Theoretical Computer Science ••• (••••) •••–•••

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

Polynomial functions over finite commutative rings

Balázs Bulyovszky, Gábor Horváth *

Institute of Mathematics, University of Debrecen, Pf. 400, Debrecen, 4002, Hungary

A R T I C L E I N F O

Article history:
Received 30 March 2017
Received in revised form 23 July 2017
Accepted 4 September 2017
Available online xxxx
Communicated by V. Pan

Keywords:
Polynomial functions
Local rings
Interpolation

A B S T R A C T

We prove a necessary and sufficient condition for a function being a polynomial function over a finite, commutative, unital ring. Further, we give an algorithm running in quasilinear time that determines whether or not a function given by its function table can be represented by a polynomial, and if the answer is yes then it provides one such polynomial.

1. Introduction

It is well-known that given finitely many pairs (a_i, b_i) $(0 \le i \le n)$ over a field, there exists a polynomial p of degree at most n such that $p(a_i) = b_i$ for all $0 \le i \le n$. Several classical interpolation methods exist e.g. by Lagrange, by Newton or by Hermite to name a few. A direct consequence of these results is that an arbitrary function over a finite field can be represented by a polynomial. These methods, however, do not generalize in a straightforward manner to commutative rings. In fact, not even every function can be represented by a polynomial over a finite commutative ring which is not a field. The question arises naturally: given a finite ring R and a function $f: R \to R$, does there exist a polynomial $p \in R[x]$ such that $p(r) = f(r)$ for every $r \in R$, and if such polynomial exists, then how could one find such a polynomial?

Carlitz [1] gave several necessary and sufficient conditions for a function over $\mathbb{Z}_{p^t}$ being a polynomial function. For example, a function $f: \mathbb{Z}_{p^t} \to \mathbb{Z}_{p^t}$ is a polynomial function if and only if there exists $\phi_0, \ldots, \phi_{t-1}: \mathbb{Z}_{p^t} \to \mathbb{Z}_{p^t}$ such that

$$f(r + sp) = \phi_0(r) + (sp)\phi_1(r) + \cdots + (sp)^{t-1}\phi_{t-1}(r)$$

holds for every $r, s \in \mathbb{Z}_{p^t}$. Several generalizations of this result have been proved since, e.g by Spira [2] or later by Jiang, Peng, Sun and Zhang [3]. Note, however, that such a condition is not useful from an algorithmic perspective as it does not help finding a polynomial representing the input function f.

Guha and Dukkipati [4] gave an algorithmically useful necessary and sufficient condition for a function $f: \mathbb{Z}_{p^t} \to \mathbb{Z}_{p^t}$ being a polynomial function. Let $u_0: \mathbb{Z}_{p^t} \to \mathbb{Z}_{p^t}$ be the function defined by

$$u_0(r) = \begin{cases} 0, & \text{if } p \nmid r, \\ 1, & \text{if } p \mid r, \end{cases}$$

and let $u_k: \mathbb{Z}_{p^t} \to \mathbb{Z}_{p^t}$ $(1 \le k \le t-1)$ be

* Corresponding author.
E-mail addresses: bulyovszkyb@hotmail.com (B. Bulyovszky), ghorvath@science.unideb.hu (G. Horváth).

http://dx.doi.org/10.1016/j.tcs.2017.09.002

$$u_k(r) = \begin{cases} 0, & \text{if } p \nmid r, \\ r^k, & \text{if } p \mid r. \end{cases}$$

Then f can be represented by a polynomial if and only if it is a linear combination of $u_0, \ldots, u_{t-1}$ and their shifts. Further, they gave an algorithm running in $O\left(p^t t + pt^3\right)$ time finding a polynomial representing f if one exists. Later they generalized their results to functions over $\mathbb{Z}_n$ [5]. Both papers [4,5] are based on Carlitz's result [1].

In this paper we generalize the results of Guha and Dukkipati [4,5] to arbitrary finite, commutative, unital rings. Our proof is direct and is not based on Carlitz's result [1]. Further, we provide an algorithm running in quasilinear time (in the size of the ring) that determines whether or not a function (over a finite, commutative, unital ring) given by its function table can be represented by a polynomial, and if yes then computes one such polynomial, as well.

As every finite commutative, unital ring is a direct sum of local rings [6, Theorem VI.2], one only needs to consider these problems over finite, commutative, unital, local rings. In Section 2 we recall some basic facts necessary for our work. In particular, in Section 2.1 we summarize the most important properties of local rings, introduce functions $u_0, \ldots, u_{t-1}$ for local rings and prove that they are indeed polynomial functions. In Section 3 we generalize Guha and Dukkipati's necessary and sufficient condition from [4] to arbitrary finite, commutative, unital, local rings by proving the following.

Theorem 1. *Let R be a finite, commutative, unital, local ring with maximal ideal M. Let t be the smallest positive integer for which $M^t = \{0\}$. Let $f: R \to R$ be an arbitrary function. Then f is a polynomial function over R if and only if f can be written as a linear combination of the shifts of $u_0, \ldots, u_{t-1}$, where u_0 is the characteristic function of M, and $u_k(x) = x^k u_0(x)$ $(1 \le k \le t-1)$.*

Let $f: R \to R$ be an arbitrary function given by its function table. That is, f is given as the set of pairs $(r, f(r))$ for all $r \in R$, and the size of f is $O(|R|)$. In Section 4 we provide an algorithm that runs in quasilinear time in $|R|$, determines whether or not f is a polynomial function, and if yes then computes a polynomial representing f.

Theorem 2. *Let R be a finite, commutative, unital, local ring with maximal ideal M. Let t be the smallest positive integer for which $M^t = \{0\}$. Let $f: R \to R$ be an arbitrary function given by its function table. Then there exists an algorithm that decides whether or not f is a polynomial function, and if yes, then gives a polynomial that represents f, and the running time of this algorithm is*

$$T \le \begin{cases} O\left(|R|t\right), & \text{if } M \text{ is a principal ideal, and } |R/M| \ge t, \\ O\left(|R|t^2\right), & \text{if } M \text{ is a principal ideal, and } |R/M| < t, \\ O\left(|R|t^2 \log^3 |M|\right), & \text{if } M \text{ is not a principal ideal.} \end{cases}$$

Here and throughout the paper by log we mean base 2 logarithm. The running time of our algorithm is similar to that of Guha and Dukkipati [4,5] for $\mathbb{Z}_{p^t}$, $p \ge t$. We need the notion of Galois rings in our algorithm, therefore we recall their main properties in Section 2.2.

2. Preliminaries

Let R be a finite, commutative, unital ring. A polynomial $p \in R[x]$ naturally induces a function $p_f: R \to R$ by substitution. A function $f: R \to R$ is a *polynomial function* if there exists a polynomial $p_f \in R[x]$ such that $p_f(r) = f(r)$ for every $r \in R$. Every finite commutative, unital ring is a direct sum of local rings [6, Theorem VI.2]. Therefore, to understand polynomial functions over an arbitrary finite, commutative, unital ring, it is enough to consider local rings in the following.

2.1. Local rings

A ring is local if it has a unique maximal ideal. We summarize some of the most important properties of local rings by [6, Chapter V]. Let R be a finite, commutative, unital, local ring with maximal ideal M. Let t denote the smallest positive integer for which $M^t = \{0\}$. Note, that the quotient R/M is a field, and for the set of invertible elements we have $R^\times = R \setminus M$. Further, if $M = (m)$ is a principal ideal, then every $r \in R$ can be written in the form sm^i for some $s \in R^\times$ and $0 \le i \le t$, and then all ideals of R are principal ideals generated by m^i for some $0 \le i \le t$.

Let $r \in R$ and $f: R \to R$ be an arbitrary function. Let the shift of f by r be the function $f_r: R \to R$, $f_r(x) = f(x - r)$. Note that if $f, g: R \to R$ are polynomial functions, then $f + g, r \cdot f$ and f_r are polynomial functions, as well (for every $r \in R$).

Let $u_1, \ldots, u_k: R \to R$ be arbitrary functions. Let $\langle u_1, \ldots, u_k \rangle$ denote the set of functions that can be written as a linear combination of shifts of $u_1, \ldots, u_k$ with coefficients from R.

For every $k \in \{0, \ldots, t-1\}$ let $u_k: R \to R$ be the function defined as

$$u_0(x) = \begin{cases} 0, & \text{if } x \notin M, \\ 1, & \text{if } x \in M, \end{cases} \tag{1}$$

and