Design and Analysis of Maximal-Period Sequences Based on Nonlinear Feedback Shift Registers

Akio Tsuneda, Mayumi Oka, Masahide Nakazawa, and Takahiro Inoue

Department of Electrical and Computer Engineering, Kumamoto University
2–39–1 Kurokami, Kumamoto 860-8555, Japan
Tel: +81-96-342-3853, Fax: +81-96-342-3630
E-mail: tsuneda@eecs.kumamoto-u.ac.jp

Abstract: A design method of nonlinear feedback shift registers that can produce maximal-period sequences is given. Such a design is based on one-to-one mappings which are similar to well-known chaotic maps. Some properties of generated binary sequences are investigated and discussed.

1. Introduction

Several engineering applications require pseudorandom numbers with good properties. Especially, code division multiple access (CDMA) systems based on spread spectrum (SS) techniques need many kinds of pseudorandom numbers called *spreading sequences* for many users. Such spreading sequences play a very important role in CDMA systems because the system performance is dominated by their correlation properties[1][2]. In general, auto-correlation functions of spreading sequences are desired to be like a delta function, that is, to have small value at every time delay except 0. On the other hand, their cross-correlation functions are required to be small for every time delay since they produce co-channel interferences that cause bit errors. The linear complexity of pseudorandom sequences is also important if the security of communication systems is required as in cryptosystems[3].

The best-known spreading sequences are the so-called linear feedback shift register (LFSR) sequences such as M-sequences, Gold sequences and Kasami sequences[1][2]. As is well known, M-sequences are maximal-period sequences generated by LFSRs and have an excellent auto-correlation property. However, the number of different kinds of M-sequences with same period is extremely small. On the other hand, Gold sequences are generated by modulo-2 addition of two M-sequences with low cross-correlations, called a *preferred pair* and they have same period as the original M-sequences. Auto-correlation and balance properties of Gold sequences slightly deteriorate compared to M-sequences but there are many kinds of sequences with good cross-correlation properties. Such a set of sequences is called a *Gold family*. Hence Gold sequences are suitable for spreading sequences in CDMA systems. Kasami sequences are also generated by a similar method.

As quite different methods for generating spreading sequences, recently, there have been several attempts to use chaotic sequences that are obtained from nonlinear one-dimensional maps[4][5]. A conventional LFSR sequence and a chaotic sequence are quite different in the sense that the former is based on a finite field (or Galois field) and the latter, on the other hand, is based on real numbers. However, we often compute chaotic sequences by the help of a digital computer with finite precision, and then, the resultant orbits are no longer real numbers and they are eventually periodic. Such sequences are called *quasi-chaotic sequences.* Nevertheless, we can empirically confirm that quasi-chaotic sequences generated by modern digital computers with 64-bit floating-point operation are reasonably chaotic even if the calculation of such dynamics includes round-off errors[6].

It is noteworthy that a shift register can be regarded as a one-dimensional map with finite bits by observing states of the register at each time[7]. We can easily confirm that one-dimensional maps of LFSRs are similar to the Bernoulli map which is a famous chaotic map. Namely, we can consider that a shift register is a kind of generators of quasi-chaotic sequences. Hence, constructing such one-dimensional maps makes it possible to generate many kinds of good pseudorandom numbers including M-sequences. In general, such one-dimensional maps are realized by nonlinear feedback shift registers (NFSRs). Since a nonlinear feedback part can be any logic circuits, it seems difficult to consider all possible sequences generated by NFSRs. However, constructing one-dimensional maps makes it easier to design NFSRs which can generate maximal-period sequences.

In this paper, we design such NFSRs that can generate new maximal-period sequences and investigate their properties. As a result, it is shown that we can generate a large number of sequences with maximal period by NFSRs which can be easily designed based on a fundamental combinational logic circuit design. Furthermore, the linear complexity of the proposed sequences is found to be excellent in contrast with that of M-sequences.

2. LFSR and NFSR

The most familiar example of binary pseudorandom numbers generator is a linear feedback shift register (LFSR) as shown in Fig.1. This consists of k boxes, representing memory elements, each containing a 0 or 1. At each time unit transition, the contents of the boxes are shifted one place to the right, and some boxes are added and fed back to the leftmost box. Namely,

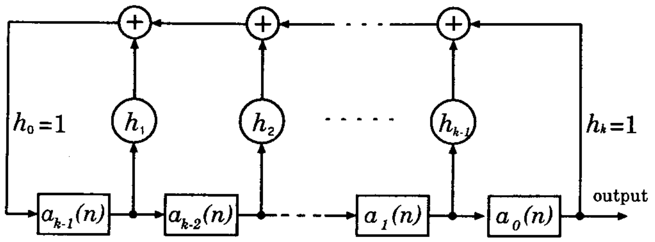


Figure 1: A linear feedback shift register.

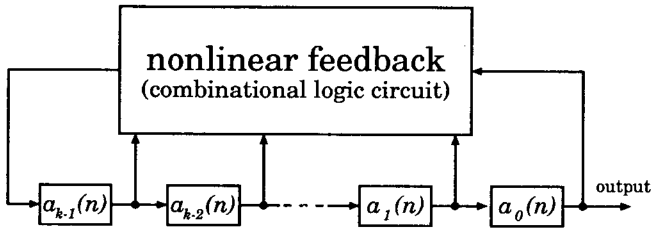
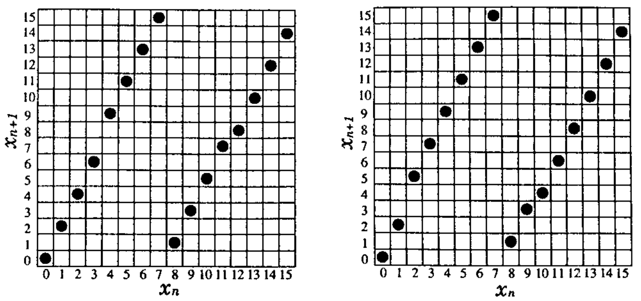


Figure 2: A nonlinear feedback shift register.



(a) LFSR (M-seq.)

(b) NFSR (M$_B$-seq.)

Figure 3: Examples of one-to-one mappings. ($k = 4$)

in Fig.1, if a state of the register is represented by $\{a_{k-1}(n), a_{k-2}(n), \cdots, a_1(n), a_0(n)\}$ at time n, then the leftmost box $a_{k-1}(n)$ is updated as

$$a_{k-1}(n+1) = h_1 a_{k-1}(n) + h_2 a_{k-2}(n) + \cdots + h_k a_0(n), \quad (1)$$

where the sum is calculated modulo-2, so $\oplus$ in the figure represents a mod-2 adder or exclusive-OR gate. Note that such a operation (mod-2 addition) is *linear* in Galois field $GF(2)$, which is the reason why the term *linear feedback* is used. Such a class of LFSRs can generate well-known M-sequences, Gold sequences, and Kasami sequences[1][2].

On the other hand, we consider a nonlinear feedback shift register (NFSR) as shown in Fig.2. The nonlinear feedback part can be any combinational logic circuit. Thus, it can be written by

$$a_{k-1}(n+1) = f(a_{k-1}(n), a_{k-2}(n), \cdots, a_0(n)) \quad (2)$$

where $f(\cdot)$ is a nonlinear function in $GF(2)$. We mainly consider sequences generated by such an NFSR.

3. Maximal-Period Sequences

3.1 Design

In Fig.1, there are 2^k possible states for the shift register. Thus, the sequence $a_0(0), a_0(1), a_0(2), \cdots$ must be periodic. But the zero state $\{0, 0, \cdots, 0\}$ cannot occur unless the sequence is an all-zero sequence. So the maximum possible period of such sequences is $2^k - 1$. It has been proved that if the polynomial specifying an LFSR defined by

$$h(x) = h_0 x^k + h_1 x^{k-1} + \cdots + h_{k-1} x + h_k \quad (3)$$

is primitive, then the LFSR generates a sequence $a_0(0), a_0(1), a_0(2), \cdots$ of period $2^k - 1$ from any nonzero starting state. Any segment $a_0(i), a_0(i+1), \cdots, a_0(i + 2^k - 2)$ of length $2^k - 1$ is called a *maximal-length sequence* or simply an *M-sequence.*

Now consider methods to generate maximal-period sequences by NFSRs. Since there are infinite kinds of combinational logic circuits which can be used as the nonlinear feedback part, it is impossible to consider all of them. However, the number of possible states is 2^k which is same as LFSRs. Hence, the number of different kinds of sequences generated by NFSRs is also finite. To find such maximal-period sequences, we propose the following method.

Firstly, a state of the register, denoted by $\{a_{k-1}(n), a_{k-2}(n), \cdots, a_0(n)\}$, is transformed into a decimal integer $x_n \in [0, 2^k - 1]$ as

$$x_n = a_0(n) \cdot 2^{k-1} + a_1(n) \cdot 2^{k-2} + \cdots + a_{k-1}(n) \cdot 2^0. \quad (4)$$

It is obvious that for any nonlinear function $f(\cdot)$ including a linear function in LFSRs, x_{n+1} must satisfy

$$x_{n+1} = \begin{cases} 2x_n \quad \text{or} \quad 2x_n + 1 & \text{for } x_n \in [0, 2^{k-1} - 1] \\ 2x_n - 2^k \quad \text{or} \quad 2x_n - 2^k + 1 & \text{for } x_n \in [2^{k-1}, 2^k - 1]. \end{cases} \quad (5)$$

Such a mapping $x_n \rightarrow x_{n+1}$ in eq.(5) specifies the nonlinear function $f(\cdot)$. Thus we consider such mappings for design of maximal-period sequences based on NFSRs. Such a mapping is easily obtained by plotting (x_n, x_{n+1}). Note that it must be a one-to-one mapping in order to generate maximal-period sequences. Hence, from eq.(5), we have the restriction of such plotting that if $x_n \in [0, 2^{k-1} - 1]$ is mapped to $2x_n$, then $x_n + 2^{k-1}$ must be mapped to $2x_n + 1$, and if $x_n \in [0, 2^{k-1} - 1]$ is mapped to $2x_n + 1$, then $x_n + 2^{k-1}$ must be mapped to $2x_n$.

In NFSRs, we can use the zero state $\{0, 0, \cdots, 0\}$ as a part of states in generating maximal-period sequences. But, in this paper, we don't use the zero state, that is, $f(0, 0, \cdots, 0) = 0$. (Simultaneously, this means $f(0, \cdots, 0, 1) = 1$.) Hence, the maximal possible period is also $2^k - 1$ which is same as in LFSRs.

Table 1: Total number of sequences and number of maximal-period sequences generated by NFSRs.

k	Total No. of Seq.	No. of M$_\text{B}$-seq. (M-seq.)
3	4	2 (2)
4	64	16 (2)
5	16,384	2,048 (6)
6	1,073,741,824	67,108,864 (6)

Examples of such mappings are shown in Fig.3, where $k = 4$. Fig.3(a) denotes the mapping for generating an M-sequence. On the other hand, Fig.3(b) denotes the mapping for generating a maximal-period sequence which is different from any M-sequences. We call such new maximal-period sequences *M_B-sequences*[7]. As shown in Fig.3, the shape of one-to-one mappings based on NFSRs in Fig.2 is similar to the *Bernoulli map* which is one of well-known chaotic maps. As pointed out in [8], an M-sequence is one of finite-word-length approximations to the Bernoulli map. Similarly, an M$_\text{B}$-sequence is also one of finite-word-length approximations to the Bernoulli map.

One-to-one mappings mentioned above cannot always generate maximal-period sequences. Thus, we find the mappings generating maximal-period sequences by exhaustive search of all possible plotting described above. For $k = 3$ to 6, the number of maximal-period sequences including M-sequences is shown in Table 1. We find that there are numerous kinds of sequences with maximal period for each k. We can show that the total number of sequences, $\Phi(k)$, is given by

$$\Phi(k) = 2^{2^{k-1}-2}. \qquad (6)$$

Furthermore, according to our conjecture from Table 1, the number of maximal-period sequences, $\Psi_B(k)$, is given by

$$\Psi_B(k) = \frac{\Phi(k)}{2^{k-1}}. \qquad (7)$$

Once the mapping is selected, we can easily design the combinational logic circuit realizing the nonlinear feedback part as follows. The mapping determines all outputs of the function $f(\cdot)$ given by eq.(2) for 2^k kinds of input patterns. Thus we can make the truth table which represents such an input-output relation. Therefore, the logic circuit realizing the truth table can be constructed based on the fundamental combinational logic circuit design. An example of such design is shown in Fig.4.

Next we consider another type of NFSRs different from Fig.2. To do this, we construct one-to-one mappings which are similar to the *tent map* which is also one of well-known chaotic maps. An examples of such mappings is shown in Fig.5. We can also find maximal-period sequences generated from such tent-type mappings by exhaustive search. Such maximal-period sequences are called *M_T-sequences.* Table 2 shows the number of maximal-period sequences generated by tent-type mappings for $k = 3$ to 6. We can find that the number of M$_\text{T}$-sequences is half of that of M$_\text{B}$-sequences for each k.

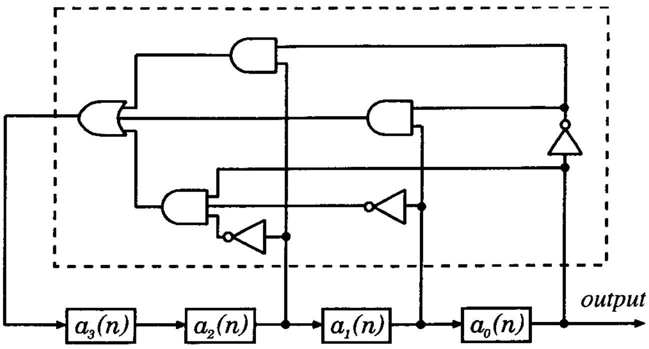


Figure 4: An example of NFSRs for M$_\text{B}$-sequences.

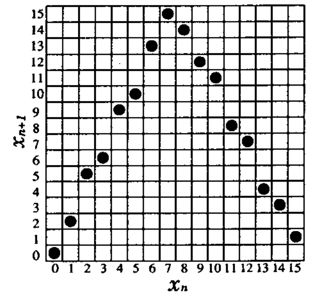


Figure 5: An example of one-to-one tent-type mappings. ($k = 4$)

Tent-type mappings can be realized by a modified NFSR shown in Fig.6. Similarly to the Bernoulli mapping, we can design logic circuits realizing the nonlinear feedback part. Figure 7 shows an example of such modified NFSRs for M$_\text{T}$-sequences.

3.2 Correlation Properties

As is well known, M-sequences generated by LFSRs have excellent periodic auto-correlation properties. However, the number of different kinds of M-sequences of same period is extremely small. On the other hand, as in the previous subsection, NFSRs can produce a large number of different kinds of maximal-period sequences, which is one of advantages of using NFSRs rather than LFSRs. But, their auto-correlation properties deteriorate compared to M-sequences as reported in [7]. Nevertheless, they can produce new families of sequences with good cross-correlation properties which are comparable to Gold families as also reported in [7].

3.3 Linear Complexity

The *linear complexity* or *linear span* is the length of the shortest linear recursion over $GF(p)$ such as eq.(1). In other words, it is the length of the shortest LFSR that

Table 2: The number of maximal-period sequences generated by tent-type mappings.

k	Total No. of Seq.	No. of $\mathrm{M_T}$-seq.
3	4	1
4	64	8
5	16,384	1,024
6	1,073,741,824	33,554,432

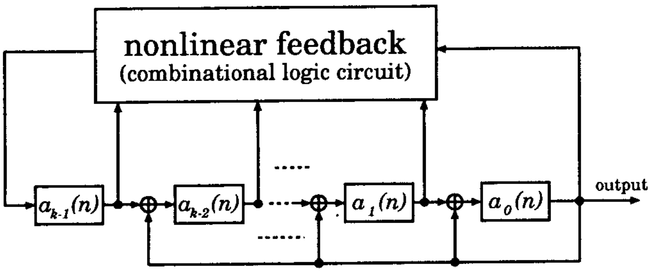


Figure 6: A modified nonlinear feedback shift register.

could produce the sequence. The linear complexity of a sequence is one measure of its unpredictability which is of great interest for cryptographic reason. Hence, a pseudorandom sequence used in cryptography should have large linear complexity compared with its period. If a sequence has linear complexity ℓ, then its linear recursion can be determined from any 2ℓ successive elements of the sequence. The remaining elements can then be produced from the recursion.

It is obvious that the linear complexity of an M-sequence of period $N = 2^k - 1$ is equal to k which is the minimum value for the period. Thus we can expect that the linear complexity of NFSR sequences proposed in this paper will be enhanced. Figure 8 shows examples of the linear complexity of $\mathrm{M_B}$-sequences of period $N = 31$. We can find that their linear complexity is almost equal to $N/2$ which is the maximum value for period N, that is, same as the linear complexity of truly random sequences. Hence, with respect to the linear complexity, the proposed NFSR sequences are superior to LFSR sequences. This is another advantage of using NFSRs rather than LFSRs.

4. Concluding Remarks

Design methods of nonlinear feedback shift registers (NFSRs) which can generate maximal-period sequences have been proposed. In such designs, we consider one-to-one mappings which specify nonlinear feedback parts of NFSRs. As a result, it has been shown that we can generate a large number of maximal-period sequences by NFSRs. Several examples of such designs has also been given. Furthermore, we found that the linear complexity of such sequences is equivalent to that of a truly random sequence.

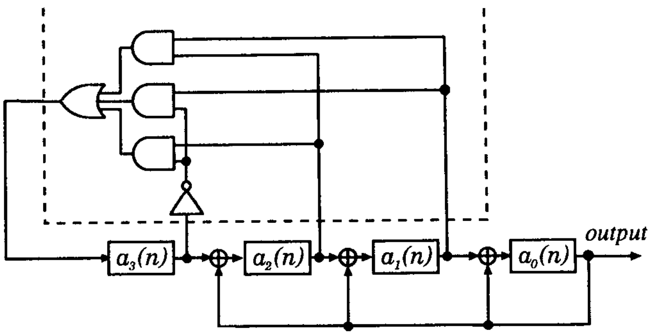


Figure 7: An example of modified NFSRs for $\mathrm{M_T}$-sequences.

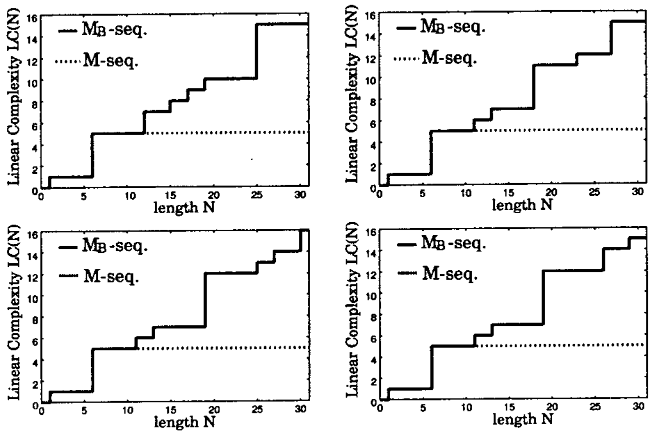


Figure 8: Examples of linear complexity of $\mathrm{M_B}$ sequences. ($k = 5$, $N = 31$)

References

[1] D. V. Sarwate and M. B. Pursley, "Crosscorrelation Properties of Pseudorandom and Related Sequences," *Proc. IEEE*, vol.68, no.3, pp.593–619, 1980.

[2] P. Fan and M. Darnell, *Sequence Design for Communications Applications*, Research Studies Press, 1996.

[3] J. L. Massey, "An Introduction to Contemporary Cryptology," *Proc. IEEE*, vol.76, no.5, pp.533–549, 1988.

[4] T. Kohda and A. Tsuneda, "Pseudonoise Sequences by Chaotic Nonlinear Maps and Their Correlation Properties," *IEICE Trans. on Communications*, vol.E76-B, no.8, 855–862, 1993.

[5] T. Kohda and A. Tsuneda, "Statistics of Chaotic Binary Sequences", *IEEE Trans., Information Theory*, vol.43, no.1, pp.104–112, 1997.

[6] E. A. Jackson, *Perspectives Nonlinear Dynamics*, Cambridge Univ. Press, 1989.

[7] A. Tsuneda, M. Nakazawa, and T.Inoue, "On Maximal-Period Sequences Based on One-to-one Mappings Using Finite Registers," *Proc. of ITC-CSCC'98*, vol.II, pp.1575–1578, July, 1998.

[8] T. Kohda and M. Fukushige, "Note on Finite-Word-Length Realization of Bernoulli Shift by *M* Sequence", *IEICE Trans.*, vol.E74, no.10, pp.3024–3028, 1991.