Information Processing Letters 114 (2014) 268–272

Contents lists available at ScienceDirect

Information Processing Letters

www.elsevier.com/locate/ipl

Searching for nonlinear feedback shift registers with parallel computing

Przemysław Dąbrowski, Grzegorz Łabuzek, Tomasz Rachwalik, Janusz Szmidt

Military Communication Institute, ul. Warszawska 22A, 05-130 Zegrze, Poland

ARTICLE INFO

Article history:
Received 26 June 2013
Received in revised form 28 October 2013
Accepted 4 December 2013
Available online 16 December 2013
Communicated by V. Rijmen

Keywords:
Nonlinear feedback shift registers
Maximum period
Parallel processing

ABSTRACT

Nonlinear feedback shift registers (*NLFSRs*) are used to construct pseudorandom generators for stream ciphers. Their theory is not so complete as that of linear feedback shift registers (*LFSRs*). In general, it is not known how to construct all *NLFSRs* with maximum period. The direct method is to search for such registers with suitable properties. Advanced technology of parallel computing has been applied both in software and hardware to search for maximum period *NLFSRs* having a fairly simple algebraic normal form.

1. Introduction

Feedback shift register (FSR) sequences have been widely used in many areas of communication theory, as key stream generators in stream ciphers cryptosystems, pseudorandom number generators in many cryptographic primitives, in the design of correlators for spread spectrum communication systems, global positioning systems or radar systems, and as testing vectors in hardware design. Golomb's book [6] is a pioneering one that discusses this type of sequences. A modern treatment of the subject is contained in the book of Golomb and Gong [7].

The theory of linear feedback shift registers (*LFSRs*) is quite well understood. In particular, it is known how to construct *LFSRs* with maximum period; they correspond to primitive polynomials over the binary field $\mathbb{F}_2$. The order n of *FSR* is the number of its cells and an *FSR* can generate a binary sequence of period up to 2^n. The main drawback of primitive *LFSRs* is that their linear complexity is equal to their order. In recent years, nonlinear feedback shift registers (*NLFSRs*) have received much attention in designing numerous cryptographic algorithms such as stream ciphers and lightweight block ciphers to provide security in communication systems. In most cases, *NLFSRs* have much greater linear complexity than *LFSRs* of the same period. However, there are no general methods of designing maximum period *NLFSRs*. The construction of a special class of *NLFSRs* with maximum period has been given by Mykkeltveit et al. [10,11]. Recently, maximum period *NLFSRs* of order up to $n = 64$ have been constructed in the paper of Mandal and Gong [8], but these *NLFSRs* have very complicated algebraic normal form (*ANF*). Dubrova [3] has given an example of a Galois shift register of order $n = 100$ generating a sequence with maximum period but this sequence does not have the de Bruijn property; i.e., some patterns of n-bits appear more than once in the sequence.

In this article the approach from the papers of Gammel, Goettfert, and Kniffler [5] and Chan, Games, and Rushanan [2] is followed. *NLFSRs* having a simple algebraic normal form and maximum period are directly found by exhaustive searching. In particular, the conjecture posed in [2] on the existence of maximum period *NLFSRs* whose feedback functions have linear terms and one quadratic term has been experimentally investigated. Like the notion of linear m-sequences, these *NLFSRs* generate quadratic m-sequences. The conjecture has been verified up to order

E-mail addresses: p.dabrowski@wil.waw.pl (P. Dąbrowski), g.labuzek@wil.waw.pl (G. Łabuzek), t.rachwalik@wil.waw.pl (T. Rachwalik), j.szmidt@wil.waw.pl (J. Szmidt).

0020-0190/$ – see front matter © 2013 Elsevier B.V. All rights reserved.
http://dx.doi.org/10.1016/j.ipl.2013.12.002

$n = 29$. Quadratic m-sequences of this type up to order $n = 21$ have been classified according to the weight (number of terms) of primitive polynomials involved. These experimental investigations support the Chan, Games and Rushanan conjecture of the existence of one term quadratic m-sequences for each order n; they have some number of linear terms and only one quadratic term in their *ANF*.

Our experiments have applied parallel computing. *NLFSRs* generating quadratic m-sequences have been found by using three servers with 54 CPU cores. The investigations from the previous paper [12] have also been continued using the Field Programmable Gate Arrays to find maximum period *NLFSRs*. Nonlinear feedback shift registers have been applied in [13] to construct modified alternating step generators.

2. Feedback shift registers

In this section, the definitions and basic facts about feedback shift registers are given. We use $\mathbb{F}_2$ to denote the binary finite field. $\mathbb{F}_2[x]$ denotes the ring of polynomials in the indeterminate x and with coefficients from $\mathbb{F}_2$. Let $\mathbb{F}_2^n$ be the n-dimensional vector space over $\mathbb{F}_2$ consisting of all n-tuples of elements of $\mathbb{F}_2$. Any function from $\mathbb{F}_2^n$ to $\mathbb{F}_2$ is referred to as a *Boolean function* of n variables. A sequence of elements $\mathbf{s} = (s_0, s_1, \ldots)$ of $\mathbb{F}_2$ is called a *binary sequence*. A sequence $\mathbf{s} = (s_i)_{i=0}^{\infty}$ is called *periodic* if there is a positive integer p such that $s_{i+p} = s_i$ for all $i \geqslant 0$. The least positive integer with this property is called the *period* of $\mathbf{s}$.

A *binary feedback shift register* of order n is a mapping $\mathfrak{F}$ from $\mathbb{F}_2^n$ into $\mathbb{F}_2^n$ of the form

$$\mathfrak{F} : (x_0, x_1, \ldots, x_{n-1}) \longmapsto \bigl(x_1, x_2, \ldots, x_{n-1}, f(x_0, x_1, \ldots, x_{n-1})\bigr),$$

where f is a Boolean function of n variables which is called the *feedback function*. The shift register is called a *linear feedback shift register* (*LFSR*) if $\mathfrak{F}$ is a linear transformation from the vector space $\mathbb{F}_2^n$ into itself. Otherwise, the shift register is called a *nonlinear feedback shift register* (*NLFSR*). The shift register is called *nonsingular* if the mapping $\mathfrak{F}$ is a bijection. Further, we will consider only nonsingular and mostly nonlinear feedback shift registers. It can be proved (see e.g. [6]) that the feedback function of a nonsingular feedback shift register has the form

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 + g(x_1, \ldots, x_{n-1}), \tag{1}$$

where g is a Boolean function of $n - 1$ variables.

Consider a binary sequence $\mathbf{s} = (s_i)_{i=0}^{\infty}$ whose first n terms $s_0, s_1, \ldots, s_{n-1}$ are given and whose remaining terms are uniquely determined by the recurrence relation

$$s_{i+n} = f(s_i, s_{i+1}, \ldots, s_{i+n-1}) \quad \text{for all } i \geqslant 0. \tag{2}$$

We call $\mathbf{s}$ an *output sequence* of the feedback shift register given by (1). The binary n-tuple $(s_0, s_1, \ldots, s_{n-1})$ is called the *initial state vector* of the sequence $\mathbf{s}$ or the *initial state* of the feedback shift register. The recurrence relation (2) can be implemented in hardware as a special electronic switching circuit consisting of n memory cells which is controlled by an external clock to generate the sequence $\mathbf{s}$.

Definition 1. A *de Bruijn sequence* of order n is a sequence of period 2^n of elements of $\mathbb{F}_2$ in which all different binary n-tuples appear in each period exactly once.

It was proved by Flye Sainte-Marie [4] in 1894 and independently by de Bruijn [1] in 1946 that the number of cyclically non-equivalent sequences satisfying Definition 1 is equal to

$$B_n = 2^{2^{n-1}-n}.$$

Definition 2. A *modified de Bruijn sequence* of order n is a sequence of period $2^n - 1$ obtained from the de Bruijn sequence of order n by removing one zero from all tuples of n consecutive zeros.

In 1990 Mayhew and Golomb [9] investigated sequences satisfying Definition 2 and calculated their linear complexity. These sequences were called by Gammel et al. [5] *primitive*. In the case of linear feedback shift registers such sequences are generated by primitive polynomials from the ring $\mathbb{F}_2[x]$ and their theory is quite well understood [6,7]. The task is to find primitive *NLFSRs* with a simple algebraic normal form and this is a time consuming work. An effective method of constructing such primitive *NLFSRs* is not known and one has to search for them. Gammel et al. [5] found simple primitive *NLFSRs* up to order 33 used in the design of the stream cipher Achterbahn, but neither the method of searching nor the average time needed to find such good *NLFSRs* have been revealed.

A search for primitive *NLFSRs* with special purpose hardware devices has been undertaken in [12]. The present paper is a continuation of the previous investigations with additional application of software implementations on parallel cores. The search is restricted to looking for nonlinear primitive *NLFSRs* with a simple *ANF*.

3. Quadratic *m*-sequences

Chan, Games and Rushanan [2] have investigated the case when the feedback function (1) is a quadratic Boolean function of n variables; i.e., it has the following algebraic normal form:

$$f(x_0, x_1, \ldots, x_{n-1}) = \sum_{0 \leqslant i \leqslant j \leqslant n-1} a_{ij} x_i x_j. \tag{3}$$

Let us note that $x_i^2 = x_i$ for all $i \geqslant 0$, hence the coefficients a_{ii} correspond to the linear terms of the function f. The recurrence (2) corresponding to the quadratic function (3) has the form

$$s_{n+k} = \sum_{0 \leqslant i \leqslant j \leqslant n-1} a_{ij} s_{i+k} s_{j+k} \tag{4}$$

for all $k \geqslant 0$. The authors of [2] have introduced a notion of quadratic m-sequences by analogy to the linear ones.

Definition 3. A binary sequence $\mathbf{s}$ is called a *quadratic m-sequence of order n* if it satisfies the quadratic recurrence (4) and has period $2^n - 1$. The quadratic recurrence (4) is