Contents lists available at ScienceDirect

Journal of Complexity

journal homepage: www.elsevier.com/locate/jco

# Lower bounds by Birkhoff interpolation[☆]

Ignacio García-Marco[*], Pascal Koiran

*LIP,[1] Ecole Normale Supérieure de Lyon, France*

ARTICLE INFO

*Article history:*
Received 8 February 2016
Accepted 6 October 2016
Available online xxxx
Communicated by L. Pardo

*Keywords:*
Polynomial interpolation
Waring problem
Arithmetic circuit
Lower bounds
Real polynomial

ABSTRACT

In this paper we give lower bounds for the representation of real univariate polynomials as sums of powers of degree 1 polynomials. We present two families of polynomials of degree $d$ such that the number of powers that are required in such a representation must be at least of order $d$. This is clearly optimal up to a constant factor. Previous lower bounds for this problem were only of order $\Omega(\sqrt{d})$, and were obtained from arguments based on Wronskian determinants and “shifted derivatives”. We obtain this improvement thanks to a new lower bound method based on Birkhoff interpolation (also known as “lacunary polynomial interpolation”).

## 1. Introduction

In this paper we obtain lower bounds for the representation of a univariate polynomial $f \in \mathbb{R}[X]$ of degree $d$ under the form:

$$f(x) = \sum_{i=1}^{l} \beta_i (x + y_i)^{e_i} \tag{1}$$

where the $\beta_i$, $y_i$ are real constants and the exponents $e_i$ nonnegative integers.

We give two families of polynomials such that the number $l$ of terms required in such a representation must be at least of order $d$. This is clearly optimal up to a constant factor. Previous lower bounds for this problem [12] were only of order $\Omega(\sqrt{d})$. The polynomials in our first family are of the form

[☆] This work was supported by ANR project CompA (project number: ANR-13-BS02-0001-01).

[*] Corresponding author.
*E-mail addresses:* iggarcia@ull.es (I. García-Marco), pascal.koiran@ens-lyon.fr (P. Koiran).

[1] UMR 5668 ENS Lyon-CNRS-UCBL-INRIA, Université de Lyon.

http://dx.doi.org/10.1016/j.jco.2016.10.001
0885-064X/© 2016 Elsevier Inc. All rights reserved.

Please cite this article in press as: I. García-Marco, P. Koiran, Lower bounds by Birkhoff interpolation, Journal of Complexity (2016), http://dx.doi.org/10.1016/j.jco.2016.10.001

$H_1(x) = \sum_{i=1}^{k} \alpha_i (x + x_i)^d$ with all $\alpha_i$ nonzero and the $x_i$'s distinct. We show that they require at least $l \geq k$ terms whenever $k \leq (d+2)/4$. In particular, for $k = (d+2)/4$ we obtain $l = k = (d+2)/4$ as a lower bound. The polynomials in our second family are of the form $H_2(x) = (x+1)^{d+1} - x^{d+1}$ and we show that they require more than $(d-1)/2$ terms. This improves the lower bound for $H_1$ by a factor of 2, but this second lower bound applies only when the exponents $e_i$ are required to be bounded by $d$ (obviously, if larger exponents are allowed we only need two terms to represent $H_2$). It is easily shown that every polynomial of degree $d$ can be represented with $\lceil (d+1)/2 \rceil$ terms. This implies that of all polynomials of degree $d$, $H_2$ is essentially (up to a small additive constant) the hardest one.

Our lower bound results are specific to polynomials with real coefficients. It would be interesting to obtain similar lower bounds for other fields, e.g., finite fields or the field of complex numbers. As an intermediate step toward our lower bound theorems, we obtain a result on the linear independence of polynomials which may be of independent interest.

**Theorem 1.** *Let $f_1, \ldots, f_k \in \mathbb{R}[X]$ be $k$ distinct polynomials of the form $f_i(x) = (x + a_i)^{e_i}$. Let us denote by $n_j$ the number of polynomials of degree less than $j$ in this family.*

*If $n_1 \leq 1$ and $n_j + n_{j-1} \leq j$ for all $j$, the family $(f_i)$ is linearly independent.*

We will see later (in Section 4, Remark 17) that this theorem is optimal up to a small additive constant when $d$ is even, and exactly optimal when $d$ is odd.

### *Motivation and connection to previous work*

Lower bounds for the representation of univariate polynomials as sums of powers of *low degree* polynomials were recently obtained in Kayal et al. [12]. We continue this line of work by focusing on powers of *degree one* polynomials. This problem is still challenging because the exponents $e_i$ may be different from $d = \deg(f)$, and may be possibly larger than $d$. The lower bounds obtained in Kayal et al. [12] are of order $\Omega(\sqrt{d})$. We obtain $\Omega(d)$ lower bounds with a new method based on polynomial interpolation (more on this below).

The work in Kayal et al. [12] and in the present paper is motivated by recent progress in arithmetic circuit complexity. It was shown that strong enough lower bounds for circuits of depth four [1,15,20] or even depth three [10,20] would yield a separation of Valiant's [21] algebraic complexity classes VP and VNP. Moreover, lower bounds for such circuits were obtained thanks to the introduction by Neeraj Kayal of the method of *shifted partial derivatives*, see e.g. [11,8,9,13,14,16,17]. Some of these lower bounds seem to come close to separating VP from VNP, but there is evidence that the method of shifted derivatives by itself will not be sufficient to achieve this goal. In fact, this method cannot prove more than a $1.5m^2$ lower bound on the determinantal complexity of the $m \times m$ permanent [7]. It is therefore desirable to develop new lower bounds methods. We view the models studied in Kayal et al. [12] and in the present paper as "test beds" for the development of such methods in a fairly simple setting. We note also that (as explained above) strong lower bounds in slightly more general models would imply a separation of VP from VNP. Indeed, if the affine functions $x + y_i$ in (1) are replaced by multivariate affine functions we obtain the model of "depth 3 powering arithmetic circuits". In general depth 3 arithmetic circuits, instead of powers of affine functions we have products of (possibly distinct) affine functions. We note that the depth reduction result of Gupta et al. [10] yields circuits where the number of factors in such products can be much larger than the degree of the polynomial represented by the circuit. It is therefore quite natural to allow exponents $e_i > d$ in (1). Likewise, the model studied in Kayal et al. [12] is close to depth 4 arithmetic circuits, see Kayal et al. [12] for details.

### *Birkhoff interpolation*

As mentioned above, our results are based on polynomial interpolation and more precisely on Birkhoff interpolation (also known as "lacunary interpolation"). The most basic form of polynomial interpolation is Lagrange interpolation. In a typical Lagrange interpolation problem, one may have to find a polynomial $g$ of degree at most 2 satisfying the 3 constraints $g(-1) = 1$, $g(0) = 4$, $g(1) = 3$. At a slightly higher level of generality we find Hermite interpolation, where at each point we must