ARTICLE IN PRESS

Journal of Complexity ▮ (▮▮▮▮) ▮▮▮–▮▮▮

Contents lists available at ScienceDirect

Journal of Complexity

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

On the linear independence of shifted powers[☆]

Pascal Koiran [a], Timothée Pecatte [a], Ignacio García-Marco [b,*]

[a] LIP,[1] Ecole Normale Supérieure de Lyon, Université de Lyon, France
[b] I2M, Aix-Marseille Université, France

ARTICLE INFO

Article history:
Received 16 May 2017
Accepted 23 October 2017
Available online xxxx

Keywords:
Linear independence
Wronskian
Shifted differential equation
Real and complex polynomial
Birkhoff interpolation
Waring rank

ABSTRACT

We call *shifted power* a polynomial of the form $(x - a)^e$. The main goal of this paper is to obtain broadly applicable criteria ensuring that the elements of a finite family F of shifted powers are linearly independent or, failing that, to give a lower bound on the dimension of the space of polynomials spanned by F. In particular, we give simple criteria ensuring that the dimension of the span of F is at least $c.|F|$ for some absolute constant $c < 1$. We also propose conjectures implying the linear independence of the elements of F. These conjectures are known to be true for the field of real numbers, but not for the field of complex numbers. The verification of these conjectures for complex polynomials directly imply new lower bounds in algebraic complexity.

1. Introduction

In this article, we consider families of univariate polynomials of the form:

$$F = \{(x - a_i)^{e_i} \ : \ 1 \leq i \leq s\},$$

where $e_i \in \mathbb{N}$ and the a_i belong to a field $\mathbb{K}$ of characteristic 0. An element of F will be called a *shifted power* (polynomials of this form are also called *affine powers* in [7]). We always assume that $(a_i, e_i) \neq (a_j, e_j)$ for $i \neq j$, i.e. that F does not contain the same element twice.

[☆] Communicated by L. Pardo.

[*] Correspondence to: Aix-Marseille Université, I2M UMR 7373, Case Courrier 907, 163 avenue de Luminy, 13288 Marseille Cedex 9, France.

E-mail addresses: Pascal.Koiran@ens-lyon.fr (P. Koiran), Timothee.Pecatte@ens-lyon.fr (T. Pecatte), iggarcia@ull.es (I. García-Marco).

[1] UMR 5668 Ecole Normale Supérieure de Lyon, CNRS, UCBL, INRIA.

https://doi.org/10.1016/j.jco.2017.11.002
0885-064X/© 2017 Elsevier Inc. All rights reserved.

Please cite this article in press as: P. Koiran, et al., On the linear independence of shifted powers, Journal of Complexity (2017), https://doi.org/10.1016/j.jco.2017.11.002.

The main goal of this paper is to obtain broadly applicable criteria ensuring that the elements of F are linearly independent or, failing that, to give a lower bound on the dimension of the space of polynomials spanned by F. For instance, we have the following well-known result for the case of equal exponents.

Proposition 1.1 (*Folklore*). *For any integer d, for any distinct $(a_i) \in \mathbb{K}^{d+1}$, the family $\{(x-a_0)^d, \ldots, (x-a_d)^d\}$ is a basis of the space of polynomials of degree at most d.*

This can be shown for instance by checking that the Wronskian determinant of the family is not identically 0. Nullity of the Wronskian is a necessary and sufficient condition for the linear independence of polynomials [3,4,12], so our problem always reduces in principle to the verification that the Wronskian of F is nonzero. Unfortunately, the resulting determinant looks hardly manageable in general. As a result, little seems to be known in the case of unequal exponents (the case of equal exponents is tractable because the Wronskian determinant becomes a Vandermonde matrix after multiplication of rows by constants). One exception is the so-called Jordan's lemma [8] (see [9, Lemma 1.35] for a recent reference), which provides the following generalization of Proposition 1.1:

Lemma 1.2. *Let $d \in \mathbb{Z}^+$, $e_1, \ldots, e_t \in \{1, \ldots, d\}$, and let $a_1, \ldots, a_t \in \mathbb{K}$ be distinct constants. If $\sum_{i=1}^{t}(d+1-e_i) \leq d+1$, then the elements of*

$$\bigcup_{i=1}^{t} \left\{(x-a_i)^{e_i},\ (x-a_i)^{e_i+1}, \ldots, (x-a_i)^d\right\}$$

are linearly independent.

So far, we have only discussed sufficient conditions for linear independence. The following "Pólya condition" is an obvious *necessary condition*:

Definition 1.3. For a sequence $e = (e_1, \ldots, e_s)$ of integers, let $n_i = |\{j : e_j < i\}|$. We say that e satisfies the Pólya condition if $n_i \leq i$ for all i.

For a family $F = \{(x-a_i)^{e_i} : 1 \leq i \leq s\}$, we say that F satisfies the Pólya condition if $e = (e_1, \ldots, e_s)$ does.

The name *Pólya condition* is borrowed from the theory of Birkhoff interpolation [14,6]. This necessary condition for linear independence is not sufficient: for instance we have the linear dependence relation $(x+1)^2-(x-1)^2-4x = 0$. As we shall see later, the Pólya condition turns out to be sufficient in a probabilistic sense: if the shifts a_i are taken uniformly at random, the resulting family is linearly independent with high probability. As pointed out above, little is known about deterministic sufficient conditions for linear independence. But there is an exception when $\mathbb{K}$ is the field of real numbers: in this case, some recent progress was made in [6] thanks to a connection between Birkhoff interpolation and linear independence of shifted powers.

In particular, the authors showed that the Pólya condition is only a factor of 2 away from being also a sufficient condition for linear independence:

Theorem 1.4 (*Theorem 3 in [6]*). *Let F and the n_i's be as in Definition 1.3, and let $d = \max e_i$. If all the a_i's are real, and $n_1 \leq 1$, $n_j + n_{j+1} \leq j+1$ for all $j = 1 \ldots d$, then the elements of F are linearly independent.*

They also gave an example of linear dependence that violates only one of the inequalities of Theorem 1.4, showing that this result is essentially optimal.

Theorem 1.4 fails badly over the field of complex numbers, as shown by this example from [6].

Proposition 1.5. *Take $k \in \mathbb{Z}^+$ and let ξ be a kth primitive root of unity. Then, for all $d \in \mathbb{Z}^+$ and all $\mu \in \mathbb{C}$ the following equality holds:*

$$\sum_{j=1}^{k} \xi^j (x+\xi^j \mu)^d = \sum_{\substack{i \equiv -1 \pmod{k} \\ 0 \leq i \leq d}} k \binom{d}{i} \mu^i x^{d-i}. \tag{1}$$

Please cite this article in press as: P. Koiran, et al., On the linear independence of shifted powers, Journal of Complexity (2017), https://doi.org/10.1016/j.jco.2017.11.002.