A class of maximum-length NLFSRs

Chunlei Li

A joint work with Chaoyun Li, Xiangyong Zeng, Tor Helleseth and Lei Hu

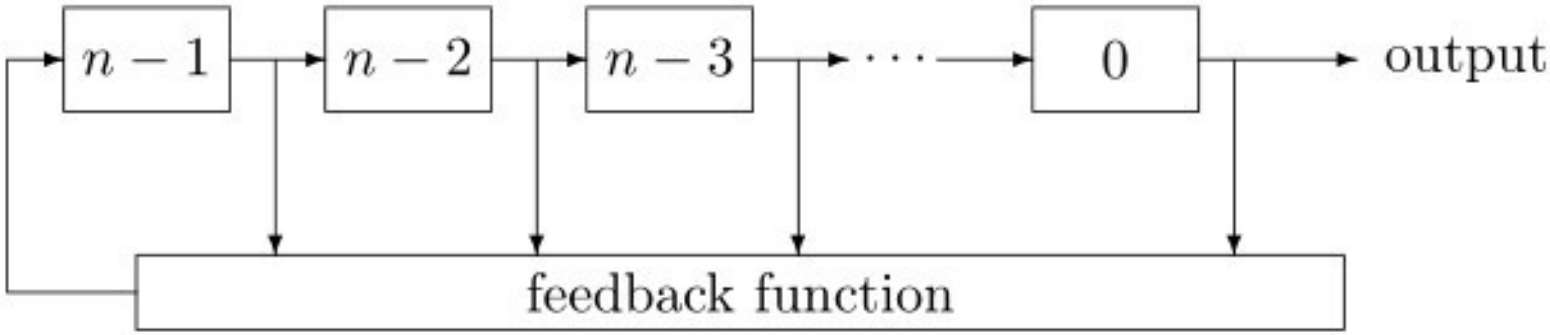
Selmer Center, University of Bergen

Sept. 3rd, 2014 - Rosendal

Outline

Feedback Shift Registers (FSRs)

- A diagram of an n-stage *feedback shift register (FSR)*.



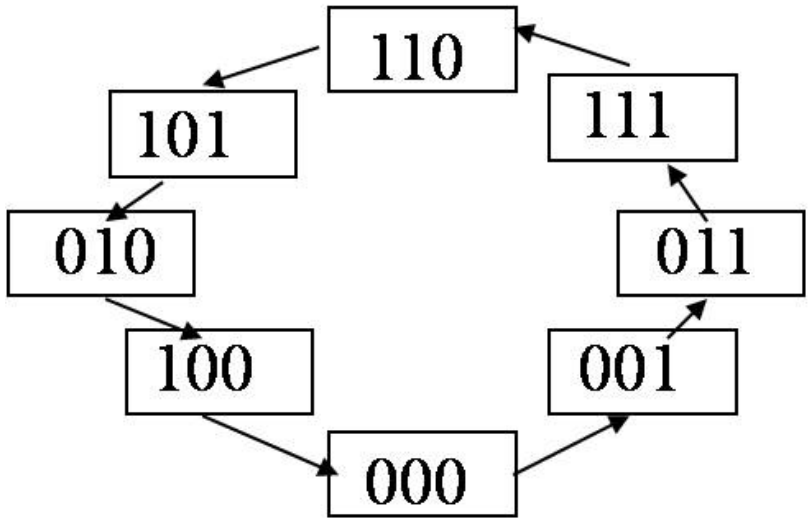
- an initial state $\mathbf{S}_0 = (s_0, s_1, \cdots, s_{n-1})$
- a feedback function: $f(x_0, x_1, \cdots, x_{n-1})$
- FSR sequecnes: for initial states $\mathbf{S}_0 = (s_0, s_1, \cdots, s_{n-1})$, a FSR generates sequences $\mathbf{s} = \{s_i\}$ via the recursion

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

A toy example

Let $f_1(x_0, x_1, x_2) = 1 + x_0 + x_1 + x_1x_2$.

i	(x_i, x_{i+1}, x_{i+2})	x_{i+3}
0	000	1
1	001	1
2	011	1
3	111	0
4	110	1
5	101	0
6	010	0
7	100	0



LFSRs and m-sequences

- **LFSRs** - the function $f(x_0, \cdots, x_{n-1}) = \sum_{i=0}^{n-1} c_i x_i$ is *linear*;
- **Period** - By associating $f(x_0, \cdots, x_{n-1})$ with a polynomial

$$f'(x) = 1 + \sum_{i=1}^{n} c_i x^i,$$

  we can characterize the periods of the sequences $\{s_i\}$ via that of the *feedback polynomial* $f'(x)$
- m**-sequences** - The LFSR sequences have the maximum length $2^n - 1$, called m**-sequences**, if $f'(x)$ is a primitive polynomial.
- **Properties of** m**-sequences**:
  - Long period.
  - Excellent pseudorandom distribution.

LFSR-based stream ciphers

- m-sequences are favored in stream ciphers due to the good randomness properties;
- However, they are not cryptographically secure due to the well-known Berlekamp-Massey algorithm.
- LFSRs have been combined in a controlled and nonlinear way to provide enough security.
- **Nevertheless**, the LFSR-based stream ciphers are still threatened by some attacks, e.g. algebraic attacks.

Nonlinear Feedback Shift Registers (NLFSRs)

NLFSRs - the feedback function $f(x_0, \cdots, x_{n-1})$ is *nonlinear*

+ The number of n-stage LFSRs is of order 2^n, while the number is 2^{2^n} for n-stage NLFSRs
+ NLFSR-based stream ciphers have been increasingly popular. For instance, the eSTREAM project hardware-oriented finalists like Trivium and Grain.

- The theory of NLFSRs is much more challenging and far less developed
- Determining the period and distribution of 0's and 1's in an NLFSR sequence is very hard
- Even constructing NLFSR sequences with maximum length 2^n is a difficult problem

Nonlinear Feedback Shift Registers (NLFSRs)

NLFSRs - the feedback function $f(x_0, \cdots, x_{n-1})$ is *nonlinear*

+ The number of n-stage LFSRs is of order 2^n, while the number is 2^{2^n} for n-stage NLFSRs
+ NLFSR-based stream ciphers have been increasingly popular. For instance, the eSTREAM project hardware-oriented finalists like Trivium and Grain.

- The theory of NLFSRs is much more challenging and far less developed
- Determining the period and distribution of 0's and 1's in an NLFSR sequence is very hard
- Even constructing NLFSR sequences with maximum length 2^n is a difficult problem

The topic of this talk

An n-stage NLFSR is called a **maximum-length NLFSR** if all its output sequences have maximum period 2^n, which are **binary deBrujin sequences** of order n.

The main talk is mainly concerned with the **construction of maximum-length NLFSRs** from a class of LFSRs.

The topic of this talk

An n-stage NLFSR is called a **maximum-length NLFSR** if all its output sequences have maximum period 2^n, which are **binary deBrujin sequences** of order n.

The main talk is mainly concerned with the **construction of maximum-length NLFSRs** from a class of LFSRs.

Preliminaries

The **state graph** $G(f)$ of an n-stage FSR with feedback func. f:

- a directed graph of 2^n vertices
- 2^n states $\mathbf{S} = (s_0, s_1, \cdots, s_{n-1}) \in \mathbb{F}_2^n$ as vertices
- directed edges: $(s_0, s_1, \cdots, s_{n-1}) \to (s_1, \cdots, s_{n-1}, s_n)$ with

$$s_n = f(s_0, s_1, \cdots, s_{n-1}),$$

- $G(f)$ consists of many cycles $C = (\mathbf{S}_0\, \mathbf{S}_1\, \cdots\, \mathbf{S}_{k-1})$:

$$\mathbf{S}_0 \to \mathbf{S}_1 \to \mathbf{S}_2 \to \cdots \to \mathbf{S}_{k-1} \to \mathbf{S}_0$$

- The cycles in $G(f)$ are disjoint **iff** f is *nonsingular*, i.e.,

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

- The **cycle structure** of $G(f)$:

$$G(f) = \{C_0, C_1, C_2, \cdots, C_{r-1}\}.$$

Preliminaries

- The *conjugate* $\widehat{\mathbf{S}}$ and *complementary* $\overline{\mathbf{S}}$ of $\mathbf{S} = (s_0, s_1, \cdots, s_{n-1})$:

$$\widehat{\mathbf{S}} = (\bar{s}_0, s_1, \cdots, s_{n-1}), \quad \overline{\mathbf{S}} = (\bar{s}_0, \bar{s}_1, \cdots, \bar{s}_{n-1}),$$

  where $\bar{s}_i = s_i \oplus 1$. $\mathbf{S}$ and $\widehat{\mathbf{S}}$ form *a conjugate pair*.
- The *complementary* cycle $\overline{C}$ of a cycle C is similarly defined.
- Two cycles C_1 and C_2 are *adjacent* if
  - C_1 and C_2 are state disjoint
  - there exists a conjugate pair $\{\mathbf{S}, \widehat{\mathbf{S}}\}$ such that

    the state $\mathbf{S}$ is on C_1, and its conjugate $\widehat{\mathbf{S}}$ is on C_2

Representations of Cycles

An (n,k)-*cycle* $(\mathbf{S}_0\,\mathbf{S}_1\,\cdots\,\mathbf{S}_{k-1})$ with $\mathbf{S}_i = (s_i, s_{i+1}, \cdots, s_{i+n-1})$ can be simply represented by a periodic sequence

$$[\mathbf{s}] = [s_0, s_1, \cdots, s_{k-1}].$$

Let $G(x) = \sum_{i=0}^{\infty} s_i x^i$ be the *generating function* of a sequence $\mathbf{s} = (s_0, s_1, s_2, \cdots)$. If the sequence $\mathbf{s}$ has period k, then

$$G(x) = \sum_{i=0}^{\infty} s_i x^i = \frac{s_0 + s_1 x + \cdots + s_{k-1} x^{k-1}}{1 + x^k}$$

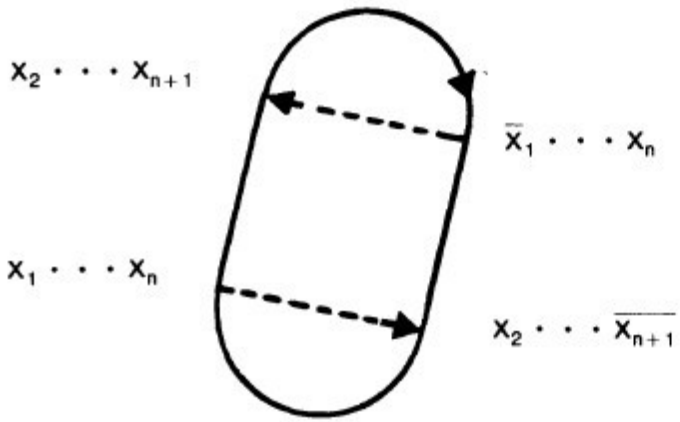
Representations of an (n,k) cylce:

- $(\mathbf{S}_0\,\mathbf{S}_1\,\cdots\,\mathbf{S}_{k-1})$
- a periodic sequence $[\mathbf{s}] = [s_0, s_1, \cdots, s_{k-1}]$
- a generating function $G(x) = \frac{s_0 + s_1 x + \cdots + s_{k-1} x^{k-1}}{1 + x^k}$

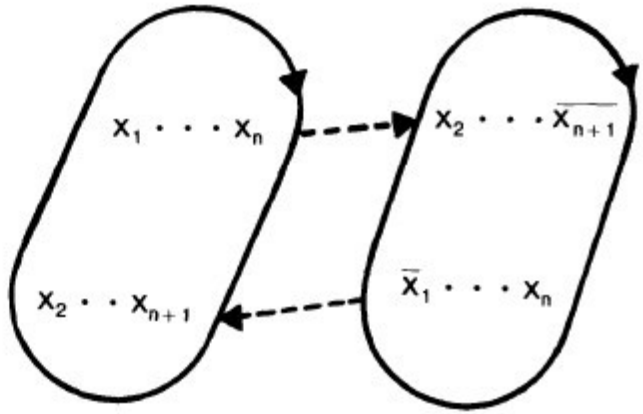
Cycle joining method

Lemma 1

- Two adjacent cycles C_1 and C_2, with $\mathbf{X}$ on C_1 and $\widehat{\mathbf{X}}$ on C_2, are **joined into a single cycle** when the successors of $\mathbf{X}$ and $\widehat{\mathbf{X}}$ are interchanged;
- A cycle C is **split into two adjacent cycles** when the successors of $\mathbf{X}$ and $\widehat{\mathbf{X}}$ on C are interchanged.



One cycle splitting into two.



Two cycles joining into one.

Cycle joining method

Given an FSR with feeback function f, the state graph $G(f)$ might consist of many cycles with small length.

By iteratively applying the **cycle joining** method, one is able to join “small" cycles into a maximum-length cycle **provided that** he knows

- whether two cycles in $G(f)$ are adjacent; and
- how to determine the conjugate pairs shared by every two adjacent cycles

Adjacency graph

Adjacency graph

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

Example: $n = 3$ and $f(x_0, x_1, x_2) = x_0 + x_2$

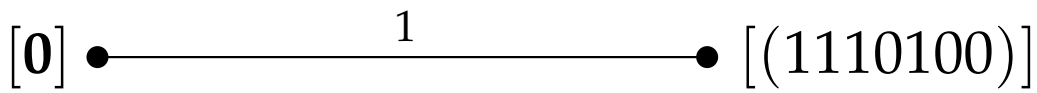


Fig. 1. The adjacency graph

Basic idea

Question: How can we get maximum-length NLFSRs?

An answer: for an FSR with feedback func. $f(x_0, x_1, \cdots, x_{n-1})$,

- **Step 1**: investigate the cycle structure of the state graph
- **Step 2**: determine the adjacent graph
- **Step 3**: find conjugate pairs shared by some adjacent cycles
- **Step 4**: iteratively apply the cycle-joining method and end up with a maximum-length cycle

The number of the constructed NLFSRs can be obtained by the well-known BEST theorem

The first two steps are quite challenging for NLFSRs!

Basic idea

Question: How can we get maximum-length NLFSRs?

An answer: for an FSR with feedback func. $f(x_0, x_1, \cdots, x_{n-1})$,

- **Step 1**: investigate the cycle structure of the state graph
- **Step 2**: determine the adjacent graph
- **Step 3**: find conjugate pairs shared by some adjacent cycles
- **Step 4**: iteratively apply the cycle-joining method and end up with a maximum-length cycle

The number of the constructed NLFSRs can be obtained by the well-known BEST theorem

The first two steps are quite challenging for NLFSRs!

Basic idea

Question: How can we get maximum-length NLFSRs?

An answer: for an FSR with feedback func. $f(x_0, x_1, \cdots, x_{n-1})$,

- **Step 1**: investigate the cycle structure of the state graph
- **Step 2**: determine the adjacent graph
- **Step 3**: find conjugate pairs shared by some adjacent cycles
- **Step 4**: iteratively apply the cycle-joining method and end up with a maximum-length cycle

The number of the constructed NLFSRs can be obtained by the well-known BEST theorem

The first two steps are quite challenging for NLFSRs!

Construction of max-length NLFSRs

A good starting point: LFSRs

Let $p(x)$ be a primitive polynomial in $\mathbb{F}_2[x]$ of degree n.

- **Trivial Cases:** LFSRs with feedback poly. $p(x)$
- **Sophisticated Cases:**
  - LFSRs with feedback poly. $(1+x)p(x)$ [Mykkelveit et al]
  - LFSRs with feedback poly. $(1+x)^2p(x)$ [Hemmati et al]
- **Our work:** denote by $\mathcal{L}_m$ the set of LFSRs with feedback poly. $q_m(x) = (1+x)^m p(x)$, we
  - investigate the cycle structure of LFSRs in $\mathcal{L}_m$ for $m \geq 3$
  - determine the adjacency graph of LFSRs in $\mathcal{L}_3$
  - construct maximum-length NLFSRs from LFSRs in $\mathcal{L}_3$

Construction of max-length NLFSRs

A good starting point: LFSRs

Let $p(x)$ be a primitive polynomial in $\mathbb{F}_2[x]$ of degree n.

- **Trivial Cases:** LFSRs with feedback poly. $p(x)$
- **Sophisticated Cases:**
  - LFSRs with feedback poly. $(1+x)p(x)$ [Mykkelveit et al]
  - LFSRs with feedback poly. $(1+x)^2p(x)$ [Hemmati et al]
- **Our work:** denote by $\mathcal{L}_m$ the set of LFSRs with feedback poly. $q_m(x) = (1+x)^m p(x)$, we
  - investigate the cycle structure of LFSRs in $\mathcal{L}_m$ for $m \geq 3$
  - determine the adjacency graph of LFSRs in $\mathcal{L}_3$
  - construct maximum-length NLFSRs from LFSRs in $\mathcal{L}_3$

D-morphism

D-morphism: a homomorphism from $\mathbb{F}_2^n$ to $\mathbb{F}_2^{n-1}$ defined by

$$(s_0, s_1, \cdots, s_{n-1}) \xrightarrow{D} (s_0 + s_1, s_1 + s_2, \cdots, s_{n-2} + s_{n-1}).$$

- D-morphism is a 2-to-1 mapping, namely, $D(\mathbf{S}) = D(\overline{\mathbf{S}})$
- each element $(s_0, \cdots, s_{n-2})$ in $\mathbb{F}_2^{n-1}$ has two preimages in $\mathbb{F}_2^n$ under D:

$$(s_0, s_1, \cdots, s_{n-2}) \xrightarrow{D_0^{-1}} (0, s_0, s_0 + s_1, \cdots, \sum_{i=0}^{n-2} s_i)$$

$$(s_0, s_1, \cdots, s_{n-2}) \xrightarrow{D_1^{-1}} (1, 1 + s_0, 1 + s_0 + s_1, \cdots, 1 + \sum_{i=0}^{n-2} s_i)$$

Pre-images of cycles under D-morphism

The D-morphism can also be defined over cycles. Lempel characterized the preimages of (n,k) cycles in $G(f)$.
Let $C = [s_0, s_1, \cdots, s_{k-1}]$ be an (n,k)-cycle in G_f.
(i) For even $wt(C)$ and $t = 0, 1$,

$$D_t^{-1}(C) = \left[t, t+s_0, t+s_0+s_1, \cdots, t+\sum_{i=0}^{k-2} s_i \right]$$

two complementary $(n+1,k)$-cycles.
(ii) For odd $wt(C)$,

$$D_0^{-1}(C) = D_1^{-1}(C)$$
$$= \left[0, s_0, s_0+s_1, \cdots, \sum_{i=0}^{k-2} s_i, 1, 1+s_0, 1+s_0+s_1, \cdots, 1+\sum_{i=0}^{k-2} s_i \right]$$

Pre-images of cycles under D-morphism

Neat Version - Generating functions

Let $C = [s_0, s_1, \cdots, s_{k-1}]$ be an (n,k)-cycle in G_n with generating function $F(x)$.

(i) For even $wt(C)$, $D_0^{-1}(C) = \frac{F(x)}{1+x}$ and $D_1^{-1}(C) = \frac{F(x)}{1+x} + \frac{1}{1+x}$ are two complementary $(n+1,k)$-cycles

(ii) For odd $wt(C)$, $D^{-1}(C) = \frac{F(x)}{1+x}$ is a self-complementary $(n+1,2k)$- cycle.

Two observations

Pre-image of the state graph:

For a state graph $G(f) = \{C_0, C_1, \cdots, C_{r-1}\}$, define

$$D^{-1}(G(f)) = \{D_t^{-1}(C) \,|\, C \in G(f), t = 0, 1\}$$

Fact 1

For a nonsingular n-stage LFSR with feedback poly. $f'_n(x)$, then there exists a unique nonsingular $(n+1)$-stage LFSR with feedback poly. $f'_{n+1}(x) = (x+1)f'_n(x)$ such that

$$G(f'_{n+1}) = D^{-1}(G(f'_n))$$

Two Observations

Pre-imgage of ajacent cycles

Fact 2

Given an n-stage LFSR with feedback poly. f, let C be an (n,k) cycle in $G(f)$ and $\mathbf{S}$ be a state on C.

- Each of the two cycles $D_0^{-1}(C)$ and $D_1^{-1}(C)$ contains exactly one of the two states $D_0^{-1}(\mathbf{S})$ and $D_1^{-1}(\mathbf{S})$;
- If the conjugate $\widehat{\mathbf{S}}$ is on C', then $\{D_0^{-1}(\mathbf{S}), D_1^{-1}(\widehat{\mathbf{S}})\}$ and $\{D_1^{-1}(\mathbf{S}), D_0^{-1}(\widehat{\mathbf{S}})\}$ are two conjugate pairs between the sets $\{D_0^{-1}(C), D_1^{-1}(C)\}$ and $\{D_0^{-1}(C'), D_1^{-1}(C')\}$

Main Approach

- By Fact 1, if the cycle structure of $G(f'_n)$ is known, then the cycle structure of $G((1+x)f'_n)$ is determined **as long as one can determine the parity of weight of each cycle in** $G(f'_n)$;
- Furthermore, by Fact 2, if adjacency graph for $G(f'_n)$ is known, one might be able to determine the adjacency graph for $G((1+x)f'_n)$ under certain conditions;
- Facts 1 and 2 can be **iteratively applied** for investigating $G((1+x)^m f'_n)$ for $m \geq 1$.

Main Approach

- By Fact 1, if the cycle structure of $G(f'_n)$ is known, then the cycle structure of $G((1+x)f'_n)$ is determined **as long as one can determine the parity of weight of each cycle in** $G(f'_n)$;
- Furthermore, by Fact 2, if adjacency graph for $G(f'_n)$ is known, one might be able to determine the adjacency graph for $G((1+x)f'_n)$ under certain conditions;
- Facts 1 and 2 can be **iteratively applied** for investigating $G((1+x)^m f'_n)$ for $m \geq 1$.

Main Approach

- By Fact 1, if the cycle structure of $G(f'_n)$ is known, then the cycle structure of $G((1+x)f'_n)$ is determined **as long as one can determine the parity of weight of each cycle in** $G(f'_n)$;
- Furthermore, by Fact 2, if adjacency graph for $G(f'_n)$ is known, one might be able to determine the adjacency graph for $G((1+x)f'_n)$ under certain conditions;
- Facts 1 and 2 can be **iteratively applied** for investigating $G((1+x)^m f'_n)$ for $m \geq 1$.

The set $\mathcal{L}_m$

Denote by $\mathcal{L}_m$ the set of all LFSRs with feedback polynomials of the form

$$q_m(x) = (1+x)^m p(x),$$

where m is a nonnegative integer.

We write $G(q_m(x))$ for the set of all cycles in the state graph of a given LFSR in $\mathcal{L}_m$.

For simplicity, in the case of $m = 0$, we choose $\frac{1}{p(x)}$ as the generating function to represent the unique $(n, 2^n - 1)$ cycle in $G(q_0(x))$, i.e., $G(q_0(x)) = \{0, \frac{1}{p(x)}\}$

Cycle structure of $G(q_m(x))$

Algorithm

Given a LFSR with feedback polynomial $q_m(x) = (1+x)^m p(x)$. Then $G(q_m(x))$ is obtained as follows.

Step 1: Set $q_0(x) = p(x)$, and we have $G(q_0(x)) = \left\{0, \frac{1}{p(x)}\right\}$.

Step 2: (Recursive Step) Set $q_i(x) = (1+x)q_{i-1}(x)$, where $1 \leq i \leq m$. All cycles in $G(q_i(x))$ are obtained by applying $D_t^{-1}(t \in \{0,1\})$ to each cycle in $G(q_{i-1}(x))$.

Cycle structure of $G(q_m(x))$

Proposition 1

The cycles in $G(q_k(x))$ for $k \geq 0$ have the following properties:

- $G(q_k(x))$ contains two cycles 0 and $\frac{1}{p(x)}$ for $k \geq 0$;
- for $k \geq 1$, other cycles except for 0 and $\frac{1}{p(x)}$ can be written as $\frac{f(x)}{(1+x)^l p(x)}$ or $\frac{g(x)}{(1+x)^l}$, where l is a positive integer, $\gcd(f(x), (1+x)^l p(x)) = 1$ and $\gcd\left(g(x), (1+x)^l\right) = 1$;
- a cycle in (ii) is of odd weight **iff** $l = 2^v$ for some $v \geq 0$.

The cycle structure of $G(q_m(x))$ can be determined for any integer $m \geq 0$.

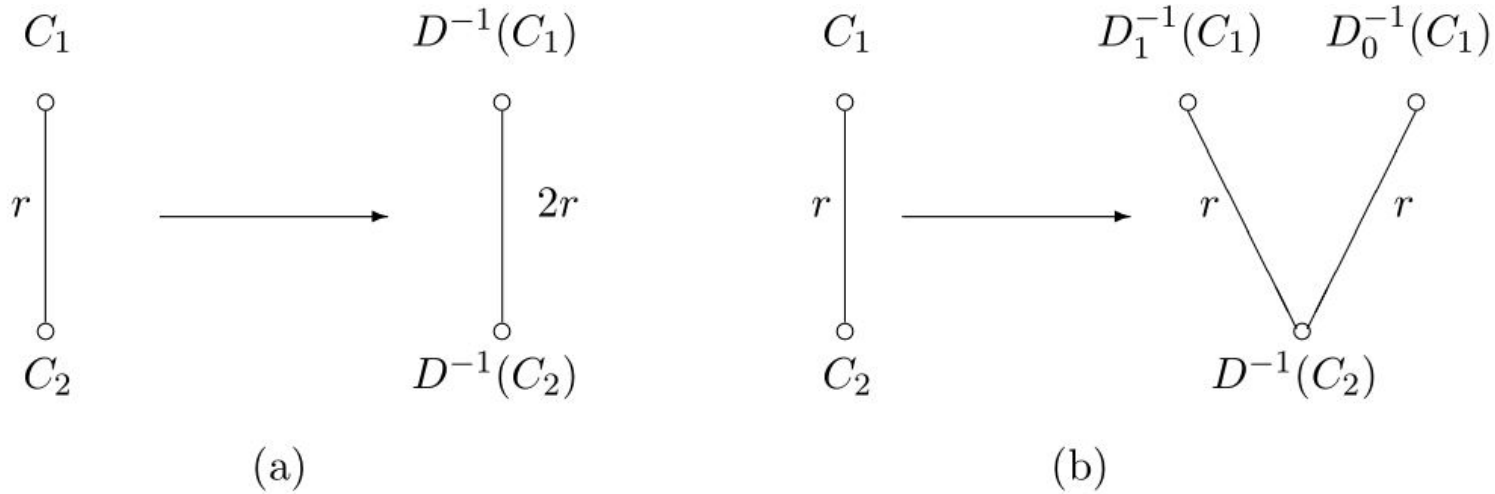
Adjacency graphs

Given the cycle structure of $G(q_m(x))$, our next task is to determine the adjacency graph.

For this purpose, the following result will be iteratively used:

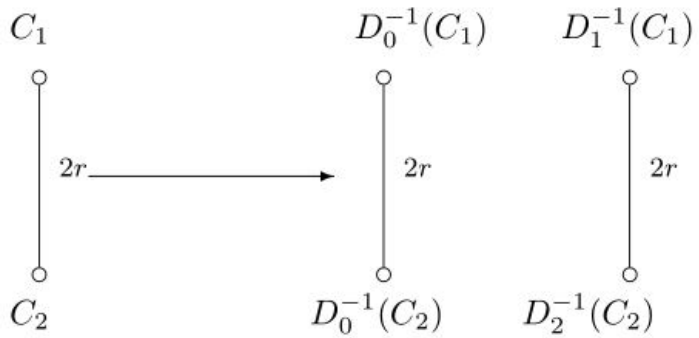
Fact 3

Let C_1 and C_2 be two adjacent cycles in $G(q_k(x))$ sharing exactly r conjugate pairs. (i) If both $wt(C_1)$ and $wt(C_2)$ are odd, see (a); (ii) If $\{wt(C_1)$ is odd and $wt(C_2)\}$ is even, see (b)

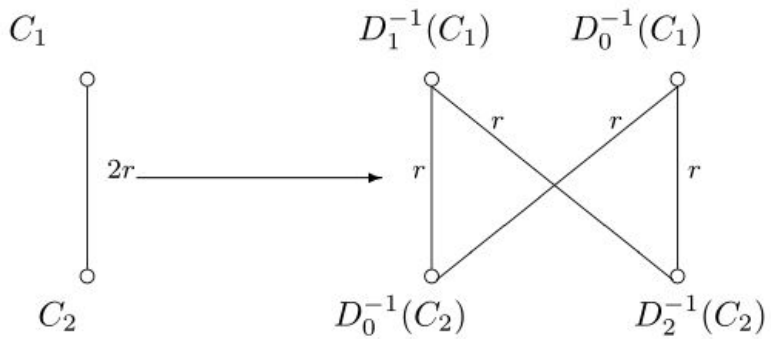


Adjacency graphs

Nevertheless, when both $wt(C_1)$ and $wt(C_2)$ are even, it is **unclear** about the exact number of conjugate pairs between the preimages of them.



(a)



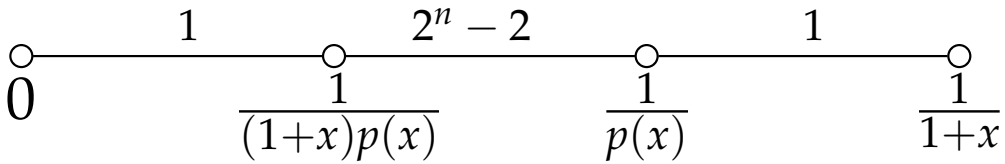
(b)

Adjacency graphs

Previous Results:

The adjacency graph of $q_1(x)$

The adjacency graph of any one LFSR in $\mathcal{L}_1$ is given as below.



J. Mykkeltveit, M. K. Siu and P. Tong, "On the cycle structure of some nonlinear shift register sequences," *Inf. Contr.*, vol. 43, pp. 202-215, 1979.

Adjacency graphs

Theorem 1

The adjacency graph of an LFSR in $\mathcal{L}_2$ is given in Fig. 1(a) and that of an LFSR in $\mathcal{L}_3$ is given in Fig. 1(b).

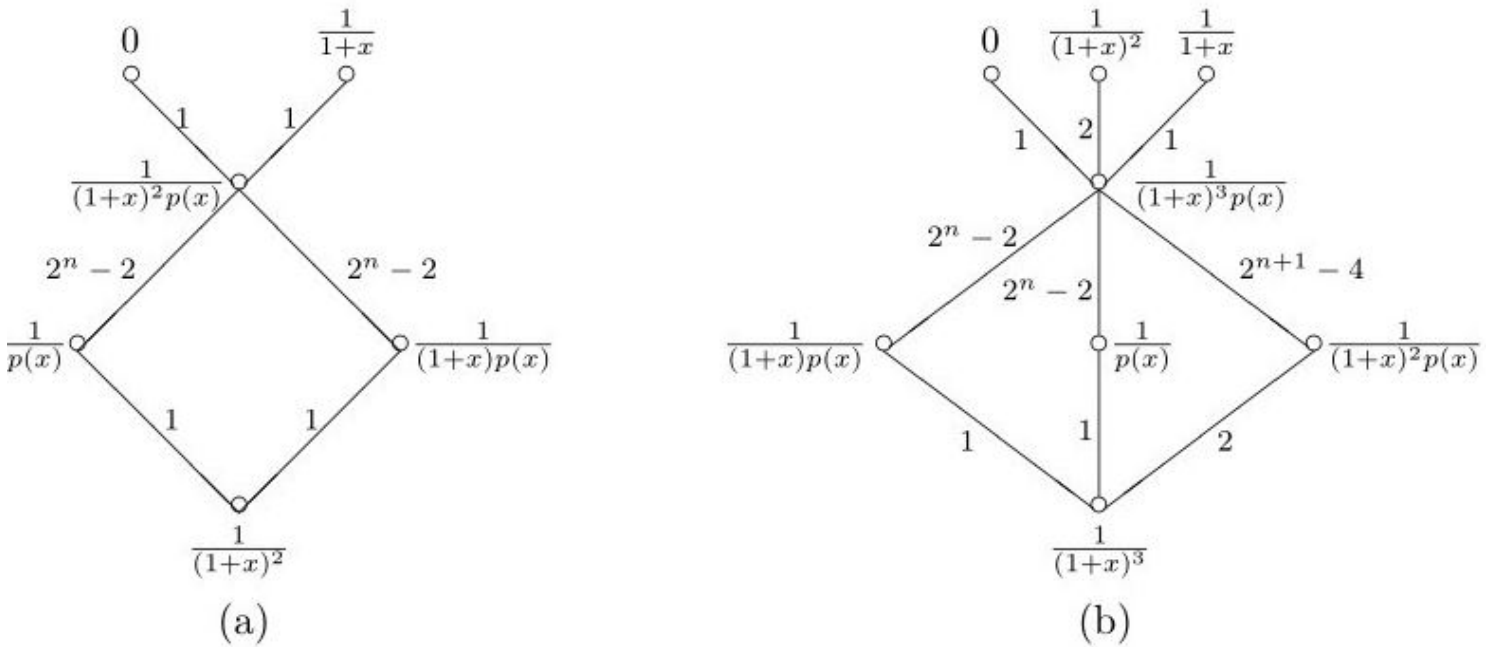


Fig. 1. (a) The adjacency graph of $q_2(x)$. (b) The adjacency graph of $q_3(x)$.

Fig. 1 (a) was also determined by a different method in F. Hemmati, "A large class of nonlinear shift register sequences," *IEEE Trans. Inf. Theory*, vol. 28, pp. 355-359, 1982.

Proof of Theorem 1 (sketch)

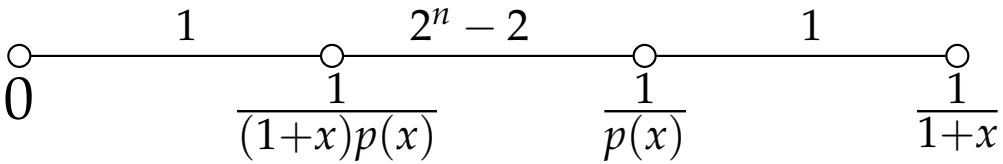
- The main idea is to deduce the adjacency graph of $G(q_{i+1}(x))$ from that of $G(q_i(x))$ by applying the D-morphism.
- To our end, the number of conjugate pairs shared by the preimages of two adjacent cycles in $G(q_i(x))$ is considered.
- If any one of the two adjacent cycles is of odd weight, then the number of conjugate pairs shared by the preimages of the two cycles can be determined. Therefore, we obtain the adjacency graphs of LFSRs in $\mathcal{L}_2$ and $\mathcal{L}_3$.

Proof of Theorem 1 (sketch)

The state graph $G(q_1(x)) = \{0, \frac{1}{(1+x)p(x)}, \frac{1}{p(x)}, \frac{1}{1+x}\}$ satisfies

cycles	0	$\frac{1}{(1+x)p(x)}$	$\frac{1}{p(x)}$	$\frac{1}{1+x}$
weight	even	odd	even	odd
$D_t^{-1}(\cdot)$	$0, \frac{1}{1+x}$	$\frac{1}{(1+x)^2p(x)}$	$\frac{1}{(1+x)p(x)}, \frac{1}{p(x)}$	$\frac{1}{(1+x)^2}$

With the adjacent graph of $G(q_1(x))$:



Then the adjacency graph of $G(q_2(x))$ is determined since

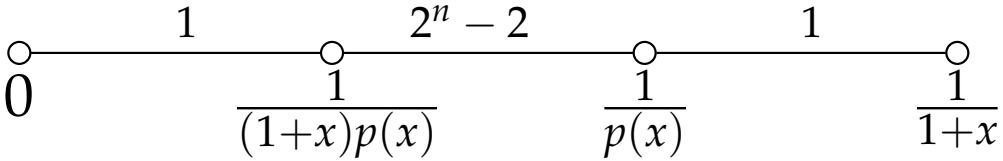
- $\frac{1}{(1+x)^2p(x)}$ shares 1 conjugate pair with 0 and $\frac{1}{1+x}$ resp.;
- $\frac{1}{(1+x)^2p(x)}$ shares $2^n - 2$ pairs with $\frac{1}{(1+x)p(x)}$ and $\frac{1}{p(x)}$ resp.;
- $\frac{1}{(1+x)^2}$ shares 1 conjugate pairs with $\frac{1}{(1+x)^2}$ and $\frac{1}{p(x)}$ resp.;

Proof of Theorem 1 (sketch)

The state graph $G(q_1(x)) = \{0, \frac{1}{(1+x)p(x)}, \frac{1}{p(x)}, \frac{1}{1+x}\}$ satisfies

cycles	0	$\frac{1}{(1+x)p(x)}$	$\frac{1}{p(x)}$	$\frac{1}{1+x}$
weight	even	odd	even	odd
$D_t^{-1}(\cdot)$	$0, \frac{1}{1+x}$	$\frac{1}{(1+x)^2p(x)}$	$\frac{1}{(1+x)p(x)}, \frac{1}{p(x)}$	$\frac{1}{(1+x)^2}$

With the adjacent graph of $G(q_1(x))$:



Then the adjacency graph of $G(q_2(x))$ is determined since

- $\frac{1}{(1+x)^2p(x)}$ shares 1 conjugate pair with 0 and $\frac{1}{1+x}$ resp.;
- $\frac{1}{(1+x)^2p(x)}$ shares $2^n - 2$ pairs with $\frac{1}{(1+x)p(x)}$ and $\frac{1}{p(x)}$ resp.;
- $\frac{1}{(1+x)^2}$ shares 1 conjugate pairs with $\frac{1}{(1+x)^2}$ and $\frac{1}{p(x)}$ resp.;

Adjacency graph for $G(q_m(x))$ with $m \geq 4$

However, we cannot determine the adjacency graph of $G(q_4(x))$ in this way.

The reason is that for **two adjacent cycles** C_1 **and** C_2 **of even weight** in $G(q_3(x))$, it is not clear about the number of conjugate pairs between $\{D_0^{-1}(C_1), D_1^{-1}(C_1)\}$ and $\{D_0^{-1}(C_2), D_1^{-1}(C_2)\}$.

Open Problem:
For any two adjacent cycles of even weight in $G(q_i(x))$ with $i \geq 3$, determine the number of conjugate pairs shared by their preimages in $G(q_{i+1}(x))$.

Construction of max-length NLFSRs

Fact 4

Let $f(x_0, x_1, \cdots, x_{n-1})$ be the feedback function of a nonsingular n-stage FSR and let

$$h(x_0, x_1, \cdots, x_{n-1}) = f(x_0, x_1, \cdots, x_{n-1}) + x_1^{a_1} x_2^{a_2} \cdots x_{n-1}^{a_{n-1}},$$

where $x_i^{a_i} = x_i + a_i + 1$. Then,

- h and f differ only at the conjugate pair $\mathbf{A} = (a_0, a_1, \cdots, a_{n-1})$ and $\widehat{\mathbf{A}} = (\overline{a}_0, a_1, \cdots, a_{n-1})$;
- $G(h)$ and $G(f)$ can be obtained from each other by interchanging the successors of $\mathbf{A}$ and $\widehat{\mathbf{A}}$.

S. W. Golomb, *Shift Register Sequences*, San Francisco, CA: Holden-Day, 1967.

Construction of deBruijn sequences

Let $\mathcal{T}$ be a spanning tree of the adjacency graph for $G(q_m(x))$, $m = 0, 1, 2, 3$. Denote by $E(\mathcal{T})$ the set of labels $(a_1, a_2, \cdots, a_{n+2})$ of all the edges in $\mathcal{T}$.

Theorem 2

Let $f(x_0, \cdots, x_{n+2})$ be the feedback function of an LFSR in $\mathcal{L}_m$, $m = 0, 1, 2, 3$, and

$$g(x_0, \cdots, x_{n+2}) = f(x_0, \cdots, x_{n+2}) + \sum_{(a_1, \cdots, a_{n+2}) \in E(\mathcal{T})} x_1^{a_1} x_2^{a_2} \cdots x_{n+2}^{a_{n+2}}.$$

Then the NLFSR with feedback func. $g(x_0, \cdots, x_{n+2})$ generates de Bruijn sequences.

The number of the constructed NLFSRs is equal to that of the spanning trees.

An example

- Take a primitive polynomial $p(x) = x^3 + x + 1 \in \mathbb{F}_2[x]$. Then the feedback function of corresponding LFSR in $\mathcal{L}_3$ is $f(x_0, x_1, x_2, x_3, x_4, x_5) = x_0 + x_1 + x_3$.
- We can choose the set $E(\mathcal{T})$ consisting of

$$
\begin{array}{ll}
(0,0,0,0,0), & (1,1,1,1,1) \\
(1,0,1,0,1), & (0,1,1,0,0) \\
(0,0,1,1,1), & (1,1,0,0,0) \\
(0,1,0,0,0) &
\end{array}
$$

An example

Consequently, we get the function

$$
\begin{aligned}
& g(x_0, x_1, x_2, x_3, x_4, x_5) \\
=& x_0 + x_1 + x_3 + \sum_{(a_1, a_2, \cdots, a_5) \in E(\mathcal{T})} x_1^{a_1} x_2^{a_2} \cdots x_5^{a_5} \\
=& 1 + x_0 + x_4 + x_5 + x_1x_2 + x_1x_3 + x_1x_4 + x_1x_5 \\
& + x_2x_3 + x_3x_4 + x_3x_5 + x_4x_5 + x_1x_2x_4 + x_1x_2x_5 \\
& + x_1x_3x_4 + x_1x_4x_5 + x_2x_3x_4 + x_2x_3x_5 + x_1x_2x_3x_5 \\
& + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_1x_2x_3x_4x_5.
\end{aligned}
$$

With the initial state $(0, 0, 0, 0, 0, 0)$, we get a de Bruijn sequence of period $2^6 = 64$:

$$
\begin{aligned}
& 0000001001010000110111001000111 \dashrightarrow \\
& \dashrightarrow 0100111111011010101110010110011
\end{aligned}
$$

Thanks for your attention!