The Search and Construction of Nonlinear Feedback Shift Registers

Janusz Szmidt
(joint work with Johannes Mykkeltveit)

Military Communication Institute
Zegrze, Poland

Magdeburg fq11
July 23, 2013

NLFSRs - Nonlinear Feedback Shift Registers

- Let $\mathbb{F}_2 = \{0, 1\}$ denote the binary field and $\mathbb{F}_2^n$ the vector space of all binary n-tuples.
- A binary Feedback Shift Register (FSR) of order n is a mapping

$$\mathfrak{F} : \mathbb{F}_2^n \longrightarrow \mathbb{F}_2^n$$

of the form

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

where the *feedback function* f is a Boolean function of n variables.

- The FSR is called *non-singular* if the mapping $\mathfrak{F}$ is one-to-one, i.e., $\mathfrak{F}$ is a bijection on $\mathbb{F}_2^n$.

NLFSRs - Nonlinear Feedback Shift Registers, cont.

- It was proved that the FSR is non-singular iff its feedback function has the form

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 + F(x_1, \ldots, x_{n-1}) \tag{2}$$

  where F is a Boolean function of $n-1$ variables.
- The FSR is called linear (LFSR) if the feedback function f is linear one and nonlinear (NLFSR) if the function f is nonlinear; i.e., the function f has higher degree terms in its Algebraic Normal Form (ANF).
- Further, we will consider nonsingular and nonlinear feedback shift registers.

De Bruijn sequences

- **Definition 1.** A de Bruijn sequence of order n is a sequence of length 2^n of elements of $\mathbb{F}_2$ in which all different n-tuples appear exactly once.
- It was proved by Flye Sainte-Marie in 1894 and independently by de Bruijn in 1946 that the number of cyclically inequivalent sequences satisfying the Definition 1 is equal to

$$B_n = 2^{2^{n-1}-n} \tag{3}$$

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

Nicolaas Govert de Bruijn, Dutch mathematician, 9 July 1918 - 17 February 2012

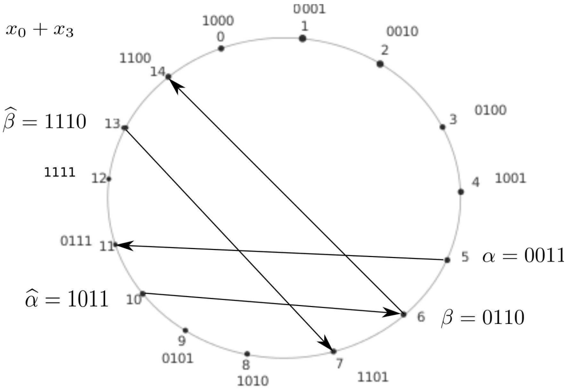
Oberwolfach, 1960

Solomon Golomb and Guang Gong, SETA 2012

Cross joint pairs

- Let $(s_t) = (s_0, s_1, \cdots, s_{2^n-2}, s_{2^n-1})$ be a de Bruijn sequence.
- We put $S_i = (s_i, s_{i+1}, \cdots, s_{i+(n-2)})$, and write the de Bruijn sequence as $(S_t) = (S_0, S_1, \cdots, S_{2^n-2}, S_{2^n-1})$.
  In the later representation each $n-1$-vector occurs exactly twice.
- **Definition 3.** Two elements $U, V \in \mathbb{F}_2^{n-1}$ constitute a cross joint pair if and only if it is possible to shift (S_t) cyclically such that the order they occur in is $U, \cdots, V, \cdots, U, \cdots, V$.
- It follows that for the pairs of states $\alpha = (u, U)$, $\widehat{\alpha} = (\overline{u}, U)$ and $\beta = (v, V)$, $\widehat{\beta} = (\overline{v}, V)$, where $\overline{u} = u + 1$ is a negation of a bit u, the order they occur in is α, β, $\widehat{\alpha}$, $\widehat{\beta}$.

Cross joint pairs - an example



$\alpha = 0011 \qquad \beta = 0110$

$\widehat{\alpha} = 1011 \qquad \widehat{\beta} = 1110$

$\overline{x_1}x_2x_3 \qquad x_1x_2\overline{x_3}$

$$x_0 + x_3 + \overline{x_1}x_2x3 + x_1x_2\overline{x_3} = x_0 + x_3 + x_1x_2 + x_2x_3$$

De Bruijn sequences and NLFSRs

Theorem 1. Let (s_t) be a de Bruijn sequence. Then there exists a Boolean function $F(x_1, \cdots, x_{n-1})$, such that

$$s_{t+n} = s_t + F(s_{t+1}, \cdots, s_{t+n-1}), \quad t = 0, 1 \cdots, 2^n - n - 1. \qquad (4)$$

(The proof is given in Golomb's book: *Shift Register Sequences*).
AN OLD PROBLEM
Construct or describe Boolean functions F which give all de Bruijn sequences.

De Bruijn sequences and NLFSRs. cont.

A. Klapper, M. Goresky, *Algebraic Shift Register Sequences*. Cambridge University Press, 2012.
page 175 :
One of the long-standing unsolved problems in the theory of de Bruijn sequences is that of finding a simple prescription for those feedback functions f which produce de Bruijn and punctured de Bruijn sequences.

De Bruijn sequences and NLFSRs, cont.

The next theorem is a classical result.
Theorem 2. Let (s_t) be a de Bruijn sequence satisfying (4) and let us assume that there is a cross joint pair U, V for the sequence (s_t). Let the Boolean function $G(x_1, \cdots, x_{n-1})$ be obtained from $F(x_1, \cdots, x_{n-1})$ by complementing $F(U), F(V)$, then $G(x_1, \cdots, x_{n-1})$ also generates a de Bruijn sequence (u_t), say.
We say that (u_t) is obtained from (s_t) by the cross joint pair operation.
Proof
Complementing $F(U)$ will split the de Bruijn sequence into two sequences, and complementing $F(V)$ will join these two sequences again, since U, V is a cross joint pair.

Cross joining de Bruijn sequences

Theorem 3. (*J. Mykkeltveit and J. Szmidt*)
Let (u_t), (v_t) be two de Bruijn sequences of degree n. Then (v_t) can be obtained from (u_t) by repeated application of the cross joint pair operation.

Proof.

- We observe that the cross joint pair operation is an equivalence relation.
- We order the functions F in (2) lexicographically and let us denote this ordered set S. We choose the ordering in such a way that $F(0, 0, \cdots, 0)$ is the most significant digit.
- Let T_1 be the equivalence class containing the lexicographical largest de Bruijn sequence.
- Suppose that the theorem is false.

Cross joining de Bruijn sequences, cont. 1

- Then there must exist an non empty equivalence class T_2 different from T_1 and let H be the truth table for the lexicographical largest de Bruijn sequence in T_2. H has the following two properties:
  1. It is not the lexicographical largest de Bruijn sequence.
  2. Any cross joint pair operation which is possible to apply to H will result in a truth table less than H.
- Define

$$S_1 = \{F \in S \ : \ F \leqslant H\} \tag{5}$$

$$S_2 = \{F \in S \ : \ F > H\} \tag{6}$$

We are done if we can prove that H does not exist.

Cross joining de Bruijn sequences, cont. 2

- Let $K \in S_2$. Let $(z_1, \cdots, z_{n-1})$ be the smallest $(n-1)$-vector such that $H(z_1, \cdots, z_{n-1})$ is different from $K(z_1, \cdots, z_{n-1})$.
- Since $H < K$ we have that $H(z_1, \cdots, z_{n-1}) = 0$ and $K(z_1, \cdots, z_{n-1}) = 1$ and the choice of $(z_1, \cdots, z_{n-1})$ implies that if

$$(u_1, \cdots, u_{n-1}) < (z_1, \cdots, z_{n-1}) \tag{7}$$

  then

$$H(u_1, \cdots, u_{n-1}) = K(u_1, \cdots, u_{n-1}).$$

- Let $H1$ be obtained from H by putting $H1(z_1, \cdots, z_{n-1}) = 1$ and keeping $H1 = H$ for all other function arguments. Clearly this change will split the de Bruijn sequence such that $H1$ generates two sequences C_1 and C_2, say.

Cross joining de Bruijn sequences, cont. 3

1. We have that

$$H1(z_1, \cdots, z_{n-1}) = K(z_1, \cdots, z_{n-1}) \tag{8}$$

   which implies
   $(z_0, z_1, \cdots, z_{n-1})$ and $(z_1, \cdots, z_{n-1}, z_0 + K(z_1, \cdots, z_{n-1}))$
   either both belong to C_1 or both belong to C_2.
2. It is no restriction to assume rhat they both belong to C_1.

Cross joining de Bruijn sequences, cont. 4

- Since K generates a de Bruijn sequence it exists n-tuple $(v_0, \cdots, v_{n-1})$ such that

$$(v_0, v_1, \cdots, v_{n-1}) \in C_1$$

and

$$(v_1, \cdots, v_{n-1}, v_0 + K(v_1, \cdots, v_{n-1}) \in C_2,$$

and since $H1$ generates $C1$ we have

$$(v_1, \cdots, v_{n-1}, v_0 + H1(v_1, \cdots, v_{n-1}) \in C_1.$$

- Because of the assumption 2 after (8) we may also assume that

$$(z_0, \cdots, z_{n-1}) \neq (v_0, \cdots, v_{n-1}).$$

Cross joining de Bruijn sequences, cont. 5

- Let $H2$ be obtained from $H1$ by putting

$$H2(v_1, \cdots, v_{n-1}) = K(v_1, \cdots, v_{n-1})$$

  and keeping $H2 = H1$ for all other function arguments.
- $H2$ will generate a de Bruijn sequence, since the later operation ($H1$ changed to $H2$) corresponds to joining C_1 and C_2.
- $H < H2$ since we have (7)

$$(u_1, \cdots, u_{n-1}) < (v_1, \cdots, v_{n-1})$$

  i.e. the de Bruijn sequence generated by $H2$ is obtained from the one generated by H by the cross joint pair operation.
- This means that H does not exist, since by definition it should not be possible to obtain a de Bruijn sequence greater than the one generated by H by the cross joint pair operation (applied to the one generated by H) . QED

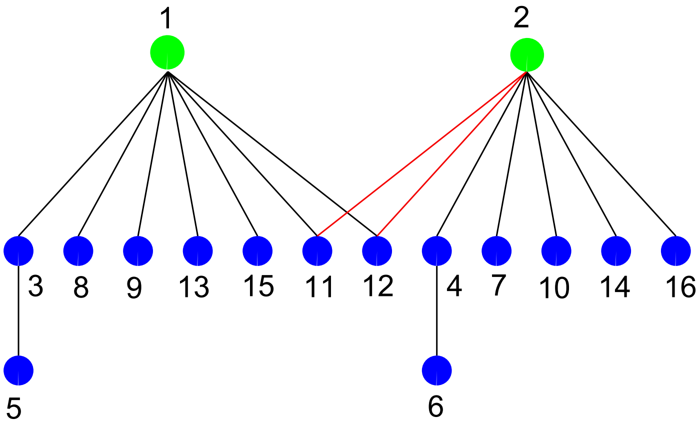
The list of all NLFSR, n = 4

- 1: $x_0 + x_1$
- 2: $x_0 + x_3$
- 3: $x_0 + x_1 + \overline{x_1}x_2x_3 + \overline{x_1}x_2\overline{x_3} = x_0 + x_1 + x_2 + x_1x_2$
- 4: $x_0 + x_3 + \overline{x_1}x_2x_3 + \overline{x_1}x_2\overline{x_3} = x_0 + x_2 + x_3 + x_1x_2$
- 5: $x_0 + x_1 + (\overline{x_1}x_2x_3 + \overline{x_1}x_2\overline{x_3}) + (x_1x_2\overline{x_3} + x_1\overline{x_2}x_3) = x_0 + x_1 + x_2 + x_1x_3$
- 6: $x_0 + x_3 + (\overline{x_1}x_2x_3 + \overline{x_1}x_2\overline{x_3}) + (x_1x_2\overline{x_3} + x_1\overline{x_2}x_3) = x_0 + x_2 + x_3 + x_1x_3$
- 7: $x_0 + x_3 + \overline{x_1}x_2\overline{x_3} + \overline{x_1x_2}x_3 = x_0 + x_2 + x_1x_2 + x_1x_3$
- 8: $x_0 + x_1 + \overline{x_1}x_2\overline{x_3} + \overline{x_1x_2}x_3 = x_0 + x_1 + x_2 + x_3 + x_1x_2 + x_1x_3$
- notation: $\overline{x_i} = x_i + 1$

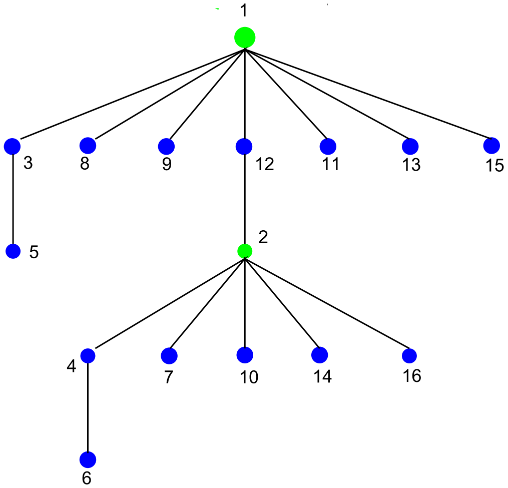
The list of all NLFSR, n = 4

- 9: $x_0 + x_1 + x_1x_2\overline{x_3} + \overline{x_1}x_2\overline{x_3} = x_0 + x_1 + x_2 + x_2x_3$
- 10: $x_0 + x_3 + x_1x_2\overline{x_3} + \overline{x_1}x_2\overline{x_3} = x_0 + x_2 + x_3 + x_2x_3$
- 11; $x_0 + x_1 + \overline{x_1}x_2x_3 + x_1x_2\overline{x_2} = x_0 + x_1 + x_1x_2 + x_2x_3$
- 12: $x_0 + x_1 + x_1\overline{x_2x_3} + \overline{x_1x_2}x_3 = x_0 + x_3 + x_1x_2 + x_2x_3$
- 13: $x_0 + x_1 + x_1\overline{x_2x_3} + \overline{x_1}x_2\overline{x_3} = x_0 + x_2 + x_1x_3 + x_2x_3$
- 14: $x_0 + x_3 + x_1\overline{x_2x_3} + x_1\overline{x_2}x_3 = x_0 + x_1 + x_2 + x_3 + x_1x_3 + x_2x_3$
- 15: $x_0 + x_1 + x_1\overline{x_2}x_3 + \overline{x_1}x_2\overline{x_3} = x_0 + x_1 + x_2 + x_1x_2 + x_1x_3 + x_2x_3$
- 16: $x_0 + x_3 + x_1\overline{x_2}x_3 + \overline{x_1}x_2\overline{x_3} = x_0 + x_2 + x_3 + x_1x_2 + x_1x_3 + x_2x_3$

First graph of NLFSRs construction for n = 4



Second graph of NLFSRs construction for n = 4



A NLFSR, n = 5

$$x_0 + x_2 + x_3 + x_4 +$$
$$\overline{x_1}\,\overline{x_2}\,\overline{x_3}x_4 + \overline{x_1}x_2x_3\overline{x_4} +$$
$$x_1x_2x_3\overline{x_4} + x_1x_2\overline{x_3}x_4 +$$
$$x_1\overline{x_2}x_3\overline{x_4} + \overline{x_1}x_2x_3\overline{x_4} =$$
$$x_0 + x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4$$

Special form NLFSRs of order n

- $n = 27, \quad x_0 + x_1 + x_2 + x_4 + x_8 + x_{10} + x_{11} + x_{14} + x_{17} + x_{19} + x_{21} + x_6 x_{10}$
- $n = 28, \quad x_0 + x_4 + x_5 + x_6 + x_8 + x_{11} + x_{14} + x_{18} + x_{19} + x_{21} + x_{22} + x_{26} + x_{27} + x_8 x_{27}$
- $n = 29, \quad x_0 + x_3 + x_5 + x_6 + x_{11} + x_{12} + x_{16} + x_{19} + x_{22} + x_{23} + x_{27} + x_{20} x_{28}$

Thank you