On Feedback Functions of Maximum Length Nonlinear Feedback Shift Registers

Çağdaş Çalik[1] and Meltem Sönmez Turan[2] and Ferruh Özbudak[1]

[1] Middle East Technical University
[2]National Institute of Standards and Technology

Abstract. Feedback shift registers are basic building blocks for many cryptographic primitives. Due to the insecurities of Linear Feedback Shift Register (LFSR) based systems, the use of Nonlinear Feedback Shift Registers (NFSRs) became more popular. In this work, we study the feedback functions of NFSRs with period 2^n. First, we provide two new necessary conditions for feedback functions to be maximum length. Then, we consider NFSRs with k-monomial feedback functions and focus on two extreme cases where $k = 4$ and $k = 2^{n-1}$. We study construction methods for these special cases.

Keywords: de Bruijn sequences, Maximal length sequences, Nonlinear feedback shift registers

1 Introduction

Feedback Shift Registers (FSRs) are widely used in many applications such as error correcting codes, test pattern generation and symmetric cryptography. The eSTREAM stream cipher project hardware finalists Grain [1], Mickey [2] and Trivium [3] use FSRs, due to their efficiency, large period and good statistical properties.

The FSRs with linear feedback function, *Linear Feedback Shift Registers* (LFSRs) are widely studied in the literature and it is easy to find LFSRs with maximum period for a given length n. However, one important drawback of LFSR outputs is that they are completely linear, thus cryptographically insecure. Whenever $2n$ bits of the output of an n-bit register is given, the sequence is totally predictable using the Berlekamp-Massey algorithm.

Many different design attempts have been done to add nonlinearity to the systems based on LFSRs, such as combining outputs of several LFSRs using a nonlinear function, nonlinearly filtering the LFSR state or irregularly decimating the output [4]. However, most of these approaches do not offer the desired security [5]. Due to the limitations of LFSRs, use of *Nonlinear Feedback Shift Registers* (NFSRs) became more popular.

NFSRs constitute a larger class compared to LFSRs and they are more resistant to algebraic attacks, but for large n, there exists no efficient method to construct a cryptographically secure NFSR.

Golomb studied on maximum length NFSRs and presented some of the properties to generate maximum length NFSRs in [6] (p. 115). Also, in 1982, Fredricksen [7] presented a survey on maximum length NFSRs including construction methods and some properties. Recently, Dubrova et al. [8] generalized the Galois type of LFSRs and defined an alternative type of NFSRs that are called (n, k)-NFSRs. Tsueda et al. [9] proposed feedback-limited NFSRs and studied their properties in terms of correlation and linear complexity measures.

There is no efficient method that finds a feedback function with maximum period and also, given a feedback function it is hard to predict the period. In this work, we study maximum length NFSRs and propose two new conditions for feedback functions to be maximum length. Since hardware efficiency of NFSRs is extremely important, especially for stream ciphers designed for restricted environments, we focus on the number of monomials in the feedback function which is highly correlated with the gate count of a design. We focus on two special cases with $k = 4$ and $k = 2^{n-1}$, and provide construction methods.

The paper is organized as follows. In Sect. 2, we give a basic review of FSRs and we list necessary conditions for maximum length feedback functions. In Sect. 3, we focus on the number of monomials k in the feedback functions and constructions of two extreme cases with $k = 4$ and $k = 2^{n-1}$ are also provided. In Sect. 4, we conclude the study.

2 Preliminaries

A *Boolean function* f with n variables is a mapping from $\mathbb{F}_2^n$ to $\mathbb{F}_2$. Let α_i be the n-bit vector corresponding to the binary representation of integers $i = 0, 1, 2, \ldots, 2^n - 1$. For a Boolean function with n variables, the sequence

$$(f(\alpha_0), f(\alpha_1), \ldots, f(\alpha_{2^n-1})) \tag{1}$$

is called the *truth table* of f. *Algebraic normal form* (ANF) of a Boolean function is the polynomial

$$f(x_1, x_2, \ldots, x_n) = c_0 \oplus c_1 x_1 \oplus \ldots \oplus c_{12\ldots n} x_1 x_2 \ldots x_n \tag{2}$$

with unique $c_{i_1 \ldots i_k}$'s in $\mathbb{F}_2$. The number of terms in the highest order product monomial with nonzero coefficient is called the *degree* of f. The Boolean functions with degree 1 are called *affine* and in particular for $c_0 = 0$, the functions are called *linear*.

A *FSR* is a device that shifts its contents into adjacent positions within the register and fills the position on the other end with a new value generated by the *feedback function*. The individual delay cells of the register are called the *stages* and the number of the stages n is called the *length* of FSR. The contents of the n stages are called the *state* of the FSR. The n bit vector $(s_0, s_1, \ldots, s_{n-1})$ initially loaded into FSR state specify the *initial state*. A block diagram of a FSR is given in Figure 1.

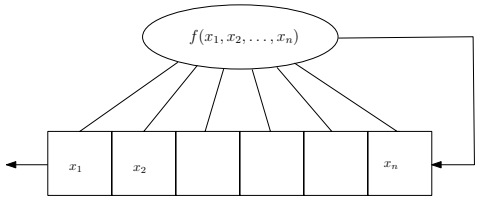

Fig. 1. Block diagram of a Feedback Shift Register.

Definition 1. *Let* $\boldsymbol{S}$= $\{s_0, s_1, s_2, \ldots\}$ *be a binary sequence. If there exists integers* $u \geq 0$ *and* $p > 0$ *such that* $s_{i+p} = s_i$ *for all* $i \geq u$*, the sequence is called ultimately periodic and smallest possible* p *is called the period of the sequence.*

A FSR is uniquely determined by its length n and feedback function f. The output sequence $\mathbf{S}$= $\{s_0, s_1, s_2, \ldots\}$ of a FSR satisfies the following recursion

$$s_{n+i} = f(s_i, \ldots, s_{n-1+i}),\ i \geq 0 \tag{3}$$

for the given initial state $(s_0, s_1, \ldots, s_{n-1})$.

For LFSRs, this recursion is linear and may be represented using the *characteristic polynomial*,

$$C(x) = \sum_{i=0}^{n} c_i x^{n-i}. \tag{4}$$

with $c_0 = 1$. If $C(x)$ is a primitive polynomial with degree n, then each of the $2^n - 1$ non-zero initial states of the LFSR produce an output with maximum possible period $2^n - 1$. Outputs of maximum length LFSRs are called *maximal length sequences* or *m-sequences*.

3 NFSRs and de Bruijn Sequences

The output sequences of NFSRs can achieve the period of 2^n. Such sequences include each n bit pattern exactly once and are called *de Bruijn sequences*. The number of de Bruijn sequences of order n is $2^{2^{n-1}-n}$ [10]. In this study, we are interested in NFSRs that generate de Bruijn sequences.

3.1 Basic Transformations

In the following propositions, we define the basic transformations on maximum length sequences and show how the feedback function of the NFSR should be modified in order to perform each transformation.

Proposition 1. *Let* $f(x_1, x_2, \ldots, x_n)$ *be a feedback function that generates a sequence with period* $2^n - 1$ *and* $f(0, 0, \ldots, 0) = 0$*. Then,* $f + x'_2 \ldots x'_n$ *produces a de Bruijn sequence where* x'_i *is the complement of* x_i*.*

Proof. To combine all zero cycle and the cycle with period $2^n - 1$, two values in the truth table of f should be changed so that $f(0, \ldots, 0) = 1$ and $f(1, 0, \ldots, 0) = 0$ are satisfied. The necessary changes are done by adding $x_2' \cdots x_n'$ to f.

Proposition 2. *Let $f(x_1, x_2, \ldots, x_n)$ be a feedback function that generates a sequence with period $2^n - 1$ and $f(1, 1, \ldots, 1) = 1$. Then, $f + x_2 x_3 \ldots x_n$ produces a de Bruijn sequence.*

Proof. Following similar argument given in Proposition 1, to combine all one cycle and the cycle with period $2^n - 1$, two values in the truth table of f should be changed so that $f(1, \ldots, 1) = 0$ and $f(0, 1, \ldots, 1) = 1$ are satisfied. The necessary changes is done by adding $x_2 \cdots x_n$ to f.

Proposition 3. *Let $f(x_1, x_2, \ldots, x_n)$ be a feedback function that generates a sequence S with period $2^n - 1$ or 2^n. Then, $f(x_1, x_2', \ldots, x_n')$ generates the bitwise complement of S.*

Proof. Let S' be the bitwise complement of S and let f' be the feedback function that generates S'. Then, the following equation holds

$$\begin{aligned} f(x_1, x_2, \ldots, x_n) &= f'(x_1', x_2', \ldots, x_n') + 1 \\ &= f'(x_1, x_2', \ldots, x_n') \end{aligned} \tag{5}$$

Then, $f'(x_1, x_2, \ldots, x_n) = f(x_1, x_2', \ldots, x_n')$ holds.

Proposition 4. *Let $f(x_1, x_2, \ldots, x_n)$ be a feedback function that generates a sequence S with period $2^n - 1$ or 2^n. Then, $f(x_1, x_n, x_{n-1}, \ldots, x_2)$ generates the reverse of S.*

Proof. Let $f'(x_1, \ldots, x_n)$ be the feedback function that generates the reverse of S. Then, $f(s_i, \ldots, s_{i+n-1}) = s_{i+n}$ and $f'(s_{i+n}, \ldots, s_{i+1}) = s_i$ hold for $i \geq 0$. Since f and f' are maximum length, there exists g and g' functions such that

$$s_{i+n} = s_i + g(s_{i+1}, \ldots, s_{i+n-1}) \tag{6}$$

and

$$s_i = s_{i+n} + g'(s_{i+n-1}, \ldots, s_{i+1}) \tag{7}$$

Summing Eq. 6 and Eq. 7, we obtain

$$g(s_2, \ldots, s_n) = g'(s_n, \ldots, s_2), \tag{8}$$

therefore

$$f'(x_1, \ldots, x_n) = f(x_1, x_n, x_{n-1}, \ldots, x_2) \tag{9}$$

holds.

3.2 Properties of Maximum Length NFSRs

In this part of the study, we survey some of the necessary conditions of the feedback function $f(x_1, \ldots, x_n)$ to generate de Bruijn sequences. We also provide two new necessary conditions; one based on the symmetry of variables, and the other based on the number of monomials.

To guarantee that every state has a unique predecessor and successor, f should be written in the form $f(x_1, \ldots, x_n) = x_1 + g(x_2, \ldots, x_n)$ [6]. Some necessary conditions on f and g to generate a de Bruijn sequence are given as follows;

1. To avoid all zero cycle, $f(0, \ldots, 0) = 1$, i.e. $c_0 = 1$.
2. To avoid all one cycle, $f(1, \ldots, 1) = 0$, therefore the number of monomials in f is even.
3. To avoid the cycle $(0 \ldots 01)$ of length $n + 1$, there must be at least one coefficient $c_i = 0$ for $i = 2, \ldots, n$ [11], i.e., g cannot contain all the linear terms. Otherwise, if all the linear terms exist in g, the cycle $(0 \ldots 01)$ repeats itself, since g always outputs 0 for inputs with weight 1.
4. The parity of the cycles generated by a FSR is equal to the parity of the truth table of g [6]. To achieve one maximum length cycle, parity of the truth table of g should be 1, which implies
   $c_{23\ldots n} = 1$.
5. The weight $w(g)$ of g satisfies the following inequality

$$Z_{n-1} \leq w(g) \leq 2^{n-1} - Z_n^* + 1 \tag{10}$$

   where Z_n is $\frac{1}{n}\sum_{d|n} \phi(d) 2^{n/d}$ and Z_n^* is $\frac{Z_n}{2} - \frac{1}{2n}\sum \phi(2d) 2^{n/2d}$ with summation over all even divisors of n [7], and ϕ is the Euler phi function.

Next, we provide a new condition based on symmetry of variables.

Proposition 5. *Let $f = x_1 + g(x_2, \ldots, x_n)$ generate a de Bruijn sequence and $n > 2$. Then,*

$$g(x_2, \ldots, x_n) \neq g(x_n, \ldots, x_2). \tag{11}$$

Proof. We call a state R-state, if its reverse is equal to itself. Let the initial state $R_1 = (s_i, s_{i+1}, \ldots, s_{i+n-1})$ be an R-state. Assume $g(x_2, \ldots, x_n) = g(x_n, \ldots, x_2)$, then the sequence generated by $f = x_1 + g$ has the following property; $s_{i-j} = s_{i+n+j-1}$ for $j \geq 1$. Then, R_2 is also an R-state. For $n \geq 3$, the number of R-states is greater than 3 (all zero state, all one state and $10 \ldots 01$ state are examples). Therefore, there exists another R-state R_3 (See Figure 2) that appears twice in the sequence resulting in a contradiction to the definition of de Bruijn sequences.

Proposition 6. *Let Sym_n be the number of n variable Boolean functions with property $g(x_1, x_2, \ldots, x_n) = g(x_n, x_{n-1}, \ldots x_1)$. Then;*

$$Sym_n = \begin{cases} 2^{2^{n-1}+2^{\frac{n}{2}}-1}, & \text{if } n \text{ is even} \\ 2^{2^{n-1}+2^{\frac{n+1}{2}}-1}, & \text{if } n \text{ is odd.} \end{cases}$$

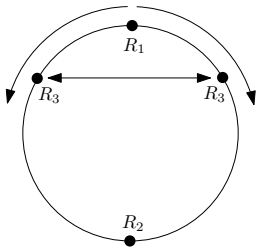

Fig. 2. R-states in NFSR output.

Proof. We call a monomial self-symmetric, if it's symmetric monomial is itself, i.e.,

$$x_{i_1}x_{i_2}\dots x_{i_k} = x_{n+1-i_1}x_{n+1-i_2}\dots x_{n+1-i_k}.$$

The number of monomials satisfying this property can be obtained by counting the monomials depending on one half of the input variables, from x_1 to $x_{\frac{n}{2}}$ for even n and from x_1 to $x_{\frac{n+1}{2}}$ for odd n. The remaining monomials can be grouped in pairs in which one monomial is the symmetric of the other. A Boolean function constructed with any combination of the self-symmetric monomials and from remaining symmetric monomial pairs is also symmetric because either each monomial is self-symmetric or its symmetric monomial exists in the function. The number of self-symmetric monomials are $2^{\frac{n}{2}}$ for even n and $2^{\frac{n+1}{2}}$ for odd n. Subtracting these numbers from the total number of 2^n monomaials and dividing by 2 to get the pair count, we obtain $2^{n-1}-2^{\frac{n}{2}-1}$ and $2^{n-1}-2^{\frac{n+1}{2}-1}$ free choices for even and odd n respectively. Hence, the result is 2 to the power of these numbers.

Following theorem gives another condition based on the number of monomials in f.

Theorem 1. *Let $f(x_1,\dots,x_n)$ generate a de Bruijn sequence and K_i be the number of monomials that depend on x_i, $i = 2,\dots,n$ in f. Then there exists at least one even K_i.*

Proof. Assume K_i is odd for all i. Following Proposition 3, if f produces a de Bruijn sequence, then $f' = f(x_1, x'_2, \dots, x'_n)$ also produces a de Bruijn sequence. Then, ANF of f' includes all linear monomials from x_2 to x_n, and that contradicts the 3^{rd} condition given above. Therefore, there exists at least one even K_i.

Corollary 1. *There exists no maximum length feedback function of the form*

$$f(x_1, x_2, \dots, x_n) = x_1 + x_2 \cdot \dots \cdot x_n + x'_{i_1} \cdots x'_{i_k} \tag{12}$$

for $2 \le i_1 < \dots < i_k \le n$.

Proof. The number of occurrences of each x_i is odd for $(2 \geq i \geq n)$, therefore following Theorem 1, it is impossible to generate a de Bruijn sequence using f of this form.

4 Number of Monomials in f

In this section, we study the number of monomials in feedback functions of maximum length NFSRs. We call a maximum length NFSR k-Monomial NFSR, if it's feedback function has k monomials.

Let $N_{n,k}$ be the number of n bit maximum length NFSRs with k monomials. Figure 3 shows the distribution of $N_{n,k}$ for $n = 6$. Trivially, $\sum_k N_{n,k} = 2^{2^{n-1}-n}$.

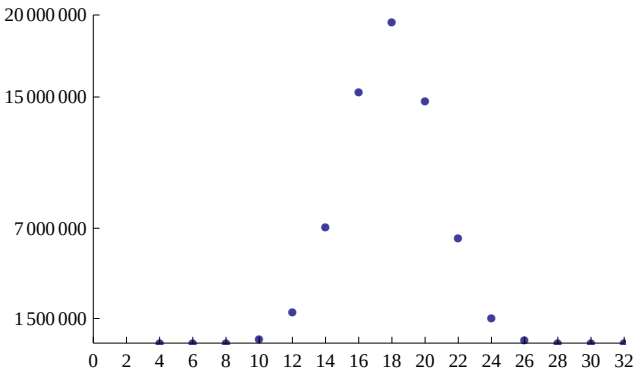

Fig. 3. The distribution of $N_{n,k}$ for $n = 6$.

Proposition 7. *Let $f(x_1, x_2, \ldots, x_n)$ generate a de Bruijn sequence and k be the number of monomials in f. Then,*
(i) *k is even,*
(ii) $4 \leq k \leq 2^{n-1}$.

Proof. (i) To avoid the cycle of all ones, the number of monomials k in f should be even.
(ii) Maximum period feedback function always include the monomials 1, x_1 and $x_2.x_3.\ldots.x_n$, therefore $k \geq 3$. To ensure maximum length, f does not include any nonlinear monomials that include x_1. Then, $k \leq 2^{n-1} + 1$. Since k is even, $4 \leq k \leq 2^{n-1}$ holds.

Proposition 8. *$N_{n,k}$ is even for $k > 0$ and $n > 2$.*

Proof. For each maximum length feedback functions f_1 with k monomials, it is possible to find another maximum length feedback function f_2 with k monomials using the transformation in Proposition 4. According to the Proposition 5,

$f_1 = f_2$. Applying the same transformation to f_2 gives f_1. Therefore, the set of maximum length feedback functions with k monomials can be grouped as pairs with respect to this transformation, which implies $N_{n,k}$ is always even.

Next, we study on the feedback functions with 4 monomials.

4.1 4-Monomial NFSRs

It is known that the maximum length feedback functions include the monomials 1, x_1 and $x_2.x_3.\ldots.x_n$. Since three of the monomials are fixed, 4-monomial feedback functions are of the form;

$$f(x_1, \ldots, x_n) = 1 + x_1 + x_2.x_3.\ldots.x_n + I \tag{13}$$

where I is the *free monomial* independent of x_1.

Next, we study the properties of I so that f produces de Bruijn sequence.

Proposition 9. *Let $f(x_1, \ldots, x_n) = 1 + x_1 + x_2.x_3.\ldots.x_n + I$ generate a de Bruijn sequence and I be $x_{i_1} \ldots x_{i_l}$ with $2 \leq i_1 < i_2 < \ldots < i_l \leq n$.*
(i) *For odd n, the indices of I satisfy the following property*

$$i_1 = i_2 = \ldots = i_l \ (mod\ 2). \tag{14}$$

(ii) *The monomial I is not symmetric, i.e.*

$$x_{i_1} \ldots x_{i_l} = x_{n+2-i_1} \ldots x_{n+2-i_l}. \tag{15}$$

Proof. (i) Assume the contrary, then the register falls in the cycle of (01).
(ii) Symmetric I contradicts the Proposition 5 given in Sect. 2.

Next, we consider the properties of the simple register with feedback function $f = 1 + x_1 + x_2.x_3.\ldots.x_n$ and we call it a *type A register*. The properties of this register is very similar to the *complemented cycling register* (CCR) with feedback function $1 + x_1$ defined in [6]. The number of cycles generated by a CCR is

$$N = \frac{1}{2}Z(n) - \frac{1}{2n}\sum_{2d|n} \phi(2d)2^{n/2d} \tag{16}$$

where $Z_n = \frac{1}{n}\sum_{d|n} \phi(d)2^{n/d}$ [6]. Then, the number of cycles generated by a type A register is $N + 1$, since adding $x_2 \ldots x_n$ to the feedback functions only affects the cycle $(\underbrace{00\ldots0}_{n}\underbrace{1\ldots1}_{n})$ by dividing it into two cycles $(\underbrace{00\ldots0}_{n}\underbrace{1\ldots1}_{n-1})$ and (1) and the rest of the cycles remain the same. As an example, the cycles generated by the 6-bit CCR and type A register are given in Table 1.

Proposition 10. *Let the degree of I be d, then the weight of $g(x_2, \ldots, x_n) = 1 + x_2 \cdots x_n + I$ is*

$$w(g) = 2^{n-1} - 2^{n-d-1} + 1. \tag{17}$$

Table 1. The cycles generated by 6-bit CCR and 6-bit type A register.

6 bit CCR	6 bit type A register
-	(1)
(0011)	(0011)
(00000011111)	(00000011111)
(000010111101)	(000010111101)
(000100111011)	(000100111011)
(000110111001)	(000110111001)
(001010110101)	(001010110101)

Proof. Let g' be $1+x_2.\cdots.x_n$, then $w(g') = 2^{n-1}-1$. I changes the truth table of g' at 2^{d-1} points. Then,

$$\begin{aligned} w(g) &= w(g') + \#(\text{Changes from 0 to 1}) \\ &\quad -\#(\text{Changes from 1 to 0}) \\ &= 2^{n-1} - 2^{n-d-1} + 1 \end{aligned} \tag{18}$$

Next, we give an upper bound on the degree of I.

Proposition 11. *The degree of I is less than $log_2 n$.*

Proof. To combine $N+1$ cycles generated by the type A register, the monomial I should make at least N changes in the truth table of $1+x_2 \dots x_n$. If the degree of I is d, following Proposition 10 the number of changes in the truth table is 2^{n-1-d}. Therefore, 2^{n-1-d} should be greater than N. Due to the special structure of the register, the maximum length of the cycles is $2n$, therefore $N > \frac{2^n}{2n}$ should be satisfied. $2^{n-1-d} > \frac{2^n}{2n}$ implies $d < log_2 n$.

Construction of 4-monomial NFSRs Here, we give two different construction methods for maximum length 4-monomial NFSRs. The first method uses a trinomial primitive polynomial, and generates a 4-monomial feedback function in which I is linear. The second method starts with a quadratic feedback function with period 2^n-1, then generates a 4-monomial feedback function in which I is quadratic.

Proposition 12. *Let $p = 1 + x^i + x^n$ be a trinomial primitive polynomial over $GF(2)$ for $1 \leq i < n$. Then, the feedback function $f = 1 + x_1 + x_{n+1-i} + x_2.x_3 \dots x_n$ with 4 monomials produces a de Bruijn sequence.*

Proof. Given p, $f_1(x) = x_1 + x_{n+1-i}$ produces a maximum length LFSR sequence with period $2^n - 1$. Applying the transformations in Proposition 3 and Proposition 2 to f respectively, we obtain a 4-monomial $f = 1 + x_1 + x_{n+1-i} + x_2.x_3 \dots x_n$ that produces a de Bruijn sequence.

Following proposition gives another construction method from a quadratic feedback functions with period $2^n - 1$.

Proposition 13. *Let $f(x_1, \ldots, x_n) = x_1 + x_i + x_j + x_i.x_j$ for some $i = j$ and $2 \leq i, j \leq n$ generate a sequence with period $2^n - 1$. Then,*

$$f'(x_1, \ldots, x_n) = 1 + x_1 + x_i.x_j + x_2.\ldots.x_n \tag{19}$$

is a 4-monomial feedback function that generates a de Bruijn sequence.

Proof. Applying the transformations in Proposition 3 and Proposition 2 to f respectively, the feedback function f' that generates a de Bruijn sequence is constructed.

Chan et al. [12] studied the maximum length quadratic feedback function of the form

$$q(x_1, \ldots, x_n) = x_1 + x_i + x_j + x_i.x_j. \tag{20}$$

After empirical analysis, they observed that the number of such polynomials decreases to zero as n gets larger. Our results also support their observation in the sense that there exists no quadratic I for $12 < n \leq 36$ (See Table 2).

We have enumerated all 4-monomial NFSRs with period 2^n and list them in Table 2. We observe that the fourth monomial I only takes linear and quadratic values.

Following conjecture states that I can only take linear values for large n.

Conjecture 1. Let $f(x_1, \ldots, x_n) = 1 + x_1 + x_2 \cdots x_n + I$ be a 4-monomial feedback function with maximum period. Then, for $n > 12$

$$d(I) = 1. \tag{21}$$

4.2 2^{n-1}-Monomial NFSRs

The feedback function with $k = 2^{n-1}$ monomials is of the form

$$f(x_1, \ldots, x_n) = x_1 + x'_2.x'_3 \ldots x'_n + x_i \tag{22}$$

for $2 \leq i \leq n$. The ANF of the monomial $x'_2.x'_3 \ldots x'_n$ consists of all of the possible 2^{n-1} monomials and it is known that not all of the linear monomials exist in the algebraic normal form of f, thus one of the linear monomials x_i $(2 \leq i \leq n)$ is added to cancel one of the linear monomials.

Construction of 2^{n-1}-monomial NFSRs The following proposition states that the only way to generate $k = 2^{n-1}$ monomial NFSRs is to use primitive trinomials and the transformation in Proposition 1.

Proposition 14. *$N_{n,2^{n-1}}$ is equal to the number of primitive trinomials of degree n.*

Table 2. Exhaustive list of maximum length feedback functions of the form $1 + x_1 + x_2 \dots x_n + I$ for $n \leq 36$

n	I	
	Linear	Quadratic
3	x_2, x_3	-
4	x_2, x_4	x_2x_3, x_3x_4
5	x_3, x_4	x_2x_4, x_3x_5
6	x_2, x_6	$x_2x_3, x_2x_5, x_3x_4,$ x_3x_6, x_4x_5, x_5x_6
7	x_2, x_4, x_5, x_7	x_2x_6, x_3x_7
8	-	$x_2x_6, x_4x_5, x_4x_8, x_5x_6$
9	x_5, x_6	-
10	x_4, x_8	-
11	x_3, x_{10}	-
12	-	x_5x_8, x_6x_9
13	-	-
14	-	-
15	$x_2, x_5, x_8, x_9, x_{12}, x_{15}$	-
16	-	-
17	$x_4, x_6, x_7, x_{12}, x_{13}, x_{15}$	-
18	x_8, x_{12}	-
19	-	-
20	x_4, x_{18}	-
21	x_3, x_{20}	-
22	x_2, x_{22}	-
23	$x_6, x_{10}, x_{15}, x_{19}$	-
24	-	-
25	x_4, x_8, x_{19}, x_{23}	-
26	-	-
27	-	-
28	$x_4, x_{10}, x_{14}, x_{16}, x_{20}, x_{26}$	-
29	x_3, x_{28}	-
30	-	-
31	$x_4, x_7, x_8, x_{14},$ $x_{19}, x_{25}, x_{26}, x_{29}$	-
32	-	-
33	x_{14}, x_{21}	-
34	-	-
35	x_3, x_{34}	-
36	x_{12}, x_{26}	-

Proof. For each primitive trinomial, there exists a linear function with period $2^n - 1$ and this linear function can be converted to a nonlinear feedback function with period 2^n using the transformation in Prop. 1.

Assume f is a maximum length feedback function with 2^{n-1} monomials. It is known that not all of the linear monomials exits in the ANF of f, therefore a maximum length feedback function with $2^n - 1$ monomial misses one of the linear monomials. Adding the monomial $x'_2x'_3 \dots x'_n$ divides the maximum cycle into two cycles, one of which is the all zero cycle and the other is a sequence with period $2^n - 1$ generated by a linear feedback function with two linear monomials, whose connection polynomial is a trinomial primitive polynomial.

Swan [13] proved that there are no primitive trinomials when n is a multiple of 8, therefore $NFSR_{8k,2^{n-1}} = 0$ for $k = 1, 2, \dots$.

5 Conclusion

In this study, we focus on the properties of feedback functions of maximum length NFSRs. We presented two new conditions on feedback functions. We also studied the number of monomials in the feedback function of maximum length NFSRs and analyzed the two extreme cases where $k = 4$ and 2^{n-1}. We gave construction methods using four basic transformations. For 4-monomial NFSRs, we conjecture that the degree of the free monomial is one, when $n > 12$.

Acknowledgments

We thank the anonymous reviewers for their useful comments. The third author is partially supported by TÜBİTAK under Grant No. TBAG-107T826.

References

1. M. Hell, T. Johansson, and Willi Meier. Grain - A Stream Cipher for Constrained Environments. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/010, 2005. http://www.ecrypt.eu.org/stream.
2. S. Babbage and M. Dodd. The Stream Cipher MICKEY (version 1). eSTREAM, ECRYPT Stream Cipher Project, Report 2005/015, 2005. http://www.ecrypt.eu.org/stream.
3. C. De Cannire and B. Preneel. Trivium specifications. eSTREAM, ECRYPT Stream Cipher Project, Report 2005/030, 2005. http://www.ecrypt.eu.org/stream.
4. A. J. Menezes, P. C. van Oorschot, and S. A. Vanstone. *Handbook of applied cryptography*. CRC Press, Boca Raton, Florida, 1996.
5. A. Braeken and J. Lano. On the (im)possibility of practical and secure nonlinear filters and combiners. In *Selected Areas in Cryptography*, pages 159–174, 2005.
6. S. W. Golomb. *Shift Register Sequences*. Holden-Day, Inc., Laguna Hills, CA, USA, 1967.
7. H. Fredricksen. A survey of full length nonlinear shift register cycle algorithms. 24(2):195–221, 1982.
8. E. Dubrova, M. Teslenko, and H. Tenhunen. On analysis and synthesis of (n, k)-non-linear feedback shift registers. In *DATE '08: Proceedings of the conference on Design, automation and test in Europe*, pages 1286–1291, New York, NY, USA, 2008. ACM.
9. A. Tsuneda, K. Kudo, D. Yoshioka, and T. Inoue. Maximal-period sequences generated by feedback-limited nonlinear shift registers. *IEICE Transactions*, 90-A(10):2079–2084, 2007.
10. N. G. de Bruijn. A combinatorial problem. *In Proceedings of the Koninklijke Nederlandse Akademie van Wetenschappen. Series A*, 49(7):758–764, 1946.
11. R. Gonzalo, D. Ferrero, and M. Soriano. Some properties of non linear feedback shift registers with maximum period. *Proc. Sixth Int. Conf. Telecommunications Systems*, 1998.
12. A. H. Chan, R. A. Games, and J. J. Rushanan. On quadratic m-sequences. In *Fast Software Encryption, Cambridge Security Workshop*, pages 166–173, London, UK, 1994. Springer-Verlag.
13. R. G. Swan. Factorization of polynomials over finite fields. *Pacific J. Math.*, 12:1099–1106, 1962.