Available online at www.sciencedirect.com
ScienceDirect
Information Sciences 178 (2008) 3300–3306
INFORMATION SCIENCES
AN INTERNATIONAL JOURNAL
www.elsevier.com/locate/ins

On the linear complexity of some new q-ary sequences

Xiaoni Du [a,b,*], Zhixiong Chen [c], Guozhen Xiao [b]

[a] College of Mathematics and Information Science, Northwest Normal University, Lanzhou, Gansu 730070, PR China
[b] National Key Laboratory of ISN, Xidian University, Xi'an, Shaanxi 710071, PR China
[c] Department of Mathematics, Putian University, Putian, Fujian 351100, PR China

Received 25 May 2007; received in revised form 13 January 2008; accepted 16 January 2008

Abstract

Some new q-ary sequences with period $q^{3ek}-1$ ($q=p^m$, p an odd prime, m, e, k integers) are first constructed and then, inspired by Antweiler's method, their linear complexity is examined. The exact value of linear complexity $k(6e)^w$ is determined when $r=\sum_{i=1}^{w}p^{e_i}$. Furthermore, an upper bound of the linear complexity is given for the other values of r. Our results show that this sequence has larger linear span than GMW sequence with the same parameters. Finally, the results of a Maple program are included to illustrate the validity of the results.

Keywords: Stream cipher; Linear complexity; Trace function; q-ary sequence

1. Introduction

Pseudo-random sequences have broad applications in many fields such as stream cipher, channel coding and spread spectrum communication [4,17]. Especially for cryptographic applications it is of course highly desirable that the linear complexity be as large as possible. We note that the linear complexity of a sequence, which is the minimal degree of a linear feedback shift register (LFSR) for generating it [5,6], is one of the important properties of a sequence employed in the secure communication and cryptography [2]. Having a large linear complexity implies difficulty in analyzing the sequence.

The trace function [12] representation of sequences plays an important role in implementing the generator of sequences and analyzing their properties. In 1984, Scholtz and Welch [16] presented a method for generating m-sequences using the trace function. Some results have been published by Komo about complex sequences with constant magnitude which are produced by linear feedback shift registers [11,14,15]. In 1992, Antweiler et al. extended it to p-ary GMW sequences [1,8]. Recently, nonbinary sequences with good cryptographic properties have been investigated [7,10,9,13].

* Corresponding author. Address: College of Mathematics and Information Science, Northwest Normal University, Lanzhou, Gansu 730070, PR China.
E-mail addresses: ymLdxn@tom.com, ymLdxn@126.com (X. Du).

0020-0255/$ - see front matter © 2008 Elsevier Inc. All rights reserved.
doi:10.1016/j.ins.2008.01.015

This paper is organized as follows. Based on the theory of finite fields, a new class of q-ary sequence is constructed in Section 2. The linear complexity of resulted sequences is investigated by using the method proposed by Antweiler [1] in Section 3. Especially, the exact value of linear complexity is obtained when $r = \sum_{i=1}^{w} p^{e_i}$ and hence the trace representation and the characteristic polynomial of the sequence can be obtained. Moreover, an upper bound of the linear complexity is given when the other forms of the value parameter r are taken. Results show that this sequence has larger linear span than the GMW sequence with the same parameters. As an example, the results of a Maple program are included to illustrate the validity of the results in Section 4.

2. The construction

In this section, we briefly describe the basic properties of the trace function and construct the new sequences.

Assume that p is a prime, $n = em > 1$, where e and m are positive integers. The trace function $\mathrm{tr}_m^n(\cdot)$ is the mapping from F_{p^n} to its subfield F_{p^m} defined by $\mathrm{tr}_m^n(\alpha) = \sum_{i=0}^{e-1} \alpha^{p^{mi}}$, where α is an element in F_{p^n}. The trace function satisfies the following:

(1) $\mathrm{tr}_m^n(\alpha) = \mathrm{tr}_m^n(\alpha^{p^{mj}})$ and $\mathrm{tr}_m^n(\alpha^{p^j}) = (\mathrm{tr}_m^n(\alpha))^{p^j}$, for all $\alpha \in F_{p^n}$ and all j.
(2) $\mathrm{tr}_m^n(a\alpha + b\beta) = a\mathrm{tr}_m^n(\alpha) + b\mathrm{tr}_m^n(\beta)$, for all $a, b \in F_{p^m}$ and $\alpha, \beta \in F_{p^n}$.
(3) $\mathrm{tr}_1^n(\alpha) = \mathrm{tr}_1^m(\mathrm{tr}_m^n(\alpha))$, for all $\alpha \in F_{p^n}$

We refer the readers to [12] for detailed properties of the trace function.

In the following description, we let $q = p^m$, p is an odd prime, m and e and k positive integers and $s = q^{2ek} - q^{ek} + 1$, $n = 3ek$. Assume α is a primitive element of F_{q^n}. Let r $(1 \leqslant r \leqslant q^k - 2)$ be relatively prime to $q^k - 1$.

Definition 1. With the previous notations, the q-ary sequences $\{a(t)\}_{t=0}^{\infty}$ of period $q^{3ek} - 1$ is defined as

$$a(t) = \mathrm{tr}_1^k\{[\mathrm{tr}_k^{3ek}(\alpha^t + \alpha^{st})]^r\}.$$

In order to determine the linear complexity of these sequences, we need the following result due to Antweiler and Bomer [1].

Lemma 1. *Assume that a sequence $\{b(t)\}$ is given by $b(t) = \sum_{i=0}^{N-1} d_i \beta^{e_i t}$, where β is a primitive element of some extension field F_{q^n} and $d_i \neq 0$ for all i. Then the polynomial $s(x) = \prod_{i=0}^{N-1}(x - \beta^{e_i})$ is the characteristic polynomial of the sequence $\{b(t)\}$ and the linear complexity is N, i.e., the number of nonzero coefficients in the representation of $\{b(t)\}$.*

According to Lemma 1, the determination of the linear complexity $LS(a)$ of the sequence $\{a(t)\}$ constructed in Definition 1 is performed in several steps: first we list the elements of the inner sequence which are given by the inner trace function power. The linear complexity is then the number of nonzero coefficients in this expansion. Next, we apply this result to the composed sequence.

3. Linear complexity of the sequences

For all $x \in \mathbb{Z}_{p^t}$, we can write it as $x = \sum_{i=0}^{t-1} x_i p^i$, $0 \leqslant x_i < p$.

Lemma 2. *Let* $c(x) = [\mathrm{tr}_k^{3ek}(x + x^s)]^r$, *where* $1 \leqslant r \leqslant q^k - 2, \gcd(r, q^k - 1) = 1$, *and* $r = \sum_{i=0}^{mk-1} r_i p^i$ *with* $0 \leqslant r_i < p$, *then*

$$c(x) = (x + \cdots + x^{Q^{l-1}} + x^s + \cdots + x^{sQ^{(l-1)}})^r = \sum_{B} d_B x^{\mathrm{tr}(AB)}, \tag{1}$$

where

(i) $Q = q^k$, $l = 3ek/k = 3e$;