On Period of Multiplexed Sequences

Jovan Dj. Golić

Information Security Research Centre, Queensland University of Technology
GPO Box 2434, Brisbane Q 4001, Australia
School of Electrical Engineering, University of Belgrade
Email: golic@fit.qut.edu.au

Abstract. Multiplexed and generalized multiplexed sequences for cryptographic and spread spectrum applications are introduced and their periods determined by using a recent result on the period of nonuniformly decimated sequences. Several published results are thus strengthened and/or generalized. In particular, the period of the well-known multiplexed sequences is derived without the constraints assumed in the literature. The period of the so-called MEM-BSG sequences is also obtained.

1 Introduction

A class of binary pseudorandom sequences for cryptographic and spread spectrum applications known as the multiplexed sequences was proposed and analyzed in [12, 13] and widely popularized in [2]. Their use has also been recommended in an EBU standard for video encryption for pay-TV [18]. Multiplexed sequences are generated by a simple and fast scheme consisting of two linear feedback shift registers and a multiplexer whose address is controlled by one of the shift registers and whose inputs are taken from the other. They were shown [12, 13, 14] to possess good standard cryptographic properties such as long period, high linear complexity, and low out-of-phase autocorrelation. On the other hand, they were also shown to exhibit certain cryptographic weaknesses such as the collision test [1], the linear consistency test [16], the resynchronization weakness [6], and the autocorrelation and correlation weaknesses [9].

In this paper we study the periods of various generalizations of multiplexed binary sequences. Note that deriving the period of a pseudorandom sequence is generally a difficult algebraic problem which seems to be tractable only for relatively simple sequences and under special constraints. Our main objective is to obtain general results and thus show that the period can be controlled without the constraints usually assumed in the literature. We will employ the technique [10] based on interleaving and will also introduce some new classes of pseudorandom sequences which may be interesting for stream cipher and spread spectrum applications.

In Section 2, some basic definitions and results [10] regarding the periods of interleaved and nonuniformly decimated sequences are briefly reviewed. Multiplexed and generalized multiplexed sequences, defined as appropriate generalizations of the class of binary sequences introduced by Jennings [12], are analyzed in Sections 3 and 4, respectively. By deriving some additional results on decimated
sequences, the periods of multiplexed and generalized multiplexed sequences are determined and the corresponding result of Jennings [12, 13] is thus generalized. In Section 5, the so-called MEM-BSG sequences based on the variable-memory binary sequence generator [8] are introduced. Their period is obtained and the corresponding result from [8] is thus strengthened and generalized. The results are summarized in Section 6.

2 Preliminaries

In this section we will give necessary definitions and results regarding the period of interleaved and nonuniformly decimated integer sequences. For a set of $K$ periodic integer sequences $a_i = \{a_i(t)\}_{t=0}^\infty$ with periods $P_i$, $0 \leq i \leq K - 1$, respectively, the interleaved sequence $b$ is defined by

$$b(i + Kt) = a_i(t), \quad 0 \leq i \leq K - 1, \quad t \geq 0.$$  \hfill (1)

It is clear that $b$ is periodic with period $P_b \mid PK$, where $P = \text{l.c.m.} (P_i : 0 \leq i \leq K - 1)$. The following lemma, proved in [10], specifies $P_b$ more precisely.

**Lemma 1.** The period $P_b$ of the interleaved sequence $b$ satisfies

$$P_b = P(P_b, K)$$ \hfill (2)

where $(\cdot, \cdot)$ denotes the greatest common divisor.

An exact characterization of $P_b$ in terms of the constituent sequences $a_i$, $0 \leq i \leq K - 1$, was also derived in [10], and then used as a basic result to determine the period of nonuniformly decimated sequences and thus generalize an old result of Blakley and Purdy [3]. Namely, let $a = \{a(t)\}_{t=0}^\infty$ be a periodic integer sequence with period $P_a$. Let $D = \{D(t)\}_{t=0}^\infty$ be a decimation sequence defined recursively by $D(t + 1) = D(t) + d(t)$, $t \geq 0$, where $D(0) = 0$ and the difference decimation sequence $d = \{d(t)\}_{t=0}^\infty$ is a periodic nonnegative integer sequence with period $M$ such that $0 \leq d(t) \leq P_a - 1$, $t \geq 0$. The decimated sequence $b$ is then defined by

$$b(t) = a(D(t)) = a \left( \sum_{i=0}^{t-1} d(i) \right), \quad t \geq 0,$$ \hfill (3)

see [3], [4], assuming that $\sum_{i=0}^{t} (\cdot) = 0$ if $j < i$. In a special case when $d(t) = d$, $t \geq 0$, the decimation is called uniform. Letting $N = D(M) \mod P_a$, it is well known [4], [5], [7] that the decimated sequence $b$ can be regarded as an interleaved sequence such that

$$b(i + Mt) = a(D(i) + Nt), \quad 0 \leq i \leq M - 1, \quad t \geq 0$$ \hfill (4)

meaning that $\{b(i + Mt)\}_{t=0}^\infty$ is a decimated sequence obtained from the uniform decimation by $N$ of $\{a(D(i) + t)\}_{t=0}^\infty$, $0 \leq i \leq M - 1$. Let $P_b$ denote the period of