = 0$$

for almost all $\xi \in k$. Since k is infinite we conclude

$$Q(X_1, \ldots, X_s, f(X_1), \ldots, f(X_s)) = 0.$$

□

Proof. (Proof of the theorem.) Let $\underline{j} = (j_1, \ldots, j_s)$ be the lexicographically first s-tuple such that the coefficient $q_{\underline{j}}$ of the polynomial Q from the lemma is nonzero. We show that $q = q_{\underline{j}}$ satisfies the theorem. Let $f \in k[X]$ be a nonzero polynomial with $L(f) \leq r$ and let $(x_1, \ldots, x_s)$ be an s-tuple of zeroes of f. Let $e_i \geq 1$ be the multiplicity of the root x_i of f. Then

$$f(X) = (X - x_i)^{e_i} \cdot h_i(X)$$

for some $h_i(X) \in k[X]$ such that $h_i(x_i) \neq 0$. Writing

$$Q(X_1, \ldots, X_s, f(X_1), \ldots, f(X_s)) \tag{2.3}$$

as a polynomial in $X_1 - x_1, \ldots, X_s - x_s$ it is easy to see that the coefficient of the monomial $(X_1 - x_1)^{e_1 j_1} \cdots (X_s - x_s)^{e_s j_s}$ is

$$c = q_{\underline{j}}(\underline{x}) h_1(x_1)^{j_1} \cdots h_s(x_s)^{j_s}.$$

By statement (iii) of the lemma the polynomial (2.3) is the zero polynomial. Hence $c = 0$ and therefore $q_{\underline{j}}(\underline{x}) = 0$. □

3. Applications

For the applications assume $k = \mathbf{C}$.

Corollary 3.1. *Let a be a squarefree integer $\neq 0, \pm 1$. Then for all sufficiently long sequences $p_1, \dots, p_s$ of pairwise different positive primes $p_i > 2^{s^{\frac{1}{2}}}$ we have $L(f) > \frac{1}{3} s^{\frac{1}{2}}$ for any polynomial $f \in \mathbf{C}[X]$ such that*

$$f(a^{\frac{1}{p_1}}) = \cdots = f(a^{\frac{1}{p_s}}) = 0.$$

Proof. Put $x_i = a^{\frac{1}{p_i}}$, $1 \leq i \leq s$. Then

$$[\mathbf{Q}(x_i) : \mathbf{Q}] = p_i, \tag{3.4}$$

and therefore, since the p_i are different primes,

$$[\mathbf{Q}(x_1, \dots, x_s) : \mathbf{Q}] = p_1 \cdots p_s. \tag{3.5}$$

Put $r = \lfloor \frac{1}{3} s^{\frac{1}{2}} \rfloor$. Then $4r^2 \leq s$.
Now apply the theorem to get a polynomial $q(X_1, \dots, X_s)$ with the properties stated there.
Since the degree of q in each indeterminate is $\leq 2^{3r} \leq 2^{s^{1/2}} < [\mathbf{Q}(x_i) : \mathbf{Q}]$ we obtain $q(\underline{x}) \neq 0$ by (3.4) and (3.5). Therefore $L(f) > r$. □

Corollary 3.2. *For all sufficiently long sequences $y_1, \dots, y_n$ of complex numbers such that $2 \leq |y_1|$ and $|y_i|^2 \leq |y_{i+1}|$ for $1 \leq i < n$ any nonzero polynomial $f \in \mathbf{C}[X]$ such that $f(y_1) = \cdots = f(y_n) = 0$ has nonscalar complexity $> \frac{1}{3} n^{\frac{1}{3}}$.*

Remark 3.3. *The sequence $y_i = 2^{2^i}$ clearly satisfies the hypotheses of the Corollary.*

Proof. Put $r = \lfloor \frac{1}{3} n^{\frac{1}{3}} \rfloor$, $d = 3r + 1$ and $s = \lfloor \frac{n}{d} \rfloor$. Then, for sufficiently large n,

$$s \geq \frac{n}{3r+1} - 1 \geq \frac{n}{n^{\frac{1}{3}} + 1} - 1 \geq n^{\frac{2}{3}} + o(n^{\frac{2}{3}}) \geq 4r^2.$$

For $1 \leq i \leq s$ put $x_i = y_{id}$.

Arguing as in the proof of the first Corollary it suffices to show that for sufficiently large s we have $q(x_1, \ldots, x_s) \neq 0$ for any nonzero polynomial

$$q(X_1, \ldots, X_s) = \sum_{\underline{j}} a_{\underline{j}} X_1^{j_1} \cdots X_s^{j_s}$$

of degree $\leq 2^{3r}$ in each indeterminate and with integer coefficients $a_{\underline{j}}$ of absolute value ≤ 1.
First note that for any $1 \leq i < s$

$$\left| x_i^{2^d} \right| = \left| y_{id}^{2^d} \right| \leq \left| y_{id+1}^{2^{d-1}} \right| \leq \cdots \leq \left| y_{(i+1)d} \right| = |x_{i+1}|$$

and therefore

$$\begin{aligned} 2 \left| x_1^{2^d-1} x_2^{2^d-1} \cdots x_i^{2^d-1} \right| &\leq \left| x_1^{2^d} x_2^{2^d-1} \cdots x_i^{2^d-1} \right| \\ &\leq \left| x_2^{2^d} x_3^{2^d-1} \cdots x_i^{2^d-1} \right| \\ &\vdots \\ &\leq |x_{i+1}| \,. \end{aligned}$$

Using this inequality an easy induction with respect to the antilexicographic ordering $<$ on $S = \{0, 1, \ldots, 2^d - 1\}^s$ shows that for any $\underline{j} \in S$

$$\sum_{\underline{l} < \underline{j}} \left| x_1^{l_1} \cdots x_s^{l_s} \right| < \left| x_1^{j_1} \cdots x_s^{j_s} \right| .$$

Since $\deg_{X_i} q \leq 2^{3r} \leq 2^d - 1$ the set S contains all indices $\underline{l}$ such that $a_{\underline{l}} \neq 0$. Therefore, if $\underline{j} = \max\{\underline{l} \in S : a_{\underline{l}} \neq 0\}$ then

$$\sum_{\underline{l} \neq \underline{j}} |a_{\underline{l}}| \cdot \left| x_1^{l_1} \cdots x_s^{l_s} \right| < \left| x_1^{j_1} \cdots x_s^{j_s} \right| .$$

Hence $q(\underline{x}) \neq 0$. □

Remark 3.4. *If the roots y_i of f in Corollary 3.2 grow even faster, e.g. $y_i = 2^{2^{ni}}$ $(1 \leq i \leq n)$ then, putting $r = \lfloor \frac{1}{2} n^{\frac{1}{2}} \rfloor$, $s = n$ and $x_i = y_i$, the same proof gives $\frac{1}{2} n^{\frac{1}{2}}$ as lower bound for the nonscalar complexity of f.*

References

[1] M. Aldaz, J. Heintz, G. Matera, J. L. Montana and L. M. Pardo, *Time-space tradeoffs in algebraic complexity theory*. Preprint.

[2] A. Baker, *Transcendental number theory*. Cambridge University Press (1975).

[3] W. Baur, *Simplified Lower Bounds for Polynomials with Algebraic Coefficients*. J. of Complexity **13** (1997), 38-41.

[4] P. Bürgisser, M. Clausen and A. Shokrollahi, *Algebraic Complexity Theory*. A Series of comprehensive studies in mathematics **315** (1997), Springer.

[5] J. Heintz and J. Morgenstern, *On the intrinsic complexity of elimination theory*. J. of Complexity **9** (1993), 471-498.

[6] M. S. Paterson and L. J. Stockmeyer, *On the number of nonscalar multiplications necessary to evaluate polynomials*. SIAM J. Comput. **2** (1973), 60-66.

[7] V. Strassen, *Polynomials with rational coefficients which are hard to compute*. SIAM J. Comput. **3** (1974), 128-149.