Available online at www.sciencedirect.com
SCIENCE DIRECT®
Journal of Complexity 21 (2005) 804–822
Journal of COMPLEXITY
www.elsevier.com/locate/jco

The expectation and variance of the joint linear complexity of random periodic multisequences

Fang-Wei Fu[a,1], Harald Niederreiter[b,*], Ming Su[c]

[a] *Temasek Laboratories, National University of Singapore, 5 Sports Drive 2, Singapore 117508, Republic of Singapore*
[b] *Department of Mathematics, National University of Singapore, 2 Science Drive 2, Singapore 117543, Republic of Singapore*
[c] *Department of Mathematics, Nankai University, Tianjin 300071, PR China*

Received 20 January 2005; accepted 25 July 2005
Available online 7 October 2005

Abstract

The linear complexity of sequences is one of the important security measures for stream cipher systems. Recently, in the study of vectorized stream cipher systems, the joint linear complexity of multisequences has been investigated. By using the generalized discrete Fourier transform for multisequences, Meidl and Niederreiter determined the expectation of the joint linear complexity of random N-periodic multisequences explicitly. In this paper, we study the expectation and variance of the joint linear complexity of random periodic multisequences. Several new lower bounds on the expectation of the joint linear complexity of random periodic multisequences are given. These new lower bounds improve on the previously known lower bounds on the expectation of the joint linear complexity of random periodic multisequences. By further developing the method of Meidl and Niederreiter, we derive a general formula and a general upper bound for the variance of the joint linear complexity of random N-periodic multisequences. These results generalize the formula and upper bound of Dai and Yang for the variance of the linear complexity of random periodic sequences. Moreover, we determine the variance of the joint linear complexity of random periodic multisequences with certain periods.

Keywords: Multisequences; Joint linear complexity; Stream ciphers; Expectation; Variance; Generalized discrete Fourier transform

* Corresponding author. Fax: +65 6779 5452.
E-mail addresses: tslfufw@nus.edu.sg (F.-W. Fu), nied@math.nus.edu.sg (H. Niederreiter).

[1] On leave from the Department of Mathematics, Nankai University, Tianjin 300071, PR China.

0885-064X/$ - see front matter © 2005 Elsevier Inc. All rights reserved.
doi:10.1016/j.jco.2005.07.001

1. Introduction

Let $\mathbf{F}_q$ be the finite field with q elements. Let $S = (s_0, s_1, s_2, \ldots)$ be a sequence with terms in the finite field $\mathbf{F}_q$. The sequence S is called *N-periodic* if $s_{i+N} = s_i$ for all $i \geqslant 0$. The N-periodic sequence S can be described by the N-tuple $S^N = (s_0, s_1, \ldots, s_{N-1})$. Define the polynomial corresponding to the N-periodic sequence S as

$$S^N(x) = s_0 + s_1 x + s_2 x^2 + \cdots + s_{N-1} x^{N-1}.$$

The *linear complexity* $L(S)$ of an N-periodic sequence S with terms in $\mathbf{F}_q$ is the smallest nonnegative integer c for which there exist coefficients $d_1, d_2, \ldots, d_c \in \mathbf{F}_q$ such that

$$s_j + d_1 s_{j-1} + \cdots + d_c s_{j-c} = 0 \quad \text{for all } j \geqslant c.$$

Equivalently, $L(S)$ is the degree of the polynomial

$$m(x) = 1 + d_1 x + \cdots + d_c x^c \in \mathbf{F}_q[x].$$

The polynomial $m(x)$ is called the *minimal polynomial* of the N-periodic sequence S. Note that $L(S) = 0$ if S is the zero sequence. Obviously, we always have $0 \leqslant L(S) \leqslant N$. Note that if S is not the zero sequence, then $L(S)$ is the length of the shortest linear feedback shift register that can generate S. For a general introduction to the theory of linear feedback shift register sequences, we refer the reader to [8, Chapter 8] and the references therein.

The linear complexity of sequences is one of the important security measures for stream cipher systems. The linear complexity of sequences has been extensively studied by many authors. For a recent survey paper, see Niederreiter [16].

Recently, in the study of vectorized stream cipher systems, the joint linear complexity of multisequences has been investigated (see [1,3,14,21,22]). The multisequence shift register synthesis with applications to decoding cyclic codes has been studied in [4,5,7,20]. Let $S_1, S_2, \ldots, S_t$ be t N-periodic sequences with terms in $\mathbf{F}_q$. Denote

$$S_i = (s_{i,0}, s_{i,1}, s_{i,2}, \ldots), \quad i = 1, 2, \ldots, t.$$

The *joint linear complexity* $L(S_1, S_2, \ldots, S_t)$ of $S_1, S_2, \ldots, S_t$ is the least order of a linear recurrence relation that $S_1, S_2, \ldots, S_t$ satisfy simultaneously, i.e., the smallest nonnegative integer c for which there exist coefficients $d_1, d_2, \ldots, d_c \in \mathbf{F}_q$ such that for $i = 1, 2, \ldots, t$,

$$s_{i,j} + d_1 s_{i,j-1} + \cdots + d_c s_{i,j-c} = 0 \quad \text{for all } j \geqslant c.$$

Since the t-dimensional vector space $\mathbf{F}_q^t$ is isomorphic to the extension field $\mathbf{F}_{q^t}$ as a vector space over $\mathbf{F}_q$, the given multisequence can also be identified with a single sequence having its terms in the extension field $\mathbf{F}_{q^t}$. Meidl and Niederreiter [14] observed that the joint linear complexity of t N-periodic sequences with terms in $\mathbf{F}_q$ can also be interpreted as the $\mathbf{F}_q$-linear complexity of a corresponding N-periodic sequence Λ with terms in $\mathbf{F}_{q^t}$, which is the least order of a linear recurrence relation in $\mathbf{F}_q$ that Λ satisfies.

Blahut and Günther found an important relationship between the linear complexity of a periodic sequence and the Günther weight of the generalized discrete Fourier transform for the periodic sequence (see [9,10] for elegant accounts and extensions of their work). Meidl and Niederreiter [14] extended this important relationship to the case of periodic multisequences. Using the