The Construction of Nonlinear Feedback Shift Registers of Small Orders

Janusz Szmidt, Przemysław Dąbrowski
Military Communication Institute
ul. Warszawska 22A, 05-130 Zegrze, Poland
{j.szmidt, p.dabrowski}@wil.waw.pl

Abstract—We investigate and implement the method of joining cycles of states generated by non-singular feedback shift registers to construct feedback Boolean functions which produce binary sequences of maximum period. The method is successfully used to obtain all registers of order 4 and 5 which output de Bruijn sequences.

Keywords: nonlinear feedback shift registers, adjacency graphs, de Bruijn sequences.

I. INTRODUCTION

Feedback shift registers (FSRs) are useful in generating periodic sequences, and they are used in communication and cryptographic systems. Linear feedback shift registers (LFSRs) and non-linear ones (NFSRs) are the main building blocks of many stream ciphers. The algorithms Mickey [1], Trivium [3], Grain [11], Achterbahn [7] and the alternating step generator [17] are examples of stream ciphers in whose design NFSRs have been used. The LFSRs are well-understood mathematically. The investigation of NFSRs was started in the pioneering book of Golomb [8] and has continued for several decades. In cryptographic applications, NFSRs generating modified de Bruijn sequences are important since in special cases the algebraic normal form (ANF) of the corresponding Boolean feedback functions is simpler than that of de Bruijn sequences (see, e.g., [7, 16]). We implement the method of joining cycles generated by chosen registers to construct all feedback functions of non-linear feedback shift registers which generate modified de Bruijn sequences of fixed order. The method of joining cycles to get longer ones was investigated in [8, 6, 9, 10, 13] and very recently in [12]. In [15] we proved that the operation of cross joining enables one to construct all de Bruijn sequences of fixed order starting from a given one. In the present note we show that one can construct all feedback functions of registers of order 4 and 5 starting from a chosen set of linear Boolean functions for order 4, and from a chosen set of linear and quadratic Boolean functions for order 5. The goal is achieved by using adjacency graphs and the algorithm to construct all spanning trees of these graphs.

II. THE BASIC FACTS

Let \( F_2 = \{0, 1\} \) denote the binary field and \( F_2^n \) the vector space of all binary \( n \)-tuples. A binary feedback shift register (FSR) of order \( n \) is a mapping \( F : F_2^n \rightarrow F_2^n \)
of the form

\[
F : (x_0, x_1, \ldots, x_{n-1}) \mapsto (x_1, x_2, \ldots, x_n, f(x_0, x_1, \ldots, x_{n-1})),
\]

where the feedback function \( f \) is a Boolean function of \( n \) variables. The FSR is called non-singular if the mapping \( F \) is one-to-one, i.e., \( F \) is a bijection of \( F_2^n \). It is known [8] that \( F \) is one-to-one if and only if the function \( f \) can be written in the form

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

where \( g \) is a function from \( F_2^{n-1} \) to \( F_2 \).

The algebraic normal form (ANF) of a Boolean function \( f \) of \( n \) variables is given by

\[
f(x_0, x_1, \ldots, x_{n-1}) = \sum a_{i_1 \ldots i_n} x_{i_1} \cdot \ldots \cdot x_{i_n}, \quad a_{i_1 \ldots i_n} \in F_2,
\]

where the sum runs through all \( t \)-subsets \( \{i_1, \ldots, i_t\} \subset \{0, 1, \ldots, n-1\} \). The algebraic degree of \( f \) is the largest \( t \) for which \( a_{i_1 \ldots i_n} \neq 0 \). The FSR is called linear (LFSR) if the feedback function \( f \) is linear, and is non-linear (NFSR) if \( f \) is nonlinear, i.e., \( f \) has terms of algebraic degree greater than one in its algebraic normal form.

DEFINITION 1. A de Bruijn sequence of order \( n \) is a sequence of length \( 2^n \) of elements of \( F_2 \) in which all different \( n \)-tuples appear exactly once.

It was proved by Flye Sainte-Marie [5] in 1894 and independently by de Bruijn [2] 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 [14] of order \( n \) is a sequence of length \( 2^n - 1 \) obtained from a de Bruijn sequence of order \( n \) by removing one zero from the tuple of \( n \) consecutive zeros.

THEOREM 1. Let \( (s) \) be a de Bruijn sequence of order \( n \). Then there exists a Boolean function \( F(x_0, \ldots, x_{n-1}) \) such that \( s_{t+1} = s_t + F(s_{t+1}, \ldots, s_{t+n}) \), \( t = 0, 1, \ldots, 2^n - n - 1 \).

This means that for the feedback function of (1) we have

\[
f(x_0, x_1, \ldots, x_{n-1}) = x_0 + F(x_1, \ldots, x_{n-1})
\]
The $n$-th order de Bruijn graph $G_n$ is a directed graph with $2^n$ vertices, each labelled with a unique $n$-tuple. For two vertices $X = (x_0, x_1, \ldots, x_{n-1})$ and $Y = (y_0, y_1, \ldots, y_{n-1})$ in $G_n$, an edge is drawn from $X$ to $Y$ if and only if $(x_i, x_{i+1}, \ldots, x_{n-1}) = (y_0, y_1, \ldots, y_{n-1})$.

Given an $n$-stage FSR, its state graph is a subgraph of $G_n$ with $2^n$ vertices such that there is an edge from $X$ to $Y$ if and only if $F(X) = Y$, where $F$ is given by (1). We say that $X$ is a predecessor of $Y$ and $Y$ is a successor of $X$. Let $a = (a_0, a_1, \ldots, a_{n-1})$ be a state of a de Bruijn sequence generated by the feedback function $f$. The conjugate of the state $a$ is $\tilde{a} = (\tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{n-1})$, where $\tilde{a} = a + 1$ is the negation of the bit $a$. For a Boolean function of the form (2) the corresponding FSR decomposes the space $F_2^n$ into several cycles; in the special case of Theorem 1 we have only one cycle. Let us consider the case when there is more than one cycle. If two different cycles have the property that there is a pair of conjugate states generated by the register such that one of the states is on one cycle and the other is on the other cycle, then the cycles can be joined to form a new cycle by the following theorem.

**Theorem 2.** Suppose a function $f$ of the form (2) generates more than one cycle and let

$$\begin{align*}
    a &= (a_0, a_1, \ldots, a_{n-1}) = (a_0 U), \\
    \tilde{a} &= (\tilde{a}_0, \tilde{a}_1, \ldots, \tilde{a}_{n-1}) = (\tilde{a}_0 U)
\end{align*}$$

be a pair of conjugate states which are on two different cycles. Let the Boolean function $h(x_0, \ldots, x_{n-1})$ be defined by the negation of $g(U)$. Then the function

$$f_i = x_i \land h(x_0, \ldots, x_{n-1})$$

has one cycle in place of two for the function $f$. We have an algebraic formula

$$h(x_0, \ldots, x_{n-1}) = g(x_0, \ldots, x_{n-1}) + (x_i + \tilde{a}_i) \cdot (x_{i+1} + \tilde{a}_{i+1}) \cdot \ldots \cdot (x_{n-1} + \tilde{a}_{n-1}).$$

For a given non-singular FSR with a feedback function $f$ the process of joining cycles can be continued and finally we obtain a register with a feedback function which generates only one cycle. The problem of determining conjugate pairs between cycles in a state graph leads to the notion of an adjacency graph [10, 13].

**Definition 3.** For an FSR, its adjacency graph is an undirected graph where the vertices correspond to the cycles in its state graph, and there is an edge between two vertices if and only if they share a conjugate pair.

### III. The Construction of Registers of Order 4

We have applied the above described method of joining cycles to construct all feedback functions of registers of order 4 generating modified de Bruijn sequences. We have chosen linear feedback functions (Table 1) and we have found the cycles and conjugate pairs of states for these registers which gives us the adjacency graphs.

**Table 1.** The number of spanning trees for linear feedback functions of order 4.

<table>
<thead>
<tr>
<th>Linear func.</th>
<th>Spann. trees</th>
<th>Linear func.</th>
<th>Spann. trees</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x_0$</td>
<td>12</td>
<td>$x_0 + x_1$</td>
<td>1</td>
</tr>
<tr>
<td>$x_0 + x_2$</td>
<td>8</td>
<td>$x_0 + x_3$</td>
<td>1</td>
</tr>
<tr>
<td>$x_0 + x_1 + x_2$</td>
<td>6</td>
<td>$x_0 + x_1 + x_3$</td>
<td>12</td>
</tr>
<tr>
<td>$x_0 + x_2 + x_3$</td>
<td>6</td>
<td>$x_0 + x_1 + x_2 + x_3$</td>
<td>8</td>
</tr>
</tbody>
</table>

To each spanning tree corresponds a feedback function generating a modified de Bruijn sequence which is obtained as the sum of a linear function from Table 1 and the expressions obtained from weights of edges of a chosen spanning tree according to (8). It turns out that some functions constructed from different linear functions of Table 1 coincide. Hence we must continue the process until we get all feedback functions of maximum period; there are 16 such functions for order 4. Here 6 functions from Table 1 (except $x_0 + x_1$ and $x_0 + x_1 + x_1$) are enough to generate all 16 feedback functions of maximum period given in List 1.

**List 1.** Functions for modified de Bruijn sequences of order 4.

1. $x_0 + x_1 x_3 + x_2 x_3 + x_2$
2. $x_0 + x_1 x_3 + x_2 + x_3$
3. $x_0 + x_1$
4. $x_0 + x_2 + x_3 x_1$
5. $x_0 + x_1 + x_2 x_3$
6. $x_0 + x_2 x_3 + x_2 + x_3 + x_1$
7. $x_0 + x_2 x_3 + x_2$
8. $x_0 + x_1 + x_2 + x_3$
9. $x_0 + x_1$
10. $x_0 + x_3 + x_1 + x_3$
11. $x_0 + x_2 x_3 + x_1$
12. $x_0 + x_2 + x_3 + x_1$
13. $x_0 + x_2 + x_3 + x_1$
14. $x_0 + x_1 + x_2 + x_3$
15. $x_0 + x_1 + x_2 x_3 + x_1 + x_3$
16. $x_0 + x_2 x_3 + x_2 + x_3 + x_1$

*Fig. 1. The adjacency graph of the register $f(x_0, x_1, x_2, x_3) = x_0$.***
IV. THE CONSTRUCTION OF REGISTERS OF ORDER 5

A similar construction has been carried out for registers of order 5. Here the situation is more complicated. To construct all 2048 (see (3) for n = 5) feedback functions of maximum period we must take a much larger set of input functions. It appears that linear functions are not enough. The functions listed in Table 2 generate together 1508 feedback functions of maximum period. One must add to the process also quadratic generating functions. It is necessary to take 464 functions (linear and quadratic ones), construct the corresponding adjacency graphs, generate their spanning trees and thus the feedback functions of maximum period. At the end of the process there are many repetitions of generated functions, but finally we achieve the number of 2048 registers. This experiment reveals the following

Observation: The linear and quadratic non-singular feedback functions generate all registers of order 5 for modified de Bruijn sequences.

V. CONCLUSIONS

We have constructed feedback functions generating all modified de Bruijn sequences of order 4 and 5. The complexity of this process is comparable to the complexity of brute force searching of such functions where (for order 5) one considers Boolean functions of the form \( f(x_0, \ldots, x_5) = x_0 + h(x_0, x_5, x_4, x_3, x_2, x_1, x_0) \), where \( h \) is a Boolean function of algebraic degree up to 3, and checks whether the period of the generated sequence is equal to 31. There is a theoretical significance of our Observation above. One can ask to what extent it is true for orders greater than 5. For order 6 there together \( 2^{20} = 67 108 864 \) de Bruijn sequences and we are able to construct and store those corresponding to spanning trees of the adjacency graph of the register \( f(x_0, \ldots, x_6) = x_0 \) which are 2 211 840 altogether. For \( n = 7 \) there are \( 2^{24} \) de Bruijin sequences and it would be impossible to generate and store all feedback functions generating them. The method presented in this note can be extended to higher orders of registers to obtain some portion of NFSRs which generate binary sequences of maximum period.

VI. REFERENCES