The Transform between the Galois NLFSR and Fibonacci NLFSR

***Abstract*—In this brief, the Galois nonlinear feedback shift register (NLFSR) and Fibonacci NLFSR are regarded as two boolean network, and semi-tensor product of matrices is used to convert these two NLFSR into two equivalent algebraic equation. Based on this, a novel way proposed to investigate the transform between the Galois NLFSR and Fibonacci NLFSR.First, the property of uniform NLFSR has been investigate. Second, two bijection Φ,Ψ between uniform Galois NLFSR and Fibonacci NLFSR obtained. Third, two algorithms are provided to achieve the transform between the Galois NLFSR and Fibonacci NLFSR. Compared with other method, the method provided in this paper is easier to achieve.**

I. INTRODUCTION

Pseudo-random sequence as a signal form with good correlation properties are extensively used in many application, such as secure communication, BER instrumentation, delay measurement and noise and spread Spectrum Communication generator. The linear feedback shift registers (LFSRs) is the one of most popular configuration for generating pseudo-random sequencesThe feedback shift registers (FSRs) are

II. PRELIMINARIES

Definition 1: Let$A \in \mathbb{R}^{n\times m}$, $B \in \mathbb{R}^{p\times q}$. The $semi-tensorproduct$ of A and B is

$$A \ltimes B = (A \otimes I_{\frac{l}{m}})(B \otimes I_{\frac{l}{p}}) \tag{1}$$

where l is the least common multiple of m and p.

Lemma 1: Any boolean function $f(x_1,x_2,...,x_n)$with variables $x_1,x_2,...,x_n \in \Delta_2$ can beexpressed as a multi-linear form:

$$f(x_1,x_2,...,x_n) = Fx_1x_2...x_n. \tag{2}$$

where F is called the $structurematrix$ of f, and is uniquely expressed as

$$F = \left[\begin{array}{cccc} s_1 & s_2 & \dots & s_{2^n} \\ 1-s_1 & 1-s_2 & \dots & 1-s_{2^n} \end{array} \right] \tag{3}$$

with $[s_1,s_2,...,s_{2^n}]$ being the truth table of f, arranged in the reverse alphabet order.

An $NLFSR$ consists of n binary memory devices, which is called bits.

An Galois configuration of $NLFSR$ can be described by a system of n nonlinear equations:

$$\begin{cases} x_0(t+1) = f_0(x_0(t),x_1(t),...,x_{n-1}(t)), \\ x_1(t+1) = f_1(x_0(t),x_1(t),...,x_{n-1}(t)), \\ \vdots \\ x_{n-2}(t+1) = f_{n-2}(x_0(t),x_1(t),...,x_{n-1}(t)), \\ x_{n-1}(t+1) = f_{n-1}(x_0(t),x_1(t),...,x_{n-1}(t)). \end{cases} \tag{4}$$

where $f_i, i \in 0,1,2...,n-1$ is boolean function.

An Fibonacci configuration of NLFSR can be described as following equation:

$$\begin{cases} x_0(t+1) = x_1(t), \\ x_1(t+1) = x_2(t), \\ \vdots \\ x_{n-2}(t+1) = x_{n-1}(t), \\ x_{n-1}(t+1) = f(x_0(t),x_1(t),...,x_{n-1}(t)). \end{cases} \tag{5}$$

The Fibonacci $NLFSR$ has an algebraic representation

$$x(t+1) = L_F x(t), t \in N, \tag{6}$$

where $x \in \Delta_{2^n}$ is the state, $L_F \in L_{2^n\times 2^n}$ is the state transition matrix, satisfying

$$L = \delta_{2^n} \left[\begin{array}{cccccc} q_1 & \dots & q_{2^{n-1}} & q_{2^{n-1}+1} & \dots & q_{2^n} \end{array} \right] \tag{7}$$

with

$$q_i = 2i - \zeta_i \tag{8}$$

$$q_{2^{n-1}+i} = 2i - \zeta_{2^{n-1}+i} \tag{9}$$

for all $i = 1,2,...,2^{n-1}$.

The set $F_{2^n\times 2^n}$ denote all the $2^n \times 2^n$ logic matrix satisfying condition (**??**),(**??**) and (9).

Definition 2: An n-bit $NLFSR$ is $uniform$ if for some $0 \leq \tau < n$:

- $f_i(x) = x_{i+1}$ for $0 \leq i < \tau$,
- $f_i(x) = x_{(i+1)modn} \oplus g_i(x_0,...,x_\tau)$ for $\tau \leq n$ where g_i is a nonzero Boolean function.,..

Definition 3: Let $(x_0(t),x_1(t),...,x_{n-1}(t))$ denote the $state$ of $NLFSR$ at time t, where $x_0(t),x_1(t),...,x_{n-1}(t) \in \{0,1\}$.

Remark 1: For arbitrary Fibonacci $NLFSR$ is uniform. In this paper, only uniform $NLFSR$ is concerned.

Definition 4: the $state\ transition\ graph$ of $NLFSR$ is a directed graph N:

- the vertex set $V(N)$ is the set $\{(i_0,i_1,...,i_{n-1}) \sim \delta_{2^n}^i | i_0,i_1,...,i_{n-1} \in \{0,1\}\}$.
- the directed edge set $E(N)$ is define as follows: there is an directed edge from $v_i \sim \delta_{2^n}^i$ to $v_j \sim \delta_{2^n}^j$, if and only if $L\delta_{2^n}^i = \delta_{2^n}^j$, v_i is called a *predecessor* of v_j, while v_j is called a *succesor* of v_i.

For the fibonacci $NLFSR$, the state which has two *predecessor* is called a $branch\ state$. For all $NLFSR$, the state without *predecessor* is called $starting\ state$.

Example 1: Given a 3-bit $NLFSR$ N_1 with the following equation:

$$\begin{cases} x_0(t+1) = x_1(t) \oplus x_0(t), \\ x_1(t+1) = x_2(t), \\ x_2(t+1) = x_2(t) \oplus x_1(t). \end{cases} \tag{10}$$

The state transition graph of N_1 show in Fig.**??**.

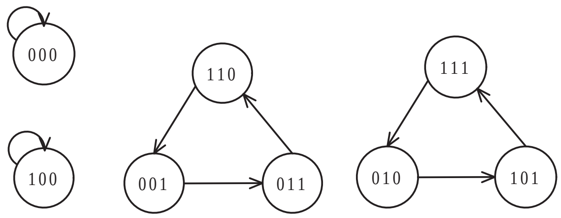

Fig. 1: State transition graph of N_1

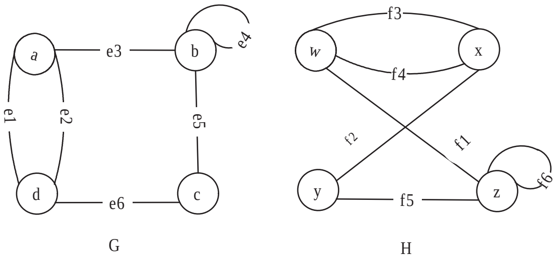

Fig. 2: Isomorphic graphs

Definition 5: Two graphs G and H are *isomorphic*, written $G \cong H$, if there are bijection θ: $V(G) \to V(H)$ and ϕ: $E(G) \to E(H)$ such that $\psi_G(e) = uv$ if and only if $\psi_H(\phi(e)) = \theta(u)\theta(v)$.

Example 2: In the Fig.**??**, graph G and graph H are isomorphic, the mapping θ and ϕ define by

$$\theta := \begin{pmatrix} a & b & c & d \\ w & z & y & x \end{pmatrix} \phi := \begin{pmatrix} e_1 & e_2 & e_3 & e_4 & e_5 & e_6 \\ f_3 & f_4 & f_1 & f_6 & f_5 & f_2 \end{pmatrix}$$

Definition 6: Let S_0 denote the set of state$\{(0, x_1, x_2, ..., x_{n-1}) | x_1, x_2, ..., x_{n-1} \in \{0,1\}\}$, and S_1 denote the set of states$\{(1, x_1, x_2, ..., x_{n-1}) | x_1, x_2, ..., x_{n-1} \in \{0,1\}\}$.

Definition 7: Two *NLFSRs* are *equivalent* if their sets of output sequences are equal, and their *state transition graphs* are *isomorphic*.

Definition 8: The

III. Main results

Theorem 1: Given a NLFSR N_1, the structure matrix of N_1 is L_1, there exist another different matrix L_2 of NLFSR N_2, such that the state transition graph of N_2 and N_1 are *isomorphic*, the output sequences of N_2 are same as N_1's.

Proof: First, we need construct a bijection $\Phi : \triangle_{2^n} \to \triangle_{2^n}$, which is the one-to-one correspondence from states of (N_1) to N_2's. The constructing method named *CM* as following:
Initialization Set $i := 0$, set $Re := \triangle_{2^n}$, state transition graph of (N_2) is $ST_2 := (V, E), V = \emptyset, E = \emptyset$.
Recursive step Set $i = i + 1$, $(i_0, i_1, ... i_{n-1}) \sim \delta_{2^n}^i \in \triangle_{2^n}$ of (N_1).
if $i_0 = 0$, then one can set $(0, j_1, ... j_{n-1}) \sim \delta_{2^n}^j \in Re$.
else one can set$(0, j_1, ... j_{n-1}) \sim \delta_{2^n}^j \in Re$.
Do $V = V \cup \delta_{2^n}^j$, and set $\Phi(\delta_{2^n}^i) = \delta_{2^n}^j$, $Re = \triangle_{2^n} \delta_{2^n}^j$.
$E = \{\Phi(u)\Phi(v) | u, v \in V(N_1), uv = e \in E(N_1)\}$, and the matrix L_2 has property following:
$\{col_i(L_2) = \delta_{2^n}^j | u = \delta_{2^n}^i \sim (i_0, i_1, ..., i_{n-1}), v = \delta_{2^n}^j \sim (j_0, j_1, ..., j_{n-1}), \Phi^{-1}(u)\Phi^{-1}(v) \in E(N_1)\}$.
From the process of construction of L_2, one find a matrix L_2 of N_2 such that N_2 is equivalent to N_1. ■

Corollary 1: If a *NLFSR* N_1 is equivalent to a *NLFSR* N_2 which is constructed, then the states in sets S_0 of these two *NLFSRs* is one-to-one, and the states in sets S_1 of these two *NLFSRs* is also one-to-one.

Proof: The proof followed by the process of *CM*. ■

Lemma 2: The number of branch states of a *NLFSR* is equal to the number of starting state.

Theorem 2: If a Galois *NLFSR GN* can be equivalent to a Fibonacci *NLFSR FN*, then for every states of *GN* has two predecessors at most, and there are at most two equilibrium states of *GN*. If the *GN* with two equilibrium states $\{e_1, e_2\}$, then $e_1 \in S_0$ and $e_2 \in S_1$.

Proof: From the lemma (**??**), the state transition graph of Fibonacci *NLFSR* and Galois *NLFSR* are *isomorphic*. Since for every states of Fibonacci *NLFSR* has two predecessors at most, Galois *NLFSR* must has the same property(i.e for every states of Galois *NLFSR* has two predecessors at most).
For the Fibonacci *NLFSR*, the equilibrium states only can be 000... or 111..., if the initial state is equilibrium state, the output sequence is 000... or 111.... By the definition of *equivalent*, the conclusion is obvious. ■

Corollary 2: If a Galois *NLFSR* is equivalent to a Fibonacci *NLFSR*, the base of $col(L_G)$ denote by $|col(L_G)|$, and $|col(L_G)| \geq 2^{n-1}$, there are at most two states $\{\delta_{2^n}^i, \delta_{2^n}^j\}$ such that $L_G \delta_{2^n}^i = \delta_{2^n}^i, L_G \delta_{2^n}^j = \delta_{2^n}^j$, and $i \in \{1, 2, ..., 2^{n-1}\}, j \in \{2^{n-1}+1, 2^{n-1}+2, ..., 2^n\}$.

Proof: If for every states $\delta_{2^n}^i \in col(L_G)$ of Galois *NLFSR* has two predecessors, then there are $\delta_{2^n}^{i_1}$ and $\delta_{2^n}^{i_2}$, such that:

$$L\delta_{2^n}^{i_1} = L\delta_{2^n}^{i_2} = \delta_{2^n}^i.$$

then $col_{i_1}(L_G)$ and $col_{i_2}(L_G)$ are equal to $\delta_{2^n}^i$, so $|col(L_G)| \geq 2^{n-1}$. ■

Theorem 3: Arbitrary Fibonacci *NLFSR FN* can transform to a *equivalent* Galois *NLFSR GN* by using *CM*.

Proof: The proof followed by theorem (**??**). ■

Theorem 4: A *uniform* Galois *NLFSR* can transform to a *equivalent* Fibonacci *NLFSR*, the nonlinear recurrence describing output sequence of these two *NLFSR* are same, and there is a bijection Φ between the initial states of equivalent *NLFSR*.

Theorem 5: Given a n-bit *uniform* Galois *NLFSR GN*, L_G is the *state transition matrix* of *GN*, there is a matrix $L_F \in F_{2^n \times 2^n}$ and a permutation matrix $M_\Phi = [M_{\Phi_1}, M_{\Phi_2}] \in L_{2^n \times 2^n}$, $col(M_{\Phi_1}) \in \{\delta_{2^n}^1, \delta_{2^n}^2, ..., \delta_{2^n}^{2^{n-1}}\}$, $col(M_{\Phi_2}) \in \{\delta_{2^n}^{2^{n-1}+1}, \delta_{2^n}^{2^{n-1}+2}, ..., \delta_{2^n}^{2^n}\}$) such that

$$L_G = M_\Phi^{-1} L_F M_\Phi. \tag{11}$$

Proof: From the theorem (**??**), the uniform Galois *NLFSR* can be equivalent to a Fibonacci *NLFSR*, and there is a bijection Φ between the states of the two *NLFSR*, so for arbitrary state $\delta_{2^n}^i$ of *GN*, satisfying

$$M_\Phi L_G \delta_{2^n}^i = L_F M_\Phi \delta_{2^n}^i. \tag{12}$$

where M_Φ is the structure matrix of bijection Φ, and M_Φ is a permutation matrix which is result of bijection's property. On the contrary, if $M_\Phi L_G \delta_{2^n}^i \neq L_F M_\Phi \delta_{2^n}^i$, ■

In this brief, an algorithm provided to transform a $uniform$ Galois to a *equivalent* Fibonacci $NLFSR$.
First, there are two array $G[2^n]$, $F[2^n]$ to storage the structure matrix of Galois $NLFSR$ and Fibonacci $NLFSR$ respectively. Suppose the the structure matrix of Galois $NLFSR$ is $L_G = \delta_{2^n}\begin{bmatrix} p_1 & p_2 & \ldots & p_{2^n} \end{bmatrix}$, array $G = \begin{bmatrix} p_1 & p_2 & \ldots & p_{2^n} \end{bmatrix}$. For every state $\delta_{2^n}^i$ as the initial state, it has a output sequence L_i, in this algorithm, the first 3 bits of L_i only needed, written as $(y_1, y_2, y_3) \sim \delta_{2^n}^{j_i}$. We provide a algorithm to calculate the transform function Φ.

Algorithm 1 Calculation of matrix L_F.

for $i = 1$ to 2^n **do**
  $\Phi(i) = j_i$
  $col_i(M_\Phi) = \delta_{2^n}^{j_i}$
end for
$M_\Phi^{-1} = M_\Phi^T$
$L_F = M_\Phi L_G M_\Phi^{-1}$

Remark 2: The algorithm [1] obtain the structure matrix of Φ M_Φ, and the M_Φ satisfy the condition in theorem (**??**).
The transform from a Fibonacci $NLFSR$ FN to a equivalent Galois $NLFSR$ GN can be achieved the inverse process of algorithm [1]. But the process is easier than the transform from a Galois $NLFSR$ to a equivalent Fibonacci $NLFSR$, one only needs construct a bijection Ψ from Galois $NLFSR$ to Fibonacci $NLFSR$, and the structure matrix of Ψ M_Ψ satisfying the condition in theorem (**??**), .

Algorithm 2 Calculation of matrix L_F.

$\Omega_1 = \{1, 2, ..., 2^{n-1}\}$,$\Omega_2 = \{2^{n-1}+1, 2^{n-1}+2, ..., 2^n\}$
for $i = 1$ to 2^{n-1} **do**
  $\Phi(i) = j_i \in \Omega_1$
  $\Omega_1 = \Omega_1 - j_i$
  $col_i(M_\Phi) = \delta_{2^n}^{j_i}$
end for
for $i = 2^{n-1}$ to 2^n **do**
  $\Phi(i) = j_i \in \Omega_2$
  $\Omega_2 = \Omega_2 - j_i$
  $col_i(M_\Phi) = \delta_{2^n}^{j_i}$
end for
$M_\Phi^{-1} = M_\Phi^T$
$L_G = M_\Phi L_F M_\Phi^{-1}$

IV. Example

V. Conclusion