Theoretical Computer Science 579 (2015) 88–99

Contents lists available at ScienceDirect

Theoretical Computer Science

www.elsevier.com/locate/tcs

A faster algorithm for testing polynomial representability of functions over finite integer rings

Ashwin Guha, Ambedkar Dukkipati *

Department of Computer Science and Automation, Indian Institute of Science, Bangalore 560012, India

ARTICLE INFO

Article history:
Received 31 July 2014
Received in revised form 9 February 2015
Accepted 10 February 2015
Available online 18 February 2015
Communicated by V.Y. Pan

Keywords:
Polynomial functions
Finite integer rings
Kempner function

ABSTRACT

Given a function from $\mathbb{Z}_n$ to itself one can determine its polynomial representability by using Kempner function. In this paper we present an alternative characterization of polynomial functions over $\mathbb{Z}_n$ by constructing a generating set for the $\mathbb{Z}_n$-module of polynomial functions. This characterization results in an algorithm that is faster on average in deciding polynomial representability. We also extend the characterization to functions in several variables.

1. Introduction

In this paper we deal with the following question: given a function from a finite integer ring to itself does there exist a polynomial that evaluates to the function? In the case of real numbers $\mathbb{R}$, if the function is specified at only a finite number of points it is possible to obtain a polynomial using Lagrange interpolation [11]. For analytic functions one may get an approximation using Taylor's series. This problem has been well-studied over finite fields as well. It was noted by Hermite [7] that every function over finite field of the form $\mathbb{Z}_p$, which is the set of integers modulo prime p, can be represented by a polynomial. This result was extended by Dickson [5] to finite fields F_q, where q is a prime power. Moreover, it was also shown that there exists a unique polynomial of degree less than q that evaluates to the given function. A thorough study of finite fields can be found in [12].

The property of polynomial representability does not hold over finite commutative rings. In this paper we study the problem of polynomial representability over finite integer rings $\mathbb{Z}_n$, which is the set of residue classes of $\mathbb{Z}$ modulo n.

The earliest work in this direction was by Kempner [10]. It was proved that the only residue class rings over which all functions can be represented by polynomials are $\mathbb{Z}_p$, where p is prime. Kempner [10] also introduced the function (sometimes referred to as Smarandache function) defined as follows.

Definition 1.1. Kempner function $\mu : \mathbb{N} \longrightarrow \mathbb{N}$ is defined as $\mu(n)$ is the smallest positive integer such that $n \mid \mu(n)!$.

The Kempner function plays an important role in the study of polynomial functions. In his work, Kempner showed that there exists a polynomial of degree less than $\mu(n)$ that evaluates to a function over $\mathbb{Z}_n$, if the function is polynomially representable. An easy method to calculate $\mu(n)$ is also given in [10]. One can show that when n factors into primes as

* Corresponding author.
E-mail addresses: guha_ashwin@csa.iisc.ernet.in (A. Guha), ad@csa.iisc.ernet.in (A. Dukkipati).

http://dx.doi.org/10.1016/j.tcs.2015.02.013
0304-3975/© 2015 Elsevier B.V. All rights reserved.

$p_1^{e_1}p_2^{e_2}\dots p_t^{e_t}$, then $\mu(n) = \max(\mu(p_i^{e_i}))$ is of the form $r \cdot p_k$ for some prime divisor p_k of n where r is a positive integer less than or equal to e_k.

It is obvious that the Kempner function is not monotonic: when n is prime $\mu(n) = n$, otherwise $\mu(n) < n$. Kempner function has been studied for its own merit and a discussion on the properties of this function is beyond the scope of this paper. However, one may claim that as n increases, $\mu(n)$ tends to be much smaller than n, by which one means that for most cases $\mu(n)$ tends to be sub-logarithmic compared to n [13].

Polynomial representation in $\mathbb{Z}_n$ has since then been studied by Carlitz [2]. The number of polynomial functions over $\mathbb{Z}_n$, when n is a prime power, is given by Keller and Olson [9]. This was extended to arbitrary positive integer n by Singmaster [15], where the Kempner function was used to give a canonical representation for the polynomial functions. Other notable results are given in [14,1,3,4].

Recently, the problem of polynomial representability of functions in several variables has been studied by Hungerbühler and Specker [8]. In this work, an elegant characterization of polynomial functions was given by generalizing the Kempner function to several variables. The result makes use of partial difference operator to determine whether a given function from $\mathbb{Z}_n^m$ to $\mathbb{Z}_n$ is polynomially representable. This work does not provide a computational complexity analysis but one can see that this method does not lead to an efficient algorithm for verifying polynomial representability of the functions. The characterization involves repeated computation of the difference operator leading to an algorithm whose time complexity is very large. In terms of computation, its performance is comparable to the intuitive method of checking for existence of scalars $c_0, \dots, c_{\mu(n)-1} \in \mathbb{Z}_n$ such that the polynomial $\sum_{i=0}^{\mu(n)-1} c_i X^i$ evaluates to the given function. For instance, in the case of single variable, the computation of $\Delta^k g(0)$ requires $O(k)$ operations for each $0 \le k \le n$, hence checking polynomial representability may require $O(n^2)$ operations.

In this paper we present a new characterization by adopting an entirely new approach that gives rise to a faster algorithm. For this, we generalize a characterization of polynomial functions over $\mathbb{Z}_{p^e}$ that is proposed in [6].

1.1. Contributions

In this paper we give an alternative characterization of polynomial functions over $\mathbb{Z}_n$. The new characterization is based on the fact that the set of polynomial functions forms a $\mathbb{Z}_n$-submodule of the $\mathbb{Z}_n$-module of all functions from $\mathbb{Z}_n$ to itself. We describe a 'special' generating set for this $\mathbb{Z}_n$-module of polynomial functions. When n is prime this generating set forms the standard basis for the vector space of polynomial functions. We present a new algorithm based on this characterization and show that this is faster on average in deciding the polynomial representability of functions. We also extend the characterization to functions in several variables and present an analysis of the algorithm in this case.

1.2. Organization

The paper is organized as follows. Section 2 contains the notation and necessary basic lemmas. The main theorem and the characterization are given in Section 3. An algorithm based on the result is given in Section 4. In Section 5 we discuss the complexity of the algorithm and compare its performance against an algorithm that makes use of a canonical set of generators. The result is extended to functions in several variables in Section 6. Section 7 contains the concluding remarks.

2. Background

Throughout this paper we use n to denote a positive integer of the form $n = p_1^{e_1}p_2^{e_2}\dots p_t^{e_t}$, where $p_1 < p_2 < \dots < p_t$ are distinct primes. Kempner function is denoted by μ (Definition 1.1). Since n is fixed through out this paper, we abbreviate $\mu(n)$ to μ in some formulae. In $\mathbb{Z}_n$, each element of the congruence class is represented by the least non-negative residue modulo n and all computations are performed modulo n unless explicitly mentioned otherwise. Polynomials are of the form $c_0 + c_1 X + \dots + c_r X^r$, where X is the indeterminate and coefficients are from $\mathbb{Z}_n$.

A function $f : \mathbb{Z}_n \longrightarrow \mathbb{Z}_n$ is represented as an n-tuple $(a_0, a_1, \dots, a_{n-1})$, where the ith component $a_i = f(i)$, for $i = 0, \dots, n-1$. Hence we denote the set of all functions by $\mathbb{Z}_n^n$.

Given $v = (a_0, a_1, \dots, a_{n-1})$, $v^{\langle k\rangle}$ represents the kth cyclic shift to the right, for $k = 0, \dots, n-1$. That is

$$v^{\langle k\rangle} = (a_{n-k}, a_{n-k+1}, \dots, a_{n-k-1}),$$

and we assume that $v^{\langle 0\rangle} = v$. In other words $v^{\langle k\rangle}(i) = v(i-k)$ for all $k = 0, \dots, n-1$.

Given a set $\{v_1, v_2, \dots, v_r\} \subset \mathbb{Z}_n^n$, $\langle v_1, v_2, \dots, v_r\rangle$ denotes the $\mathbb{Z}_n$-module generated by that set. $\langle\langle v_1, v_2, \dots, v_r\rangle\rangle$ denotes the $\mathbb{Z}_n$-module generated by v_i with $i = 1, \dots, r$ along with their cyclic shifts, *i.e.*, $\langle\langle v_1, v_2, \dots, v_r\rangle\rangle = \{\sum \alpha_{ij} v_i^{\langle j\rangle} \mid \alpha_{ij} \in \mathbb{Z}_n, i = 1, \dots, r,\ j = 0, \dots, n-1\}$. We say a function is polynomial if there exists some polynomial in $\mathbb{Z}_n[X]$ that evaluates to the given function.

We now make a few simple observations that are easy to verify.

Lemma 2.1. *Suppose $v \in \mathbb{Z}_n^n$ is a polynomial function. Then $v^{\langle k\rangle}$ is also a polynomial function for all $k = 0, \dots, n-1$.*