On Cross-Join Method for de Bruijn Sequences and Zech Logarithms

Martianus Frederic Ezerman, Adamas Aqsa Fahreza
NTU, Singapore
Janusz Szmidt, MCI, Poland

The 3rd International Workshop on Boolean Functions and their Applications
BFA 2018

20 June 2018

The Feedback Shift Registers - *FSRs*

- Let $\mathbb{F}_2$ be the binary field and $\mathbb{F}_2^n$ the n-dimensional vector space over $\mathbb{F}_2$. Let us consider a mapping

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

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

where f is a Boolean function of n variables of the form

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

and F is a Boolean function of $n - 1$ variables.

- The formula (1) defines a nonsingular *FSR* of order n.
- A nonsingular register decomposes the space $\mathbb{F}_2^n$ into a finite number of disjoint cycles.

Generating Binary Sequences

- If there is only one cycle (of length 2^n), then we have a de Bruijn sequence.
- The number of cyclically non-equivalent de Bruijn sequences of order n is (published 1946)

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

- In fact, these sequences were discovered by Fench mathematician C. Flye Sainte-Marie in 1984 and he proved the above formula.
- Consider the binary sequence $\mathbf{s} = (s_0, s_1, \ldots)$ with given n-initial elements $(s_0, \ldots, s_{n-1})$. The next elements, for $i \geqslant 0$, are calculated from the formula

$$s_{i+n} = f(s_i, s_{i+1}, \ldots, s_{i+n-1}) = s_i + F(s_{i+1}, \ldots, s_{i+n-1}).$$

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

Oberwolfach, 1960

Nonlinear Feedback Shift Registers

- *The Algebraic Normal Form (ANF)* of a Boolean function f of n variables is given by

$$f(x_0, x_1, \ldots, x_{n-1}) = \sum a_{i_1,\ldots,i_t} x_{i_1} \cdots x_{i_t} \text{ with } a_{i_1,\ldots,i_t} \in \mathbb{F}_2,$$

  where the sum is over all t-subsets

$$\{i_1, \ldots, i_t\} \subset \{0, 1, \ldots, n-1\}.$$

- In particular we have the linear recurrence

$$f(x_0, x_1, \ldots, x_{n-1}) = x_0 + c_1 x_1 + \ldots + c_{n-1} x_{n-1}.$$

  and the corresponding Linear Feedback Shift Register (*LFSR*).
- When the Boolean function F is a non-linear one, we have a Nonlinear Feedback Shift Register (*NLFSR*).

Solomon Golomb (30 May 1932 - 1 May 2016) and Guang Gong, SETA 2012

Cross-Join Pairs of States

- Let $(s_t) = (s_0, s_1, \cdots, s_{2^n-2}, s_{2^n-1})$ be a de Bruijn sequence.
- Let $S_i = (s_i, s_{i+1}, \cdots, s_{i+(n-1)})$ denote a state. Consider the de Bruijn sequence as a sequence of its states

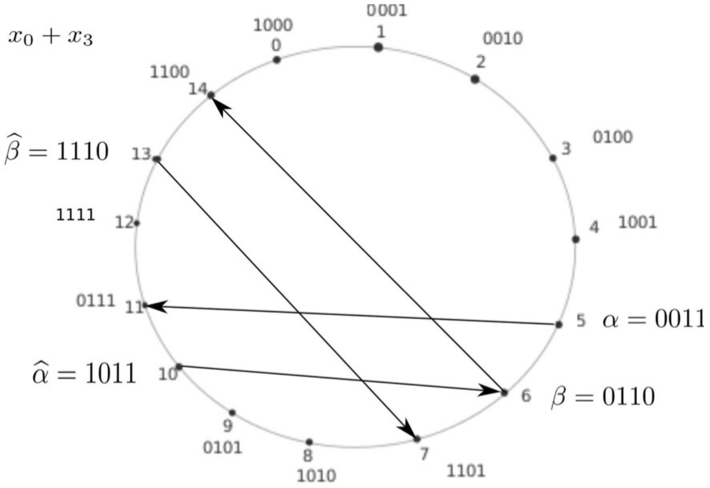
$$(S_t) = (S_0, S_1, \cdots, S_{2^n-2}, S_{2^n-1})$$

.

Definition

Two pairs of states $(a, \widehat{a})$ and $(b, \widehat{b})$ constitute cross-join pairs of states if $a = (a_0, A), \quad \widehat{a} = (\overline{a_0}, A)$ and $b = (b_0, B), \quad \widehat{b} = (\overline{b_0}, B)$, where $\overline{u} = u + 1$ is the negation of the bit u and the states appear in the order $a,\ b,\ \widehat{a},\ \widehat{b}$ in the sequence of states of a given de Bruijn sequence.
We write $A = (a_1, \cdots, a_{n-1})$ and $B = (b_1, \cdots, b_{n-1})$.

Cross-Join Pairs of States - an Example for $n = 4$



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

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

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

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

de Bruijn Sequences and the Cross-Join Pair Operation

Let $\{s_n\}$ be a de Bruijn sequence of order n (or modified de Bruijn sequence with period $2^n - 1$) generated by the feedback Boolean function f of the form (2). Let $(a, \widehat{a})$ and $(b, \widehat{b})$ are cross-join pairs of states for that sequence. Then the feedback Boolean function

$$f(x_0.x_1, \ldots, x_{n-1}) + \prod_{i=1}^{n-1}(x_i + a_i + 1) + \prod_{i=1}^{n-1}(x_i + b_i + 1) \qquad (3)$$

generates new de Bruijn sequence. We call (3) the cross-join pair operation.

Theorem 1. (*J. Mykkeltveit and J. Szmidt*, 2015)
Let (u_t), (v_t) be two de Bruijn sequences of order n. Then (v_t) can be obtained from (u_t) by repeated applications of the cross-join operation.

The List of NLFSRs for $n = 4$

- 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 NLFSRs for n = 4

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

Finite Fields, Primitive Polynomials and *m*-Sequences

- Let $p(x) = x^n + c_{n-1}x^{n-1} + \cdots + c_1 x + 1$ be a primitive polynomial of degree n with binary coefficients.
- Then the linear recurrence

$$g(x_0, x_1, \ldots, x_{n-1}) = x_0 + c_1 x_1 + \cdots + c_{n-1} x_{n-1}$$

  generates the *m*-sequence which is a binary sequence of the period $2^n - 1$.
- Let a be a root of the polynomial $p(x)$, i.e. $p(a) = 0$ in the Galois field $GF(2^n)$ constructed by the polynomial $p(x)$.
- The sequence of elements $\{1, a, a^2, \ldots, a^{2^n-2}\}$ in $GF(2^n)$ has period $2^n - 1$ and directly leads to a binary *m*-sequence.

Evariste Galois (25 October 1811 - 31 May 1832)

Zech Logarithms in $GF(2^n)$

- Let $j \in \{1, \ldots, 2^n - 2\}$
- Then the integer $Z(j)$ such that

$$1 + a^j = a^{Z(j)}$$

  is the Zech logarithm of j.
- Then we have a one-to-one function

$$Z : \{1, \ldots, 2^n - 2\} \longrightarrow \{1, \ldots, 2^n - 2\}$$

- The Zech logarithms are tabularized. There are effective algorithms to calculate them.
- The `Magma` computer algebra system can calculate the Zech logarithms for $n \leqslant 430$, *i.e.*, in $GF(2^{430})$.

The Feedback Functions of the Constructed NFSRs

- Take the primitive polynomial $x^5 + x^2 + 1$.
- The values of the feedback function at the points of 'the jumps', say $Z(2) = 5$ and $Z(4) = 10$ are

$$A = (0,0,0,0,1) \text{ and } B = (0,0,1,0,0).$$

- The feedback function of the NLFSR is $f =$

$$x_0 + x_2 + (x_1+1)(x_2+1)(x_3+1)x_4 + (x_1+1)x_2(x_3+1)(x_4+1)$$
$$= x_0 + x_4 + x_1x_2x_3 + x_1x_2 + x_1x_3x_4 + x_1x_4 + x_2x_3 + x_3x_4.$$

- The quadratic feedback function for the register of order 5 obtained by applying the cross-join operation twice is

$$x_0 + x_4 + x_2x_3 + x_3x_4.$$

- The quadratic feedback function for the register of order 6 obtained similarly is

$$x_0 + x_1 + x_2 + x_5 + x_1x_2 + x_1x_5.$$

The Cross-Join Pair for LFSR of Order $n = 31$

- Let a be a root of the primitive polynomial $p(x) = x^{31} + x^3 + 1$.
- We use the mapping $Z(2n) = 2Z(n)$ for the Zech logarithm. The cross-join pairs $c := (3, 6, 31, 62)$ abbreviates the pair of states $(a^3, a^6, 1 + a^3 = a^{31}, 1 + a^6 = a^{62})$ since $Z(3) = 31$.
- The states of LFSR at 'the jumps':
  $A = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
  $0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0)$, $A_{28} = 1$,
  $B = (0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$
  $0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0)$, $B_{25} = 1$.
- The corresponding feedback function of the constructed NLFSR

$$f = x_0 + x_3 + \prod_{i=1}^{30} (x_i + A_i + 1) + \prod_{i=1}^{30} (x_i + B_i + 1).$$

It is a Boolean function of degree 29.

The Cross-Join Pairs for Order $n = 127$

- Use the primitive polynomial $p(x) = x^{127} + x + 1$.
- Since $Z(1) = 127$, making $Z(2) = 254$, we have the sequence of mutually disjoint cross-join pairs:

$$c_i = (2^{8i}, 2^{1+8i}, 127 \cdot 2^{8i}, 127 \cdot 2^{1+8i}) \text{ for } i = 0, 1, \ldots, 15.$$

- From this family we can construct $2^{16} - 1$ NFSRs of order $n = 127$ which generate sequences of the period $2^{127} - 1$.
- An Example: the cross-join pairs $c_3 = (2^{24}, 2^{25}, 127 \cdot 2^{24}, 127 \cdot 2^{127})$.
- The corresponding Boolean feedback function has algebraic degree 125.

The Quadratic NLFSRs of Order $n \in \{27, 28, 29\}$

- For $n = 27$

$$x_0 + x_1 + x_2 + x_4 + x_8 + x_{10} + x_{11} + x_{14} + x_{17} + x_{19} + x_{21} + x_6 x_{10}.$$

- For $n = 28$

$$x_0 + x_4 + x_5 + x_6 + x_8 + x_{11} + x_{14} + x_{18} + x_{19} + x_{21} + x_{22} + x_{26} + x_{27} + x_8 x_{27}.$$

- For $n = 29$

$$x_0 + x_3 + x_5 + x_6 + x_{11} + x_{12} + x_{16} + x_{19} + x_{22} + x_{23} + x_{27} + x_{20} x_{28}$$

and

$$x_0 + x_4 + x_6 + x_7 + x_9 + x_{10} + x_{11} + x_{12} +$$
$$x_{16} + x_{17} + x_{21} + x_{25} + x_{26} + x_{17} x_{21}$$

Publications

- C.Y. Li, X.Y. Zeng, T. Helleseth, C.L. Li and L. Hu. The properties of a class of linear FSRs and their applications to the construction of nonlinear FSRs. IEEE Trans. Inf. Theory, vol. 60, no. 5, 2014, pp. 3052-3061.
- C.Y. Li, X.Y. Zeng, C.L. Li and T. Helleseth. A class of de Bruijn sequences. IEEE Trans. Inf. Theory, vol. 60, no. 12, 2014, pp. 7955-7969.
- C.Y. Li, X.Y. Zeng, C.L. Li, T. Helleseth and M. Li. Construction of de Bruijn sequences from LFSRs with reducible characteristic polynomial. IEEE Trans. Inf. Theory, vol. 62, no. 1, 2016, pp. 610-624.
- M. Li, Y. Jiang, D. Lin. The adjacency graphs of some feedback shift registers. Design, Codes and Cryptography, accepted to publish, February 2016.
- J. Dong, D. Pei. Construction for de Bruijn sequences with large stage, under review.

Publications

- T. Rachwalik, J. Szmidt, R. Wicik, J. Zabłocki. Generation of nonlinear feedback shift register with special-purpose hardware. Military Comunications and Information Systems Conference MCC 2012, pp.151-154.
- P. Dąbrowski, G. Łabuzek, T. Rachwalik, J. Szmidt. Searching for nonlinear feedback Shift register with parallel computing. Information Processing Letters, 114,(2014), pp. 268-272.
- J. Mykkeltveit, J. Szmidt. Nieliniowe rejestry przesuwne I łączenie skrzyżowanych par stanów. Studia Bezpieczeństwa Naro-dowego. Kryptologia i Cyberbezpieczeństwo. Wojskowa Akademia Techniczna. Warszawa 2014. str. 271 – 283.
- J. Mykkeltveit, J. Szmidt. On cross joining de Bruijn sequences. Contemporary Mathematics, 2015, vol.63, s.335-346.
- J. Szmidt, P. Dąbrowski. The construction of nonlinear feedback shift registers of small orders . In International Conference on Military Communications and Information Systems (ICMCIS), 18-19 May 2015 Cracow.

THANK YOU