Combinatorial Hardness Proofs for Polynomial Evaluation*
(Extended Abstract)

Mikel Aldaz\(^1\), Joos Heintz\(^2,3\), Guillermo Matera\(^3,4\), José L. Montaña\(^1\), and Luis M. Pardo\(^2\)

\(^1\) Universidad Pública de Navarra, Departamento de Matemática e Informática, 31006 Pamplona, Spain mikaldaz, pepe@upna.es
\(^2\) Universidad de Cantabria, Fac. de Ciencias, Depto. de Matemáticas, Est. y Comp., 39071 Santander, Spain heintz, pardo@matesco.unican.es
\(^3\) Universidad de Buenos Aires, FCEyN, Departamento de Matemáticas, (1428) Buenos Aires, Argentina joos, gmatera@dm.uba.ar
\(^4\) Universidad Nacional de Gral. Sarmiento, Instituto de Desarrollo Humano, (1663) San Miguel, Argentina.

Abstract. We exhibit a new method for showing lower bounds for the time complexity of polynomial evaluation procedures. Time, denoted by \(L\), is measured in terms of nonscalar arithmetic operations. The time complexity function considered in this paper is \(L^2\). 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 transcendency can be shown easily by our method.

1 Background and Results

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.

* Work partially supported by spanish DGCYT grant PB 96–0671–C02–02.
Following Motzkin ([1955]), Belaga ([1958]) and Paterson-Stockmeyer ([1973]) “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 constant $c > 0$ 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 limitations for the generality of our statements.

Families of specific polynomials which are hard to compute where first considered by Strassen ([1974]). The method used in Strassen ([1974]) was later refined by Schnorr ([1978]) and Stoss ([1989]). Heintz & Sieveking ([1980]) 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 Heintz & Morgenstern ([1993]) the method of Heintz-Sieveking was adapted to polynomials given by their roots and this adaption was considerably simplified in Baur ([1997]).

Finally the methods of Strassen ([1974]) and Heintz & Sieveking ([1980]) were unified to a common approach in Aldaz et al. ([1996]). This new approach was based on effective elimination and intersection theory with their implications for diophantine geometry (see e.g. Fitchas et al. ([1990]), Krick & Pardo ([1996]) and Puddu & Sabia ([1997])). 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 simplified version of the unified approach mentioned before. Geometric considerations are replaced by simple counting arguments which make our new method more flexible and adaptive. Our new method is inspired in Shoup & Smolensky ([1991]) and Baur ([1997]) and relies on a counting technique developed in Strassen ([1974]) (see also Schnorr ([1978]) and Stoss ([1989])). Except for this result (see Theorem 1) our method (Lemma 1) is elementary and requires only basic knowledge of algebra.

## 2 A General Lower Bound for the Nonscalar Complexity of Rational Functions

Let $K$ be an algebraic 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 $\alpha$ 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 $g(\alpha) \neq 0$. 