A new method to obtain lower bounds for polynomial evaluation ⋆

M. Aldaz [a,1], G. Matera [b,c,2], J.L. Montaña [a,1], and L.M. Pardo [d,3]

[a] *Universidad Pública de Navarra, Departamento de Matemática e Informática, 31006 Pamplona, Spain*
{mikaldaz, pepe}@unavarra.es

[b] *Universidad Favaloro, Laboratorio de Computación, Solis 453 (1078) Buenos Aires, Argentina*
gmatera@favaloro.edu.ar

[c] *Universidad Nacional de Gral. Sarmiento, Instituto de Desarrollo Humano, Roca 850 (1663) San Miguel, Argentina*
gmatera@ungs.edu.ar

[d] *Universidad de Cantabria, Fac. de Ciencias, Depto. de Matemáticas, Estadística y Computación, 39071 Santander, Spain*
pardo@hall.matesco.unican.es

Abstract

We present a new method to obtain lower bounds for the time complexity of polynomial evaluation procedures. Time, denoted by L, is measured in terms of nonscalar arithmetic operations. In contrast with known methods for proving lower complexity bounds, our method is purely combinatorial and does not require powerful tools from algebraic or diophantine geometry.

By means of our method we are able to verify the computational hardness of new natural families of univariate polynomials for which this was impossible up to now. By computational hardness we mean that the complexity function L^2 grows linearly in the degree of the polynomials of the family we are considering.

Our method can also be applied to classical questions of transcendence proofs in number theory and geometry. A list of (old and new) formal power series is given whose transcendence can be shown easily by our method.

Key words: Algebraic Complexity; Straight-line program complexity; Complexity of polynomial evaluation; Transcendence criterion.

1 Introduction

The study of complexity issues for straight-line programs evaluating univariate polynomials is a standard subject in theoretical computer science. One of the most fundamental tasks in this domain is the exhibition of *explicit* families of univariate polynomials which are "hard to compute" in the given context. Following Motzkin [18], Belaga [3] and Paterson–Stockmeyer [20] "almost all" univariate polynomials of degree d need for their evaluation at least $\Omega(d)$ additions/subtractions, $\Omega(d)$ scalar multiplications/divisions, and $\Omega(\sqrt{d})$ nonscalar multiplications/divisions. A family $(F_d)_{d\in\mathbb{N}}$ of univariate polynomials F_d satisfying the condition $\deg F_d = d$ is called *hard to compute* in a given complexity model if there exists a positive constant c such that any straight-line program evaluating the polynomial F_d requires the execution of at least $\Omega(d^c)$ arithmetic operations in the given model.

In the present contribution we shall restrict ourselves to the nonscalar complexity model. This model is well suited for lower bound considerations and does not represent any limitation for the generality of our statements.

Families of specific polynomials which are hard to compute were first considered by Strassen in [25]. The method used by Strassen was later refined by Schnorr [22] and Stoss [24]. In [14], Heintz and Sieveking introduced a considerably more adaptive method which allowed the exhibition of quite larger classes of specific polynomials which are hard to compute. However in its beginning the application of this new method was restricted to polynomials with *algebraic* coefficients. In [13], Heintz and Morgenstern adapted the method of Heintz–Sieveking to polynomials given by their algebraic roots and this adaptation was considerably simplified in [2].

Finally the methods of Strassen [25] and Heintz–Sieveking [14] were unified to a common approach by Aldaz *et alii* in [1]. This new approach was based on effective elimination and intersection theory with their implications for diophantine geometry (see e.g. [8,15,21]). This method allowed for the first time applications to polynomials having only integer roots.

The results of the present contribution are based on a new, considerably sim-

---

⋆ An extended abstract of this paper appeared in the Proceedings of the 23rd Symposium on the Mathematical Foundations of Computer Science, Springer Lecture Notes in Computer Science **1450** (1998) pp. 167–175.

[1] Partially supported by Gobierno de Navarra under project "Complejidad y Estructuras de Datos en Cálculo Simbólico", Spain.

[2] Partially supported by UBA–CYT TW80, PIP CONICET 4571 and ANPCYT PICT 03–00000–01593, Argentina.

[3] Partially supported by DGCYT PB 96–0671–C02–02, Spain.

plified version of the unified approach mentioned before. Geometric considerations are replaced by simple counting arguments which make our new method more flexible and adaptive (see Lemma 4). The new method is inspired in [23] and [2] and relies on a counting technique developed in [25] (see also [22,24]). Except for this result (Theorem 2) the method is elementary and requires only basic knowledge of algebra.

Our new method yields a simple criterion (Theorem 6) to establish computational hardness results for several new families of polynomials given either by their integer coefficients or by their integer roots (see Theorems 10, 11 and 12). The method also implies some known results for polynomials with algebraic coefficients (see Theorems 7 and 8).

Our method can also be applied to establish transcendence proofs for power series. Using Newton's method to approximate algebraic functions we obtain a simple criterion of transcendence (see Theorem 13 and Criterion 14). Several (old and new) power series are given whose transcendence can be shown easily by our method (see Corollary 15).

Let us finally remark that our method does not apply to polynomials having "small" integer roots such as the Pochhammer–Wilkinson polynomials. Some result in this direction would be of great interest because of their relationship with other subjects of theoretical computer science. Connections with boolean complexity problems can be found in [13] where the complexity of evaluation of the Pochhammer–Wilkinson polynomials is related with the complexity of a geometric elimination problem, and also in [17] where the complexity of evaluating polynomials with many different rational roots is related with the complexity of integer factorization. In [4, Chapter 7] the hypothesis that the multiples of the Pochhammer–Wilkinson polynomials are hard to compute is used to show that $P \neq NP$ holds for computations over algebraically closed fields of characteristic zero.

2 Straight-line Programs and Representation Theorem

Let K be an algebraically closed field of characteristic zero. By $K[X]$ we denote the ring of univariate polynomials in the indeterminate X over K and by $K(X)$ its fraction field. Let α be a point of K. By $K[[X-\alpha]]$ we denote the ring of formal power series in $X-\alpha$ with coefficients in K and by $\mathcal{O}_\alpha$ the localization of $K[X]$ by the maximal ideal generated by the linear polynomial $X-\alpha$. This means that $\mathcal{O}_\alpha$ is the subring of $K(X)$ given by the rational functions $F := f/g$, with $f, g \in K[X]$ and $g(\alpha) \neq 0$.

Since K has characteristic zero for every $\alpha \in K$ there exists a natural embed-

ding i_α from $\mathcal{O}_\alpha$ into $K[[X-\alpha]]$ defined as follows: for any $F \in \mathcal{O}_\alpha$, let $i_\alpha(F)$ be the Taylor expansion of F at the point α, namely

$$i_\alpha(F) := \sum_{j\in\mathbb{N}} \frac{F^{(j)}(\alpha)}{j!} \cdot (X-\alpha)^j \ .$$

Here we denote by $F^{(j)}$, $j \in \mathbb{N}$, the j-th derivative of the rational function F.

Let A be one of the following K-algebras: $K[X]$, $K(X)$ or $\mathcal{O}_\alpha$, where $\alpha \in K$. We recall the following standard notion of algebraic complexity theory (see [6,10,12,24,26,19] and [7, Chapter 4]).

Definition 1 *Let L be a natural number. A* straight-line program of nonscalar length L in A *is a sequence β of elements of A, namely $\beta := (Q_{-1}, Q_0, \ldots, Q_L)$, satisfying the following conditions:*

- $Q_{-1} := 1$.
- $Q_0 := X$.
- *For any ρ, $1 \le \rho \le L$, there exist $d_\rho \in \{0,1\}$ and $a_{\rho,j}$, $b_{\rho,j} \in K$, with $-1 \le j < \rho$, such that*

$$Q_\rho := \Big(\sum_{-1\le j<\rho} a_{\rho,j}\cdot Q_j\Big)\cdot\Big((1-d_\rho)\cdot\Big(\sum_{-1\le j<\rho} b_{\rho,j}\cdot Q_j\Big)+d_\rho\cdot\Big(\sum_{-1\le j<\rho} b_{\rho,j}\cdot Q_j\Big)^{-1}\Big)$$

holds.

Let F be an arbitrary element of the K-algebra A. We say that the straight-line program $\beta = (Q_{-1}, Q_0, \ldots, Q_L)$ computes F if there exist field elements $c_l \in K$, with $-1 \le l \le L$, such that the following identity holds:

$$F = \sum_{-1\le l\le L} c_l \cdot Q_l \ .$$

The nonscalar complexity $L_A(F)$ of an element F of the K-algebra A is defined as

$$L_A(F) := \min\{\text{nonscalar length of } \beta : \beta \text{ in } A \text{ that computes } F\} \ .$$

Now let F be a rational function belonging to the K-algebra $\mathcal{O}_\alpha$. Suppose that F is given by a straight-line program β in $\mathcal{O}_\alpha$. We are going to analyze how F depends on the parameters of the straight-line program β. To this end we use an idea going back to [25] (see also [22,24]). The following analysis of the rational function F represents the main technical tool we use in this paper. A detailed proof of a similar result can be found in [7, Chapter 9, Theorem 9.9, pp. 212–215].

Let us first recall that the *height* of a given polynomial with integer coefficients is the maximum of the absolute values of its coefficients and the *weight* is the sum of the absolute values of these coefficients. Note that the weight is subadditive and submultiplicative.

Theorem 2 (Representation theorem for rational functions) *Let L be a natural number and $N := (L+1)(L+2)$. Then there exists a family $(P_{L,j})_{j\in\mathbb{N}}$ of polynomials $P_{L,j} \in \mathbb{Z}[Z_1, \ldots, Z_N]$ with*

$$\deg P_{L,j} \leq j(2L-1)+2 \tag{1}$$

and

$$\text{weight } P_{L,j} \leq 2^{3((j+1)^L-1)} \tag{2}$$

such that for any $\alpha \in K$ and any $F \in \mathcal{O}_\alpha$ with $L_{\mathcal{O}_\alpha}(F) \leq L$ there exists a point $z_F \in K^N$ satisfying the identity

$$i_\alpha(F) = \sum_{j\in\mathbb{N}} P_{L,j}(z_F) \cdot (X-\alpha)^j \ .$$

Following [14] for given natural numbers d and L let

$$\Phi_{d,L} : K^N \longrightarrow K^{d+1}$$

be the morphism of affine spaces defined by $\Phi_{d,L}(z) := (P_{L,0}(z), \ldots, P_{L,d}(z))$ for arbitrary $z \in K^N$. Let $W_{d,L} := \overline{im\, \Phi_{d,L}} \subseteq K^{d+1}$ be the Zariski closure over $\mathbb{Q}$ of the image $im\, \Phi_{d,L}$ of the morphism $\Phi_{d,L}$.

In the sequel we shall identify any polynomial $\sum_{0\leq j\leq d} f_j X^j \in K[X]$ of degree d with its coefficient vector $(f_0, \ldots, f_d)$ which we consider as a point of the affine space K^{d+1}.

3 Combinatorial Method

This Section is devoted to present the main results of this paper. In order to state our technical lemma (namely Lemma 4 below) we need the following notion and notation.

Definition 3 *Let n be a given natural number. For fixed $d \in \mathbb{N}$ we define a map*

$$\mu : K^{d+1} \longrightarrow \mathbb{N}$$

which is given in the following way: for any point $F := (f_0, \ldots, f_d)$ *belonging to* K^{d+1} *let*

$$\mu(F;n) := \#\left\{\sum_{S\subseteq\{0,\ldots,d\}} \theta_S \prod_{j\in S} f_j^{v_j} : 1 \leq v_j \leq n, 0 \leq j \leq d, \theta_S \in \{0,1\}\right\} \ .$$

For $n = 1$ *we write simply*

$$\mu(F) := \mu(F;1) \ .$$

Lemma 4 (Main Lemma) *Let* d, L *and* n *be given nonzero natural numbers. Then for any point* F *belonging to the algebraic variety* $W_{d,L} \subseteq K^{d+1}$ *we have*

$$\mu(F;n) \leq 2^{(n(d+1))^{20L^2}} \ . \tag{3}$$

PROOF. First of all observe that for any given natural numbers d, n and k the subset

$$\left\{F \in K^{d+1} : \mu(F;n) \leq k\right\}$$

is closed in the $\mathbb{Q}$-Zariski topology of K^{d+1}. Hence, since the variety $W_{d,L}$ is the $\mathbb{Q}$-Zariski closure of the image of the morphism $\Phi_{d,L} = (P_{L,0}, \ldots, P_{L,d})$, it suffices to prove the statement of the lemma for an arbitrary $(d+1)$-tuple $F := (f_0, \ldots, f_d)$ which belongs to $im\,\Phi_{d,L}$. Let $N := (L+1)(L+2)$. For fixed d, L and $n \in \mathbb{N}$ let us define the following set of polynomials of $\mathbb{Z}[Z_1, \ldots, Z_N]$:

$$\Gamma := \left\{\sum_{S\subseteq\{0,\ldots,d\}} \theta_S \prod_{j\in S} P_{L,j}^{v_j} : 1 \leq v_j \leq n, 0 \leq j \leq d, \theta_S \in \{0,1\}\right\} \ .$$

For any $z \in K^N$ let us write $\Gamma(z) := \{P(z) : P \in \Gamma\} \subseteq K$. Clearly we have $\#\,\Gamma(z) \leq \#\,\Gamma$. From Theorem 2 and Definition 3 we conclude that for any $(d+1)$-tuple $F := (f_0, \ldots, f_d)$ belonging to $im\,\Phi_{d,L}$ there exists a point $z_F \in K^N$ such that the following holds:

$$\mu(F;n) = \#\,\Gamma(z_F) \leq \#\,\Gamma \ .$$

Therefore, in order to prove (3) it suffices to show that the inequality

$$\#\,\Gamma \leq 2^{(n(d+1))^{20L^2}}$$

holds.

Let $D := \max\{\deg P : P \in \Gamma\}$ and $H := \max\{\text{height}\, P : P \in \Gamma\}$. Then every polynomial in Γ has at most $\binom{D+N}{N}$ monomials each of them with an integer coefficient of absolute value less or equal than H. Therefore

$$\#\,\Gamma \leq (2H+1)^{\binom{D+N}{N}} \leq (2H+1)^{(D+1)^N} \ , \tag{4}$$

since the inequality

$$\binom{D+N}{N} \leq (D+1)^N$$

holds for every pair of natural numbers D and N.

From the degree bound (1) we deduce the estimate:

$$D+1 \leq n \sum_{0 \leq j \leq d} (j(2L-1)+2)+1 \leq n(d+1)(Ld+2) \ . \tag{5}$$

Since every polynomial $P \in \mathbb{Z}[Z_1, \ldots, Z_N]$ verifies $\text{height}\,(P) \leq \text{weight}\,(P)$, from (2) we infer the following bound for the height of any polynomial in Γ:

$$H \leq 2^{d+1} \cdot \prod_{0 \leq j \leq d} 2^{3n((j+1)^L-1)} \leq 2^{3n(d+1)^{L+1}-(3n-1)(d+1)} \ . \tag{6}$$

Now, putting together (4), (5) and (6) we obtain the following estimate:

$$\begin{aligned} \#\,\Gamma \leq (2H+1)^{(D+1)^N} &\leq 2^{3n(d+1)^{L+1}(n(d+1)(Ld+2))^{(L+1)(L+2)}} \leq \\ &\leq 2^{n(d+1)^{L+1}(n(d+1)^2(L+1))^{(L+1)(L+2)}} \ . \end{aligned}$$

By Horner's rule we may suppose without loss of generality that $L \leq d$ holds. This implies finally

$$\#\,\Gamma \leq 2^{n(d+1)^{L+1}(n(d+1)^3)^{(L+1)(L+2)}} \leq 2^{(n(d+1))^{20L^2}} \ . \qquad \square$$

From Lemma 4 we obtain easily a sufficient condition (Theorem 6) saying when a polynomial with integer coefficients is hard to compute. Let $p \in \mathbb{N}$ be a prime number. For any integer $f \in \mathbb{Z}$ let us denote by $\nu_p(f)$ the multiplicity of p in the prime factor decomposition of f.

In the proof of Theorem 6 we need the following elementary fact.

Claim 5 *Let $a_1, \ldots, a_b$ be nonzero natural numbers and let p be a prime number such that $\nu_p(a_j) < \nu_p(a_{j+1})$ holds for each j, $1 \leq j < b$. Then*

$$\#\left\{\sum_{j \in S} a_j : S \subseteq \{1, \ldots, b\}\right\} = 2^b \ .$$

PROOF. It suffices to show that for any pair of different subsets S and S' of $\{1, \ldots, b\}$ it holds:

$$\sum_{j \in S} a_j \neq \sum_{j \in S'} a_j \ . \tag{7}$$

By cancelling common elements in both sides of the former inequality (if necessary) we conclude that it is enough to prove that inequality (7) holds for any pair of disjoint subsets S and S' of $\{1,\ldots,b\}$.

Now for each j, $1 \leq j \leq b$, let $n_j := \nu_p(a_j)$ be the multiplicity of p in the prime factor decomposition of the natural number a_j. We can write $a_j = p^{n_j} \cdot \tilde{a}_j$ with $\nu_p(\tilde{a}_j) = 0$. By hypothesis for each j, $1 \leq j \leq b$, we know that $n_j < n_{j+1}$. Consequently, we deduce that for any subset S of $\{1,\ldots,b\}$ the following equality holds:

$$\nu_p\Big(\sum_{j\in S} a_j\Big) = \nu_p\Big(p^{n_m} \cdot \Big(\tilde{a}_m + \sum_{\substack{j\in S\\ m<j}} p^{n_j - n_m} \cdot \tilde{a}_j\Big)\Big) = n_m \ , \tag{8}$$

where $m \in \{1,\ldots,b\}$ is the minimum of S.

From (8) we deduce immediatly that for any pair of different subsets S and S' of $\{1,\ldots,b\}$ it holds:

$$\nu_p\Big(\sum_{j\in S} a_j\Big) \neq \nu_p\Big(\sum_{j\in S'} a_j\Big) \ ,$$

and this finishes the prove of Claim 5. $\square$

Theorem 6 *There exists a positive universal constant c with the following property: let d and L be given nonzero natural numbers, $d > 1$. Let $F := \sum_{0\leq j\leq d} f_j X^j \in \mathbb{Z}[X]$ be a polynomial of degree at most d with integer coefficients such that F belongs to the algebraic variety $W_{d,L}$. Then for any prime number $p \in \mathbb{N}$ we have*

$$L^2 \geq c \cdot \frac{\log_2\Big(\#\Big\{\sum_{j\in S} \nu_p(f_j) : S \subseteq \{0,\ldots,d\}\Big\}\Big)}{\log_2 d} \ .$$

PROOF. Let $p \in \mathbb{N}$ be a prime number and let

$$b := \#\Big\{\nu_p\Big(\prod_{j\in S} f_j\Big) : S \subseteq \{0,\ldots,d\}\Big\} \ .$$

Then from Claim 5 we deduce that the following estimate holds:

$$\mu(F) = \#\Big\{\sum_{S\subseteq\{0,\ldots,d\}} \theta_S \prod_{j\in S} f_j : \theta_S \in \{0,1\}, S \subseteq \{0,\ldots,d\}\Big\} \geq 2^b \ . \tag{9}$$

Combining (9) with the inequality (3) for $n = 1$ and taking logarithms twice gives

$$L^2 \geq \frac{1}{20} \cdot \frac{\log_2\Big(\#\left\{\sum_{j\in S} \nu_p(f_j) : S \subseteq \{0,\ldots,d\}\right\}\Big)}{\log_2(d+1)} \ .$$

Finally, since $d > 1$, we conclude

$$L^2 \geq \frac{1}{20\log_2 3} \cdot \frac{\log_2\Big(\#\left\{\sum_{j\in S} \nu_p(f_j) : S \subseteq \{0,\ldots,d\}\right\}\Big)}{\log_2 d} \ . \qquad \square$$

Theorem 6 is the key result to show computational hardness of several new families of polynomials with integer coefficients. From Theorem 6 we can also obtain simple hardness proofs for some known families of polynomials with integer coefficients. For example Theorem 6 easily implies that the family of polynomials $(F_d)_{d\in\mathbb{N}}$ defined by $F_d := \sum_{0\leq j\leq d} 2^{2^j} X^j$ satisfies the complexity bound $L^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right)$ (see [25]).

Lemma 4 implies also some known hardness results for polynomials with algebraic coefficients. This is the content of the next two theorems.

Theorem 7 (Heintz–Sieveking [14]) *There exists a positive universal constant c with the following property: let D a given natural number and let $F := \sum_{0\leq j\leq d} f_j X^j \in \mathbb{C}[X]$ be a polynomial of degree at most d with algebraic complex coefficients. Let N be the dimension of the $\mathbb{Q}$-vector space $\mathbb{Q}[f_0,\ldots,f_d]$. Suppose that there exist polynomials $g_1,\ldots,g_s \in \mathbb{Q}[X_0,\ldots,X_d]$ of degree at most D, such that the locus of common zeroes of these polynomials in $\mathbb{C}^{d+1}$, $Z(g_1,\ldots,g_s)$, is finite and contains the point $(f_0,\ldots,f_d)$. Then for any natural number L such that F belongs to the algebraic variety $W_{d,L}$ we have the estimate*

$$L^2 \geq c \cdot \frac{\log_2 N}{\log_2 d + \log_2 D} \ .$$

PROOF. For any subset $V \subset K^{d+1}$ let us denote by $I(V) \subset \mathbb{Q}[X_0,\ldots,X_d]$ the ideal of the polynomials of $\mathbb{Q}[X_0,\ldots,X_d]$ which vanish on V. From the assumption $(f_0,\ldots,f_d) \in Z(g_1,\ldots,g_s)$ we deduce the following inclusions of ideals:

$$(g_1,\ldots,g_s) \subseteq I(Z(g_1,\ldots,g_s)) \subseteq I(\overline{\{(f_0,\ldots,f_d)\}}) \ ,$$

where $\overline{\{(f_0,\ldots,f_d)\}}$ is the closure in the $\mathbb{Q}$-Zariski topology of $\mathbb{C}^{d+1}$ of the set containing only the point $(f_0,\ldots,f_d)$. These inclusions and the fact that the $\mathbb{Q}$-vector space $\mathbb{Q}[f_0,\ldots,f_d]$ and the $\mathbb{Q}$-algebra $\mathbb{Q}[X_0,\ldots,X_d]/I(\overline{\{(f_0,\ldots,f_d)\}})$ are isomorphic imply that the morphism of $\mathbb{Q}$-algebras

$$\pi : \mathbb{Q}[X_0,\ldots,X_d]/(g_1,\ldots,g_s) \longrightarrow \mathbb{Q}[f_0,\ldots,f_d] \ ,$$

defined by $\pi(X_j + (g_1, \ldots, g_s)) := f_j$ for any j, $0 \leq j \leq d$, is an epimorphism.

From the assumption that the polynomials $g_1, \ldots, g_s$ define a nonempty finite subset we deduce that the $\mathbb{Q}$-vector space $\mathbb{Q}[X_0, \ldots, X_d]/(g_1, \ldots, g_s)$ is finite dimensional. According to [9] it is possible to find for $\mathbb{Q}[X_0, \ldots, X_d]/(g_1, \ldots, g_s)$ a monomial basis β of the form

$$\beta := \left\{ X_0^{v_0} \cdots X_d^{v_d} + (g_1, \ldots, g_s) : 0 \leq v_0 + \cdots + v_d \leq D(d+1) \right\} \ .$$

The image of the basis β under the epimorphism π,

$$\pi(\beta) = \left\{ f_0^{v_0} \cdots f_d^{v_d} : 0 \leq v_0 + \cdots + v_d \leq D(d+1) \right\} \ ,$$

is a set of generators of the $\mathbb{Q}$-vector space $\mathbb{Q}[f_0, \ldots, f_d]$. Therefore, if N is the dimension of $\mathbb{Q}[f_0, \ldots, f_d]$ then

$$\# \left\{ \sum_{f \in S} f : S \subseteq \pi(\beta) \right\} \geq 2^N \ .$$

Taking into account Definition 3 and the inclusion

$$\left\{ \sum_{f \in S} f : S \subseteq \pi(\beta) \right\} \subseteq \left\{ \sum_{S \subseteq \{0, \ldots, d\}} \theta_S \prod_{j \in S} f_j^{v_j} : 1 \leq v_j \leq D(d+1), \theta_S \in \{0,1\} \right\}$$

we can write

$$2^N \leq \mu(F; D(d+1)) \ . \tag{10}$$

Finally, let L be a natural number such that the point F belongs to the variety $W_{d,L}$. Then Lemma 4 yields the inequality

$$\mu(F; D(d+1)) \leq 2^{(D(d+1)^2)^{20L^2}} \ . \tag{11}$$

The proof finishes combining (10) and (11) and taking logarithms twice. $\square$

Theorem 7 implies that the following families of polynomials with algebraic coefficients $(F_d)_{d \in \mathbb{N}}$ satisfy the complexity bound $L^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right)$:

- $F_d := \sum_{1 \leq j \leq d} e^{\frac{2\pi i}{j}} X^j$ (see [14]),
- $F_d := \sum_{1 \leq j \leq d} \sqrt{p_j} X^j$, where p_j is the j-th prime number (see [11]).

Theorem 8 (Baur [2]) *There exists a positive universal constant c with the following property: let D be a natural number and let $F := \sum_{0 \leq j \leq d} f_j X^j \in \mathbb{C}[X]$ be a polynomial of degree at most d with complex coefficients. Suppose*

that there exist polynomials $g_1, \ldots, g_s \in \mathbb{Q}[X_0, \ldots, X_d]$ *of degree at most* D *such that the complex numbers* $g_1(f_0, \ldots, f_d), \ldots, g_s(f_0, \ldots, f_d)$ *are* $\mathbb{Q}$*-linearly independent. Then for any natural number* L *such that* F *belongs to the algebraic variety* $W_{d,L}$ *we have the estimate*

$$L^2 \geq c \cdot \frac{\log_2 s}{\log_2 d + \log_2 D} \quad .$$

PROOF. Let $\langle g_i(f_0, \ldots, f_d) : 1 \leq i \leq s \rangle$ be the vector space over $\mathbb{Q}$ spanned by the set $\{g_1(f_0, \ldots, f_d), \ldots, g_s(f_0, \ldots, f_d)\}$. Similarly, let $\langle f_0^{v_0} \cdots f_d^{v_d} : 0 \leq v_0 + \cdots + v_d \leq D \rangle$ be the vector space over $\mathbb{Q}$ generated by the set $\{f_0^{v_0} \cdots f_d^{v_d} : 0 \leq v_0 + \cdots + v_d \leq D\}$. Since for each i, $1 \leq i \leq s$, there exist coefficients $a_{i,v} \in \mathbb{Q}$, with $v := (v_0, \ldots, v_d) \in \mathbb{N}^{d+1}$ and $0 \leq |v| \leq D$, such that

$$g_i(f_0, \ldots, f_d) = \sum_{\substack{v:=(v_0,\ldots,v_d)\in\mathbb{N}^{d+1} \\ 0\leq|v|\leq D}} a_{i,v} \cdot f_0^{v_0} \cdots f_d^{v_d}$$

holds, we have the following inclusion between vector spaces:

$$\langle g_i(f_0, \ldots, f_d) : 1 \leq i \leq s \rangle \subseteq \langle f_0^{v_0} \cdots f_d^{v_d} : 0 \leq v_0 + \cdots + v_d \leq D \rangle \quad .$$

This inclusion and the linear independence in $\mathbb{Q}$ of the complex numbers $g_i(f_0, \ldots, f_d)$, $1 \leq i \leq s$, yield the inequality

$$\dim_{\mathbb{Q}} \langle f_0^{v_0} \cdots f_d^{v_d} : 0 \leq v_0 + \cdots + v_d \leq D \rangle \geq s \quad .$$

This inequality implies that there exist at least 2^s elements which can be expressed as sums of distinct elements of the set $\{f_0^{v_0} \cdots f_d^{v_d} : 0 \leq v_0 + \cdots + v_d \leq D\}$. From this and by Definition 3 we deduce

$$\mu((f_0, \ldots, f_d); D) \geq 2^s \quad . \tag{12}$$

Finally, let $L \in \mathbb{N}$ such that F belongs to the variety $W_{d,L}$. Then from Lemma 4 we deduce the inequality

$$\mu(F; D) \leq 2^{(D(d+1))^{20L^2}} \quad . \tag{13}$$

Combining (12) and (13) and taking logarithms twice finishes the proof. □

Theorem 8 implies that the family of polynomials with algebraic coefficients $(F_d)_{d\in\mathbb{N}}$ defined by $F_d := \prod_{1\leq j\leq d}(X - \sqrt{p_j})$, where p_j is the j-th prime number, satisfies the complexity bound $L^2(F_d) = \Omega\left(\frac{d}{\log_2 d}\right)$ (see [13]).

4 Polynomials Which Are Hard to Compute

As mentioned in the previous section, Theorem 6 yields hardness proofs for several new families of polynomials with integer coefficients, which are collected in Theorems 10, 11 and 12 below.

In the proofs of these theorems we need the following elementary fact.

Claim 9 *Let $a_1, \ldots, a_b$ be natural numbers such that $\sum_{1 \le k < j} a_k < a_j$ holds for each j, $1 \le j \le b$. Then*

$$\# \left\{ \sum_{j \in S} a_j : S \subseteq \{1, \ldots, b\} \right\} = 2^b \ .$$

PROOF. In order to prove Claim 9 it suffices to show that for any pair of different subsets S, S' of $\{1, \ldots, b\}$ the inequality $\sum_{j \in S} a_j \neq \sum_{j \in S'} a_j$ holds. Without loss of generality we may assume that the conditions $S \cap S' = \emptyset$ and $\max(S) < \max(S')$ are satisfied. Thus

$$\sum_{j \in S} a_j \le \sum_{1 \le j \le \max(S)} a_j \le \sum_{1 \le j < \max(S')} a_j < a_{\max(S')} \le \sum_{j \in S'} a_j$$

holds and therefore

$$\sum_{j \in S} a_j \neq \sum_{j \in S'} a_j \ . \qquad \square$$

Theorem 10 *Let n be a fixed positive integer number. Let φ be the Euler totient function and let $\pi(j)$ be the number of primes not exceeding j. Let $\mathcal{F} := (F_d)_{d \in \mathbb{N}}$ be the family of polynomials defined by any of the following expressions:*

$$\begin{aligned}
&(i)\ F_d := \sum_{0 \le j \le d} 2^{2^{\varphi(\lfloor \sqrt[n]{j} \rfloor)}} X^j, \\
&(ii)\ F_d := \sum_{0 \le j \le d} 2^{\varphi(\lfloor \sqrt[n]{j} \rfloor)!} X^j, \\
&(iii)\ F_d := \sum_{0 \le j \le d} 2^{2^{\pi(\lfloor \sqrt[n]{j} \rfloor)}} X^j, \\
&(iv)\ F_d := \sum_{0 \le j \le d} 2^{\pi(\lfloor \sqrt[n]{j} \rfloor)!} X^j.
\end{aligned}$$

Then the family $\mathcal{F}$ satisfies the complexity bound $L^2(F_d) = \Omega\Big(\frac{n \sqrt[n]{d}}{(\log_2 d)^2}\Big)$.

PROOF. Let $\mathcal{F} := (F_d)_{d \in \mathbb{N}}$ be the family defined by the expression (i) of the statement of Theorem 10. We are going to show that for any nonzero natural

number d the following estimate holds:

$$\#\Big\{\nu_2\Big(\prod_{j\in S} 2^{2^{\varphi(\lfloor \sqrt[n]{j}\rfloor)}}\Big) : S\subseteq\{0,\ldots,d\}\Big\} \geq 2^{\pi(\lfloor \sqrt[n]{d}\rfloor)} \ . \tag{14}$$

Therefore the complexity bound of the statement of Theorem 10 follows immediately applying Theorem 6 and the Chebyshev's Theorem (see [7, Chapter 9, Exercises 9.19–9.21]): for any natural number d, $d>1$, the following estimate holds

$$\frac{1}{6}\cdot\frac{d}{\ln d} \leq \pi(d) \leq 6\cdot\frac{d}{\ln d} \ .$$

For any $j\geq 1$, let p_j be the j-th prime number. From the inclusion

$$\Big\{p_j^n : 1\leq j\leq \pi(\lfloor\sqrt[n]{d}\rfloor)\Big\}\subset\Big\{j : 0\leq j\leq d\Big\}$$

we deduce the inclusion:

$$\Big\{\nu_2\Big(\prod_{j\in S} 2^{2^{\varphi(p_j)}}\Big) : S\subseteq\{1,\ldots,\pi(\lfloor\sqrt[n]{d}\rfloor)\}\Big\}\subseteq\Big\{\nu_2\Big(\prod_{j\in S} 2^{2^{\varphi(\lfloor \sqrt[n]{j}\rfloor)}}\Big) : S\subseteq\{0,\ldots,d\}\Big\}.$$

Therefore, to show inequality (14) it is sufficient to prove the following equality

$$\#\Big\{\nu_2\Big(\prod_{j\in S} 2^{2^{\varphi(p_j)}}\Big) : S\subseteq\{1,\ldots,\pi(\lfloor\sqrt[n]{d}\rfloor)\}\Big\} = 2^{\pi(\lfloor \sqrt[n]{d}\rfloor)} \ .$$

For this purpose, according to Claim 9, we only need to demonstrate that for any j, $1\leq j\leq\pi(\lfloor\sqrt[n]{d}\rfloor)$, the following inequality holds:

$$\nu_2\Big(\prod_{1\leq k<j} 2^{2^{\varphi(p_k)}}\Big) = \sum_{1\leq k<j}\nu_2\Big(2^{2^{\varphi(p_k)}}\Big) = \sum_{1\leq k<j} 2^{\varphi(p_k)} < 2^{\varphi(p_j)} = \nu_2\Big(2^{2^{\varphi(p_j)}}\Big) \ ,$$

which follows from the estimate

$$\sum_{1\leq k<j} 2^{\varphi(p_k)} = \sum_{1\leq k<j} 2^{p_k-1} \leq \sum_{0\leq k<p_{j-1}} 2^k = 2^{p_{j-1}}-1 < 2^{p_{j-1}} < 2^{p_j-1} = 2^{\varphi(p_j)} \ .$$

Similarly the lower bounds for the nonscalar complexity of the families of polynomials defined by the expressions (ii), (iii) and (iv) of the statement of Theorem 10 can be obtained respectively using the following estimations:

- $\displaystyle\sum_{1\leq k<j}\varphi(p_k)! = \sum_{1\leq k<j}(p_k-1)! \leq \sum_{0\leq k<p_{j-1}} k! \leq p_{j-1}! < (p_j-1)! = \varphi(p_j)!,$
- $\displaystyle\sum_{1\leq k<j} 2^{\pi(p_k)} = \sum_{1\leq k<j} 2^k = 2^j-2 < 2^j = 2^{\pi(p_j)},$
- $\displaystyle\sum_{1\leq k<j}\pi(p_k)! = \sum_{1\leq k<j} k! \leq j!-1 < j! = \pi(p_j)!$ $\qquad\square$

Theorem 11 *Let $n \geq 1$ be a fixed natural number. Let $\mathcal{F} := (F_d)_{d\in\mathbb{N}}$ be the family of polynomials defined by any of the following expressions:*

$$(i)\ F_d := \sum_{0\leq j\leq d} 2^{2^{\lfloor \sqrt[n]{j}\rfloor}} X^j,$$

$$(ii)\ F_d := \prod_{1\leq j\leq d} (X - 2^{2^{\lfloor \sqrt[n]{j}\rfloor}}),$$

$$(iii)\ F_d := \sum_{0\leq j\leq d} 2^{\lfloor \sqrt[n]{j}\rfloor !} X^j,$$

$$(iv)\ F_d := \prod_{1\leq j\leq d} (X - 2^{\lfloor \sqrt[n]{j}\rfloor !}).$$

Then the family $\mathcal{F}$ satisfies the complexity bound $L^2(F_d) = \Omega\Big(\frac{\sqrt[n]{d}}{\log_2 d}\Big)$.

PROOF. Let $\mathcal{F} := (F_d)_{d\in\mathbb{N}}$ be any of the families of polynomials defined by any of the expressions (i) or (iii). Let us write $F_d := \sum_{0\leq j\leq d} f_j X^j$ where $f_0, \ldots, f_d$ are suitable integers. We are going to show that for any nonzero natural number d the following estimate holds:

$$\#\Big\{\nu_2\Big(\prod_{j\in S} f_j\Big) : S \subseteq \{0,\ldots,d\}\Big\} \geq 2^{\lfloor \sqrt[n]{d}\rfloor} \quad . \tag{15}$$

Therefore the complexity bound of the statement of Theorem 11 for the families of polynomials defined by any of the expressions (i) or (iii) follows immediately from the application of Theorem 6 and the estimate (15).

In order to obtain the estimate (15) we observe that for any j, $1 \leq j \leq \lfloor \sqrt[n]{d}\rfloor$, the following estimations holds:

- $\displaystyle\sum_{1\leq k<j} \nu_2\Big(2^{2^k}\Big) = \sum_{1\leq k<j} 2^k = 2^j - 2 < 2^j = \nu_2\Big(2^{2^j}\Big),$
- $\displaystyle\sum_{1\leq k<j} \nu_2\Big(2^{k!}\Big) = \sum_{1\leq k<j} k! \leq j! - 1 < j! = \nu_2(2^{j!}).$

Applying Claim 9 we deduce that the equality

$$\#\Big\{\sum_{j\in S} \nu_2(f_{j^n}) : S \subseteq \{1,\ldots,\lfloor \sqrt[n]{d}\rfloor\}\Big\} = 2^{\lfloor \sqrt[n]{d}\rfloor}$$

holds for the sets constructed employing only the coefficients of the form f_{j^n}, $1 \leq j \leq \lfloor \sqrt[n]{d}\rfloor$, of the polynomials defined by the expressions (i) or (iii). Taking into account the inclusion

$$\Big\{\sum_{j\in S} \nu_2(f_{j^n}) : S \subseteq \{1,\ldots,\lfloor \sqrt[n]{d}\rfloor\}\Big\} \subseteq \Big\{\sum_{j\in S} \nu_2(f_j) : S \subseteq \{0,\ldots,d\}\Big\} \ ,$$

we deduce that estimate (15) holds for the family of polynomials defined either by the expression (i) or by the expression (iii).

Now, let $\mathcal{F} := (F_d)_{d\in\mathbb{N}}$ be any of the families of polynomials defined either by the expression (ii) or by the expression (iv). Let us write $F_d := \sum_{0\le j\le d} f_{d-j}X^j$ where $f_0,\dots,f_d$ are suitable integers. We are going to show that for any j, $1 \le j < \lfloor \sqrt[n]{d}\rfloor$, we have:

$$\sum_{1\le k<j} \nu_2(f_{(k+1)^n-1}) < \nu_2(f_{(j+1)^n-1}) \ .$$

For this purpose, we observe that the multiplicity of the roots 2^{2^j} and $2^{j!}$, $1 \le j < \lfloor \sqrt[n]{d}\rfloor$, in the polynomials F_d defined by the expressions (ii) or (iv) is exactly $(j+1)^n - j^n$.

From this last remark, we deduce the following estimations:

- $$\begin{aligned}\sum_{1\le k<j} \nu_2(f_{(k+1)^n-1}) &= \sum_{1\le k<j}\sum_{1\le l\le k}((l+1)^n - l^n)2^l \le \\ &\le \sum_{1\le k<j}((k+1)^n-k^n)\Big(\sum_{1\le l\le k}2^l\Big) = \\ &= \sum_{1\le k<j}((k+1)^n-k^n)(2^{k+1}-2) < \\ &< \sum_{1\le k\le j}((k+1)^n-k^n)2^k = \nu_2(f_{(j+1)^n-1}) \ ,\end{aligned}$$
- $$\begin{aligned}\sum_{1\le k<j} \nu_2(f_{(k+1)^n-1}) &= \sum_{1\le k<j}\sum_{1\le l\le k}((l+1)^n - l^n)l! \le \\ &\le \sum_{1\le k<j}((k+1)^n-k^n)\Big(\sum_{1\le l\le k}l!\Big) \le \\ &\le \sum_{1\le k<j}((k+1)^n-k^n)((k+1)!-1) < \\ &< \sum_{1\le k\le j}((k+1)^n-k^n)k! = \nu_2(f_{(j+1)^n-1}) \ .\end{aligned}$$

Now applying Claim 9 we deduce that the equality

$$\#\Big\{\sum_{j\in S}\nu_2(f_{(j+1)^n-1}) : S\subseteq\{1,\dots,\lfloor\sqrt[n]{d}\rfloor-1\}\Big\} = 2^{\lfloor\sqrt[n]{d}\rfloor-1}$$

holds for the sets constructed employing only the coefficients of the form $f_{(j+1)^n-1}$, $1 \le j < \lfloor\sqrt[n]{d}/2\rfloor$, of the polynomials defined by expressions (ii) or (iv). Since the following inclusion holds

$$\Big\{\sum_{j\in S}\nu_2(f_{(j+1)^n-1}) : S\subseteq\{1,\dots,\lfloor\sqrt[n]{d}\rfloor-1\}\Big\} \subseteq \Big\{\sum_{j\in S}\nu_2(f_j) : S\subseteq\{0,\dots,d\}\Big\} \ ,$$

we deduce the following inequality

$$\#\Big\{\sum_{j\in S}\nu_2(f_j) : S\subseteq\{0,\ldots,d\}\Big\}\geq 2^{\lfloor\sqrt[n]{d}\rfloor-1}$$

for any of the families of polynomials defined either by the expression (ii) or by the expression (iv), and therefore the complexity bound of the statement of Theorem 11 for these families follows immediately applying Theorem 6. $\square$

Theorem 12 *Let n be a fixed positive integer number. Let $\mathcal{F}:=(F_d)_{d\in\mathbb{N}}$ be the family of polynomials defined by any of the following expressions:*

(i) $F_d:=\displaystyle\sum_{0\leq j\leq d}2^{\mathsf{F}_{\lfloor\sqrt[n]{j}\rfloor}}X^j$,

(ii) $F_d:=\displaystyle\prod_{1\leq j\leq d}(X-2^{\mathsf{F}_{\lfloor\sqrt[n]{j}\rfloor}})$.

where F_j is the j-th Fibonacci number. Then the family $\mathcal{F}$ satisfies the complexity bound $L^2(F_d)=\Omega\Big(\frac{\sqrt[n]{d}}{\log_2 d}\Big)$.

PROOF. Let $\mathcal{F}:=(F_d)_{d\in\mathbb{N}}$ be the family defined by the expression (i). Let us write $\sum_{0\leq j\leq d}f_jX^j:=\sum_{0\leq j\leq d}2^{\mathsf{F}_{\lfloor\sqrt[n]{j}\rfloor}}X^j$ where f_j, $0\leq j\leq d$, are suitable integers. Since for $j\geq 1$ it holds

$$\sum_{1\leq k<j}\mathsf{F}_{2k}=\mathsf{F}_{2j-1}-1<\mathsf{F}_{2j}\ ,$$

we deduce from Claim 9 the following equality

$$\#\Big\{\nu_2\Big(\prod_{j\in S}f_{(2j)^n}\Big):S\subseteq\{1,\ldots,\lfloor\sqrt[n]{d}/2\rfloor\}\Big\}=$$
$$=\#\Big\{\sum_{j\in S}\mathsf{F}_{2j}:S\subseteq\{1,\ldots,\lfloor\sqrt[n]{d}/2\rfloor\}\Big\}=2^{\left\lfloor\frac{\sqrt[n]{d}}{2}\right\rfloor}\ .$$

From this last equality we deduce the estimate

$$\#\Big\{\nu_2\Big(\prod_{j\in S}f_j\Big):S\subseteq\{0,\ldots,d\}\Big\}\geq 2^{\left\lfloor\frac{\sqrt[n]{d}}{2}\right\rfloor}\ . \tag{16}$$

Finally the complexity bound for the family $\mathcal{F}$ defined by the expression (i) follows from Theorem 6 and the estimate (16).

Let $\mathcal{F}:=(F_d)_{d\in\mathbb{N}}$ be the family of polynomials defined by expression (ii). Let us write $\sum_{0\leq j\leq d}f_{d-j}X^j:=\prod_{1\leq j\leq d}(X-2^{\mathsf{F}_{\lfloor\sqrt[n]{j}\rfloor}})$ where f_j, $0\leq j\leq d$ are

suitable integers. We are going to show that the inequality

$$\sum_{1\leq k<j} \nu_2(f_{(2k+1)^n-1}) < \nu_2(f_{(2j+1)^n-1})$$

holds for any j satisfying $1 \leq j < \lfloor \sqrt[n]{d}/2 \rfloor$. For this purpose we observe that the multiplicity of the root 2^{F_j}, $1 \leq j < \lfloor \sqrt[n]{d} \rfloor$, in the polynomial F_d defined by the expression (ii) is exactly $(j+1)^n - j^n$.

From this observation we deduce that for any j, $1 \leq j < \lfloor \sqrt[n]{d}/2 \rfloor$, it holds:

$$\begin{aligned}
\sum_{1\leq k<j} \nu_2(f_{(2k+1)^n-1}) &= \sum_{1\leq k<j} \sum_{1\leq l\leq 2k} ((l+1)^n - l^n)\mathsf{F}_l \leq \\
&\leq \sum_{1\leq k<j} ((2k+1)^n - (2k)^n)\Big(\sum_{1\leq l\leq 2k} \mathsf{F}_l\Big) = \\
&= \sum_{1\leq k<j} ((2k+1)^n - (2k)^n)(\mathsf{F}_{2k+2} - 1) < \\
&< \sum_{1\leq k<j} ((2k+1)^n - (2k)^n)\mathsf{F}_{2k+2} < \\
&< \sum_{1\leq k\leq 2j} ((k+1)^n - k^n)\mathsf{F}_k = \nu_2(f_{(2j+1)^n-1}) \ .
\end{aligned}$$

Therefore, applying Claim 9 we deduce the following inequality

$$\#\Big\{\nu_2\Big(\prod_{j\in S} f_j\Big) : S \subseteq \{0,\ldots,d\}\Big\} \geq 2^{\left\lfloor \frac{\sqrt[n]{d}}{2} \right\rfloor - 1} \ . \tag{17}$$

The complexity bound for the family $\mathcal{F} := (F_d)_{d\in\mathbb{N}}$ follows now from Theorem 6 and the estimate (17). $\square$

5 Applications to Transcendental Function Theory

Our algebraic complexity method can be applied to classical questions of transcendence in number theory and geometry. Using Newton's method to approximate algebraic functions we obtain a sufficient condition (Theorem 13) for the transcendence of formal power series.

Theorem 13 *Let K be an algebraically closed field of characteristic zero and let $\sigma := \sum_{j\in\mathbb{N}} f_j X^j \in K[[X]]$ be a given formal power series. Suppose that for any positive integer c there exists a natural number k such that the open condition*

$$(f_0,\ldots,f_{2^k-1}) \notin W_{2^k-1,ck}$$

holds. Then the power series σ is transcendental over $K(X)$.

PROOF. Let us suppose that σ is algebraic over $K(X)$. Then by Bochnak *et alii* ([5, Chapter 8]) the power series series σ defines a holomorphic function around the origin. Now using the Newton's method we are able to approximate the holomorphic funtion σ. More precisely, using the construction given in [16] we conclude that there exist a positive integer c and a Zariski open subset $U \subset K$ with the following property: for any point $\alpha \in U$ belonging to the domain of σ and for any natural number k there exists a rational function ξ_k such that the initial segment of degree $2^k - 1$ of the Taylor expansion around α of ξ_k agrees with the initial segment of degree $2^k - 1$ of the Taylor expansion around α of the holomorphic function σ, namely

$$\sum_{0 \leq j \leq 2^k - 1} \frac{\xi_k^{(j)}(\alpha)}{j!} \cdot (X - \alpha)^j = \sum_{0 \leq j \leq 2^k - 1} \frac{\sigma^{(j)}(\alpha)}{j!} \cdot (X - \alpha)^j \ .$$

Moreover, in the construction of the rational function ξ_k we employ $c \cdot k$ non-scalar operations, that is $L_{\mathcal{O}_\alpha}(\xi_k) \leq c \cdot k$.

Now using Theorem 2, the previous property can be paraphrased as follows: there exist a positive integer number c and a Zariski open subset $U \subset K$ such that for any point $\alpha \in U$ belonging to the domain of σ and for any natural number k the point given by the coefficients of the Taylor polynomial of (formal) degree $2^k - 1$ in α of the holomorphic function σ belongs to the variety $W_{2^k-1,ck}$, that is,

$$\left(\sigma^{(j)}(\alpha)/j! : 0 \leq j \leq 2^k - 1\right) \in W_{2^k-1,ck} \ . \tag{18}$$

On the other hand, for the given c, according to the hypothesis of the theorem, there must exists a natural number k such that

$$(f_0, \ldots, f_{2^k-1}) \notin W_{2^k-1,ck} \ .$$

Since the power series σ is holomorphic so is any derivative $\sigma^{(j)}$ of σ, $j \in \mathbb{N}$. Then any coefficient f_j of σ, $j \in \mathbb{N}$, verifies

$$f_j = \frac{\sigma^{(j)}(0)}{j!} \ ,$$

and consequently

$$(\sigma^{(j)}(0)/j! : 0 \leq j \leq 2^k - 1) \notin W_{2^k-1,ck} \ .$$

By the continuity of $\sigma^{(j)}$ we deduce that there exists a neighbourhood of zero $V \subset K$ such that for any $\alpha \in V$ the following open condition holds:

$$\left(\sigma^{(j)}(\alpha)/j! : 0 \leq j \leq 2^k - 1\right) \notin W_{2^k-1,ck} \ .$$

But this contradicts the condition (18) which is satisfied for any point α of the Zariski open subset U if we suppose that the power series σ is algebraic. Hence σ must be transcendental. $\square$

From Lemma 4 and Theorem 13 we deduce the following criterion of transcendence.

Criterion 14 *Let K be an algebraically closed field of characteristic zero and let $\sigma := \sum_{j\in\mathbb{N}} f_j X^j \in K[[X]]$ be a given power series. Suppose that for any positive real number c there exists a natural number k such that the following inequality holds*

$$\mu((f_0,\ldots,f_{2^k-1})) > 2^{2^{ck^3}} \quad . \tag{19}$$

Then the power series σ is transcendental over $K(X)$.

PROOF. Let c be an arbitrary positive real number and let k be a natural number for which, according to the hypothesis, the inequality (19) holds.

Fixed c and k, let L be a natural number such that the point $(f_0,\ldots,f_{2^k-1})$ belongs to the variety $W_{2^k-1,L}$. Then from Lemma 4 we have

$$\mu((f_0,\ldots,f_{2^k-1})) \le 2^{2^{20kL^2}} \quad . \tag{20}$$

Combining (20) with (19) and taking logarithms twice we obtain

$$L > \sqrt{\frac{c}{20}}\cdot k \ ,$$

and from this inequality we deduce that the point $(f_0,\ldots,f_{2^k-1})$ does not belong to the variety $W_{2^k-1,c'k}$, where $c' := \left\lfloor\sqrt{\frac{c}{20}}\right\rfloor$. Since c is arbitrary, the transcendence of σ follows from Theorem 13. $\square$

From Criterion 14 we obtain the following transcendence results.

Corollary 15 *Let n be a given nonzero natural number. The following power series which belong to $\mathbb{Q}[[X]]$ are transcendental over the function field $\mathbb{C}(X)$:*

(i) $\displaystyle\sum_{j\in\mathbb{N}} \frac{1}{2^{2^{\varphi(\lfloor\sqrt[n]{j}\rfloor)}}}X^j$ *and* $\displaystyle\sum_{j\in\mathbb{N}} \frac{1}{2^{\varphi(\lfloor\sqrt[n]{j}\rfloor)!}}X^j$, *where φ is the Euler totient function.*

(ii) $\displaystyle\sum_{j\in\mathbb{N}} \frac{1}{2^{2^{\pi(\lfloor \sqrt[n]{j}\rfloor)}}}X^j$ *and* $\displaystyle\sum_{j\in\mathbb{N}} \frac{1}{2^{\pi(\lfloor \sqrt[n]{j}\rfloor)!}}X^j$, *where* $\pi(j)$ *is the number of primes not exceeding* j.

(iii) $\displaystyle\sum_{j\in\mathbb{N}} \frac{1}{2^{2^{\lfloor \sqrt[n]{j}\rfloor}}}X^j$ *and* $\displaystyle\sum_{j\in\mathbb{N}} \frac{1}{2^{\lfloor \sqrt[n]{j}\rfloor!}}X^j$.

(iv) $\displaystyle\sum_{j\in\mathbb{N}} \frac{1}{2^{\mathsf{F}_{\lfloor \sqrt[n]{j}\rfloor}}}X^j$, *where* F_j *denotes the* j*-th Fibonacci number.*

(v) $\displaystyle\sum_{j\in\mathbb{N}} \frac{1}{2^{2^{\lfloor(\log_2(j+1))^n\rfloor}}}X^j$, *for* $n \geq 4$.

PROOF. First of all we observe that, according to Definition 3, the equality

$$\mu((a_1^{-1},\ldots,a_b^{-1})) = \mu((a_1,\ldots,a_b)) \tag{21}$$

holds for any nonzero elements a_j, $1 \leq j \leq b$, of the field K.

Let $\sigma := \sum_{j\in\mathbb{N}} f_j^{-1}X^j$ be any of the power series of (i) or (ii). For any natural number k the estimate (14) and Claim 5 imply

$$\mu((f_j : 0 \leq j \leq 2^k-1)) \geq 2^{2^{\pi(\lfloor \sqrt[n]{2^k-1}\rfloor)}} \quad .$$

Then from (21), the inequality

$$\mu((f_j^{-1} : 0 \leq j \leq 2^k-1)) \geq 2^{2^{\pi(\lfloor \sqrt[n]{2^k-1}\rfloor)}}$$

holds for any natural number k and therefore the transcendence of the series σ follows from Criterion 14 and Chebyshev's Theorem.

Employing estimations (15) and (16) in a similar way we deduce from Criterion 14 the transcendence of the power series of (iii) and (iv).

In order to prove the transcendence of the power series of (v) we are going to demonstrate that the inequality

$$\#\left\{\nu_2\Big(\prod_{j\in S} 2^{2^{\lfloor(\log_2 j)^n\rfloor}}\Big) : S \subseteq \{1,\ldots,2^k\}\right\} \geq 2^{k^n-\lambda(n)+1} \quad , \tag{22}$$

holds for any natural number k, where $\lambda(n) := \left\lceil \frac{1}{2}\left(\frac{(2n)!}{(\ln 2)^{2n}} - 1\right)\right\rceil$. From Claim 5 we deduce that to prove the estimate (22) it is sufficient to show that the estimate

$$\#\left\{\lfloor(\log_2 j)^n\rfloor : 1 \leq j \leq 2^k\right\} \geq k^n - \lambda(n) + 1$$

holds for any natural number k. Fixed k, this estimate is satisfied if for any natural number l such that $\lambda(n) \leq l \leq k^n$ there exists a natural number j, $1 \leq j \leq 2^k$, such that the inequalities

$$2^{\sqrt[n]{l}} \leq j < 2^{\sqrt[n]{l+1}} \tag{23}$$

hold. To prove (23), we consider $2^{\sqrt[n]{l+1}}$ and $2^{\sqrt[n]{l}}$ as functions in l. Expanding them in power series and retaining only the $(2n)$-th term in the expansions we obtain the following inequality:

$$\begin{aligned} 2^{\sqrt[n]{l+1}} - 2^{\sqrt[n]{l}} &= \sum_{i\in\mathbb{N}} \frac{((l+1)^{\frac{1}{n}} \ln 2)^i}{i!} - \sum_{i\in\mathbb{N}} \frac{(l^{\frac{1}{n}} \ln 2)^i}{i!} \geq \\ &\geq \frac{(\ln 2)^{2n}}{(2n)!} \cdot (l+1)^2 - \frac{(\ln 2)^{2n}}{(2n)!} \cdot l^2 = \frac{(\ln 2)^{2n}}{(2n)!} \cdot (2l+1) \ . \end{aligned}$$

Now taking l such that $l \geq \frac{1}{2}\left(\frac{(2n)!}{(\ln 2)^{2n}} - 1\right)$ we deduce the inequality

$$2^{\sqrt[n]{l+1}} - 2^{\sqrt[n]{l}} \geq 1$$

and this is sufficient to guarantee the existence of a natural number j such that (23) holds.

For any natural number k, the estimate (22) and Claim 5 yield the inequality

$$\mu((2^{2^{\lfloor (\log_2 j)^n \rfloor}} : 1 \leq j \leq 2^k)) \geq 2^{2^{k^n - \lambda(n)+1}} \ .$$

From this inequality and (21), we finally deduce that the inequality

$$\mu((2^{-2^{\lfloor (\log_2 j)^n \rfloor}} : 1 \leq j \leq 2^k)) \geq 2^{2^{k^n - \lambda(n)+1}}$$

holds for any natural number k. The transcendence of power series of (v) now follows from Criterion 14. $\square$

References

[1] M. Aldaz, J. Heintz, G. Matera, J.L. Montaña and L.M. Pardo, Time-space tradeoffs in algebraic complexity theory, *Journal of Complexity* (2000, to appear).

[2] W. Baur, Simplified lower bounds for polynomials with algebraic coefficients, *Journal of Complexity*, **13** (1997) 38–41.

[3] E.G. Belaga, Some problems involved in the computations of polynomials, *Dokl. Akad. Nauk. SSSR*, **123** (1958) 775–777.

[4] L. Blum, F. Cucker, M. Shub and S. Smale, *Real Complexity and Computation* (Springer, Berlin, 1998).

[5] J. Bochnak, M. Coste and M.F. Roy. *Géométrie Algébrique Réelle*, Ergebnisse der Mathematik und ihrer Grenzgebiete vol. 12 (Springer, Berlin, 1987).

[6] A. Borodin and I. Munro, *The Computational Complexity of Algebraic and Numeric Problems* (Elsevier, 1975).

[7] P. Bürguisser, M. Clausen and M.A. Shokrollahi, *Algebraic Complexity Theory*, Comprehensive Studies in Mathematics vol. 315 (Springer, Berlin, 1997).

[8] N. Fitchas, A. Galligo and J. Morgenstern, Precise sequential and parallel complexity bounds for the quantifier elimination over algebraically closed fields, *Journal of Pure and Applied Algebra* **67** (1990) 1–14.

[9] N. Fitchas, M. Giusti and F. Smietanski, Sur la complexitè du Thèoréme des Zèros, in: B. Brosowski, F. Deutsch and J. Guddat, eds., *Proceedings Second International Conference on Non-Linear Optimization and Approximation* (Peter Lange, 1995) 274–329.

[10] J. von zur Gathen, Algebraic complexity theory, *Ann. Review of Computer Science* **3** (1988) 317–347, .

[11] J. von zur Gathen and V. Strassen, Some polynomials which are hard to compute, *Theoretical Computer Science* **11**(3) (1980) 331–335.

[12] J. Heintz, On the computational complexity of polynomials and bilinear mappings. a survey, in: L. Huget and A. Poli, eds., *Proceedings 5th International Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes, AAECC-5*, Lecture Notes in Computer Science vol. 356 (Springer, Berlin, 1989) 269–300.

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

[14] J. Heintz and M. Sieveking, Lower bounds for polynomials with algebraic coefficients, *Theoretical Computer Science* **11**(3) (1980) 321–330.

[15] T. Krick and L.M. Pardo, A computational method for diophantine approximation, in: L. González-Vega and T. Recio, eds., *Proceedings MEGA'94 Algorithms in Algebraic Geometry and Applications* (1996) 193–254.

[16] H.T. Kung and J.F. Traub, All algebraic functions can be computed fast, *Journal of the ACM* **25**(2) (1978) 245–260.

[17] R.J. Lipton, Straight-line complexity and integer factorization, in: L.M. Adleman and M.D. Huang, eds., *Proceedings First International Symposium on Algorithmic Number Theory, ANTS-I*, Lecture Notes in Computer Science vol. 877, (Springer, Berlin, 1994) 71–79.

[18] T.S. Motzkin, Evaluation of polynomials and evaluation of rational functions, *Bulletin of American Mathematical Society* **61** (1955) 163.

[19] L.M. Pardo, How lower and upper complexity bounds meet in elimination theory, in: G. Cohen, M. Giusti and T. Mora, eds., *Proceedings 11th International Symposium on Applied Algebra, Algebraic Algorithms and Error Correcting Codes, AAECC-11*, Lecture Notes in Computer Science vol. 948, (Springer, Berlin, 1995) 33–69.

[20] M.S. Paterson and L.J. Stockmeyer, On the number of nonscalar multiplications necessary to evaluate polynomials, *SIAM Journal on Computing* **2** (1973) 60–66.

[21] S. Puddu and J. Sabia, An effective algorithm for quantifier elimination over algebraically closed fields using straight-line programs, *Journal of Pure and Applied Algebra* **129**(2) (1998) 173–200.

[22] C.P. Schnorr, Improved lower bounds on the number of multiplications-divisions which are necessary to evaluate polynomials, *Theoretical Computer Science* **7**(3) (1978) 251–261.

[23] V. Shoup and R. Smolensky, Lower bounds for polynomial evaluation and interpolation problems, in *Proceedings 31st Annual IEEE Symposium on Foundations of Computer Science* (1991) 378–383, 1991.

[24] H.J. Stoss, On the representation of rational functions of bounded complexity, *Theoretical Computer Science* **64** (1989) 1–13.

[25] V. Strassen, Polynomials with rational coefficients which are hard to compute, *SIAM Journal on Computing* **3**(2) (1974) 128–149.

[26] V. Strassen, Algebraic Complexity Theory, in *Handbook of Theoretical Computer Science* (Elsevier Science, Amsterdam, 1990) 634–672.