ARTICLE IN PRESS

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

Contents lists available at ScienceDirect

Journal of Complexity

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

On the linear complexity for multidimensional sequences☆

Domingo Gómez-Pérez [a], Min Sha [b,*], Andrew Tirkel [c]

[a] Department of Mathematics, Statistics and Computer Science, University of Cantabria, 39005 Santander, Spain
[b] Department of Computing, Macquarie University, Sydney, NSW 2109, Australia
[c] Scientific Technology Pty Ltd., 8 Cecil St, East Brighton, VIC 3187, Australia

ARTICLE INFO

Article history:
Received 12 April 2018
Accepted 15 July 2018
Available online xxxx

Keywords:
Multidimensional sequence
Linear complexity
k-error linear complexity

ABSTRACT

In this paper, we define the linear complexity for multidimensional sequences over finite fields, generalizing the one-dimensional case. We give some lower and upper bounds, valid with large probability, for the linear complexity and *k*-error linear complexity of multidimensional periodic sequences.

1. Introduction

One-dimensional periodic sequences with low auto- and cross-correlations have extensive applications in modern communications. Meanwhile, digital watermarking, which has been used to provide copyright protection, certificates of authenticity, access control, audit trail and many other security features, require multidimensional arrays (identified with multidimensional periodic sequences) with similar properties. There are several constructions of these objects proposed by Oscar Moreno, Andrew Tirkel et al. [1,12,13,17].

Recently, in [6] the concept of linear complexity of one-dimensional periodic sequences has been extended to higher dimensions, and an efficient algorithm has been given. Moreover, the numerical results in [6] suggest that the Moreno–Tirkel arrays [13] have high linear complexity. This concept in fact is equivalent to ours for periodic sequences, which is explained later on.

☆ Communicated by Peter Kritzer.

* Corresponding author.
E-mail addresses: domingo.gomez@unican.es (D. Gómez-Pérez), shamin2010@gmail.com (M. Sha), atirkel@bigpond.net.au (A. Tirkel).

https://doi.org/10.1016/j.jco.2018.07.003
0885-064X/

A cryptographically strong sequence should have a high linear complexity, and it should also not be possible to decrease significantly the linear complexity by changing a few terms of the sequence. This leads to the concept of k-error linear complexity defined by Stamp and Martin [16], which is based on the sphere complexity due to Ding, Xiao, and Shan [3]. Note that, in practice, changes in the bitstream can occur due to noise, multipath, or other distortion in the wireless channel.

In this paper, continuing previous work [6], we define the linear complexity for multidimensional sequences, including that of multidimensional arrays as a particular example and introduce the k-error linear complexity for such sequences. We obtain some lower and upper bounds, valid with large probability, for the linear complexity and k-error linear complexity of periodic sequences.

The paper is organized as follows: Section 2 recalls some basic definitions. The proofs of the main results are based on some combinatorial analysis, which is included in Section 3. The main results are presented and proved in Section 4.

2. Preliminaries

2.1. Multidimensional sequences

Let $\mathbb{N}_0$ be the set of non-negative integers and $\mathbb{F}_q$ the finite field of q elements. For any integer $n \geq 1$, an *n-dimensional sequence* over $\mathbb{F}_q$ is a mapping $s\colon \mathbb{N}_0^n \to \mathbb{F}_q$. We write $\boldsymbol{m} = (m_1, \ldots, m_n)$ for the elements of $\mathbb{N}_0^n$, and the corresponding term in the sequence s is denoted by $s(\boldsymbol{m})$. Further, let $\mathbb{F}_q[X_1, \ldots, X_n]$ be the polynomial ring in variables $X_1, \ldots, X_n$ over $\mathbb{F}_q$. A *monomial* in this ring has the form

$$\boldsymbol{X}^{\boldsymbol{j}} = X_1^{j_1} \ldots X_n^{j_n},$$

where $\boldsymbol{X} = (X_1, \ldots, X_n)$ and $\boldsymbol{j} = (j_1, \ldots, j_n) \in \mathbb{N}_0^n$.

Let $\mathbb{F}_q[X_1, \ldots, X_n]$ act on the sequence s as follows. For any

$$P(\boldsymbol{X}) = \sum_{\boldsymbol{j}} a_{\boldsymbol{j}} \boldsymbol{X}^{\boldsymbol{j}} \in \mathbb{F}_q[X_1, \ldots, X_n],$$

let Ps be the n-dimensional sequence defined by

$$Ps(\boldsymbol{m}) = \sum_{\boldsymbol{j}} a_{\boldsymbol{j}} s(\boldsymbol{m} + \boldsymbol{j}).$$

We denote by $I(s)$ the set of polynomials $P \in \mathbb{F}_q[X_1, \ldots, X_n]$ for which $Ps = 0$. Clearly, each polynomial in $I(s)$ actually represents a linear recurrence of s. In fact, $I(s)$ is an ideal of the ring $\mathbb{F}_q[X_1, \ldots, X_n]$, so the quotient $\mathbb{F}_q[X_1, \ldots, X_n]/I(s)$ is well defined (and is an $\mathbb{F}_q$-linear space). If the quotient space $\mathbb{F}_q[X_1, \ldots, X_n]/I(s)$ has finite dimension (say d) over $\mathbb{F}_q$, we say that the sequence s is an *n-dimensional recurrence sequence of order d*. We refer to the survey by Schmidt [15] for a general introduction to this topic. When $n = 1$, this definition recovers the so-called *linear recurrence sequence*; see the book by Everest et al. [4] for an extensive introduction. Moreover, for any ideal I, the quotient space $\mathbb{F}_q[X_1, \ldots, X_n]/I$ has finite dimension over $\mathbb{F}_q$ if and only if there is a non-zero polynomial in $I \cap \mathbb{F}_q[X_i]$ for each $i = 1, \ldots, n$.

Particularly, the sequence s is said to be *periodic* if there is an n-tuple $(T_1, \ldots, T_n)$ of positive integers such that all the binomials $X_1^{T_1} - 1, \ldots, X_n^{T_n} - 1$ belong to $I(s)$, that is, the sequence is periodic in every dimension. Then, we call $(T_1, \ldots, T_n)$ a *period* of s. Periodic sequences of dimension two are called *doubly-periodic sequences*, a largely studied object with applications in algebraic coding theory [5,14].

An n-dimensional array A of size $T_1 \times \cdots \times T_n$ can be naturally extended to an n-dimensional sequence:

$$s_A(m_1, \ldots, m_n) = A(m_1 \bmod T_1, \ldots, m_n \bmod T_n).$$

(Note that $(T_1, \ldots, T_n)$ is a period of s_A.) Conversely, we can view every periodic sequence as the extension of an array. Hence, we can identify multidimensional arrays with multidimensional periodic sequences.

The concept of multidimensional sequences we deal with must not be confused with that of *multisequences*, which consists of finitely many parallel streams of one-dimensional sequences [11].

Please cite this article in press as: D. Gómez-Pérez, et al., On the linear complexity for multidimensional sequences, Journal of Complexity (2018), https://doi.org/10.1016/j.jco.2018.07.003.