A Unified Synchronization Criterion for Impulsive Dynamical Networks ⋆

Jianquan Lu [a,b], Daniel W.C. Ho [b], Jinde Cao [a]

[a] *Department of Mathematics, Southeast University, Nanjing 210096, China*

[b] *Department of Mathematics, City University of Hong Kong, Hong Kong, China*

Abstract

In this paper, Galois nonlinear feedback shift register (NLFSR) and Fibonacci NLFSR are regarded as two Boolean networks (BNs), and semi-tensor product (STP) of matrices is used to convert these two nonlinear feedback shift registers (NLFSRs) into two equivalent algebraic equations. Based on STP, a novel way is proposed to investigate the transformation between the Galois NLFSR and Fibonacci NLFSR. Firstly, we redefine the uniform NLFSR, and the properties of uniform NLFSR have been investigated. Secondly, two bijections between initial states of Galois NLFSR and Fibonacci NLFSR are obtained. Thirdly, two algorithms are provided to achieve the transformation between the Galois NLFSR and Fibonacci NLFSR. Compared with some existing methods, the method provided in this paper is easier to realize, and we extend the range of Galois NLFSR which can be transformed to a Fibonacci NLFSR. At last, two examples illustrate the results obtained in this paper.

Key words: Impulsive dynamical networks, Unified synchronization criterion, Average impulsive interval, Synchronizing impulses, Desynchronizing impulses.

1 Introduction

The information security is important for our society. The information encryption is essential. Pseudo-random sequences as signal form with good correlation properties have been widely used in many applications, such as secure communication, delay measurement and noise and spread spectrum communication generator. The linear feedback shift register (LFSR) is one of the most popular configurations for generating pseudo-random sequences **???**, where its current state is decided by a linear function of its previous states. In **?**, the author investigated the some properties about LFSR. The advantages of LFSR are fast, easy and simple to implement in hardware and software, and they can generate random sequences with same statistical distribution of 0's and 1's **?**. Nevertheless, they are not safe in stream cipher. Inspecting $2n$ consecutive bits of it's output sequence can deduce the structure of a n-bit LFSR **?**.

To solve this problem, nonlinear feedback shift register (NLFSR) was proposed in **?**, where its feedback functions are nonlinear Boolean functions. Due to the complicate structures of NLFSR, the output sequences of NLFSR are very difficult to deduce with cryptanalytic method, such as correlation attacks **?**. Many different designed methods of NLFSR-based stream ciphers have been proposed in **????**.

There exist two types of nonlinear feedback shift registers (NLFSRs): Galois NLFSR and Fibonacci NLFSR. The Galois NLFSR is shown in Fig. 1, which consists of a number of binary storage elements from left to right as $n-1, n-2, ..., 1, 0$, and each bit is updated by its own feedback function which relates to every bit. The value of the 0-th bit is the output of Galois NLFSR. There is a special kind of Galois NLFSR which has been proposed in **?**, named uniform Galois NLFSR as shown in Fig. 2. The i-th feedback function of uniform Galois NLFSR only relates to the i-th bit and the right bits of i-th bit. While for the Fibonacci NLFSR, as show in Fig. 3, only the $(n-1)$-th bit is updated by the feedback function. At each time, the value of the i-th bit is moved to the $(i-1)$-th bit in Fibonacci NLFSR. These two types of NLFSRs

⋆ This work was jointly supported by CityU 101109 (9041432), the National Natural Science Foundation of China under Grant 60874088, the Specialized Research Fund for the Doctoral Program of Higher Education under Grant 20070286003, and the Natural Science Foundation of Jiangsu Province of China under Grant BK2009271.

Email addresses: `jqluma@gmail.com;jqluma@seu.edu.cn` (Jianquan Lu), `madaniel@cityu.edu.hk` (Daniel W.C. Ho), `jdcao@seu.edu.cn` (Jinde Cao).

have their own disadvantages. The depth of the circuits implementing the Fibonacci NLFSR is larger than the depth of the circuits implementing the Galois NLFSR **?**. But for uniform Galois NLFSR, the period of the output sequence may not equal to the length of the longest cyclic sequence of its consecutive states. In **?**, Lin *et al.* proved that the uniform Galois NLFSR can be transformed to an equivalent Fibonacci NLFSR. In **?**, a method of the transformation from Fibonacci NLFSR to Galois NLFSR was provided. In **?**, Dubrova provided a method to find the matching initial states between Fibonacci NLFSR and its equivalent Galois NLFSR. For an arbitrary initial state of a NLFSR A, there is an initial state in equivalent NLFSR B which can deduce same output sequence, and the initial states of NLFSR A and NLFSR B are one-to-one mapping. Unfortunately the methods in **???** all need algebraic calculation, and the methods in **???** can not be realized through programming. For a given n-bit NLFSR with a big n, the methods in **???** are not applicable.

Lately, a new mathematical tool of matrix calculation named the semi-tensor product (STP) of matrices was proposed in **?**. This STP method has been used to study Boolean networks (BNs). In **?**, Lu *et al.* studied the controllability of delayed Boolean control networks (BCNs) based on the method of STP. By using STP, the pinning controllability problem, synchronization problem, stabilization problem, observability problem and output tracking control problem of BCNs have been investigated in **???????**. Based on the method of STP, the stability of BNs has been studied in **?**. The controllability problem of BNs was investigated in **??** by using the method of STP. In **?**, the method of STP was used to study the problems of game theory. The tool of STP has also been successfully applied to the Fibonacci NLFSR **???**. Up to now some interesting results about Fibonacci NLFSR have been obtained by using STP. In this paper, motivated by above discussions , the method of STP is used to study the transformation between Galois NLFSR and Fibonacci NLFSR.

In this paper, we investigate the transformation between Fibonacci NLFSR and Galois NLFSR by using STP. Firstly, the Fibonacci NLFSR and the Galois NLFSR are regarded as BNs. Then, we redefine the uniform NLFSR, and the properties of uniform NLFSR will be investigated. Secondly, two bijections Φ, Ψ between initial states of Galois NLFSR and Fibonacci NLFSRs are obtained. Thirdly, two algorithms are provided to achieve the transformation between the Galois NLFSR and Fibonacci NLFSR. At last, two examples are presented to illustrate the results obtained in this paper. The contribution of this paper:

- Compared with the results in **??**, the transformation between these two types of NLFSRs can be achieved by programming, and hence the methods provided in this paper is more convenient to realize and implement.
- The initial states matching between two types of NLFSRs can be easily obtained by computations.
- We expand the range of Galois NLFSR that can be transformed to Fibonacci NLFSR.

The remainder of this paper is organized as follows. Section 2 gives some preliminaries on STP, Galois NLFSR, Fibonacci NLFSR and the definition of isomorphic graph. In Section 3, we study the properties of uniform NLFSR, and present two algorithms to achieve the transformation between these two types of NLFSRs. In Section 4, two example are given to illustrate our theoretical results. At last, a conclusion is given.

2 Model description and some preliminaries

In this section, the STP of matrices is firstly reviewed. Then we obtain the algebraic expressions of Galois NLFSR and Fibonacci NLFSR. By using the STP, multilinear forms of Galois NLFSR and Fibonacci NLFSR are obtained. Finally, we revisit some related results about Fibonacci NLFSR and also some definitions about NLFSR here. We first give some notations used in this paper.

- $\mathcal{D} = \{0, 1\}$.
- I_n : the identity matrix of dimension n.
- $\delta_{2^n}^i$: the i-th column of identity matrix I_n.
- $\Delta_{2^n} = \{\delta_{2^n}^i | i = 1, 2, 3, ..., 2^n\}$.
- $\mathcal{L}_{n\times m}$: the set of $n \times m$ matrices, whose column belong to Δ_n. For a matrix $L \in (L)_{n\times m}$, and $L = [\delta_n^{i_1}\ \delta_n^{i_2}\ ...\ \delta_n^{i_m}]$, we write $L = \delta_{2^n}[i_1\ i_2\ ...\ i_m]$ for simplicity.
- $col_i(L)$: the i-th column of matrix L.
- $col(L)$: the set of all column of matrix L.
- $\mathbb{R}$: the set of all real number.
- $|S|$: the base of set S.

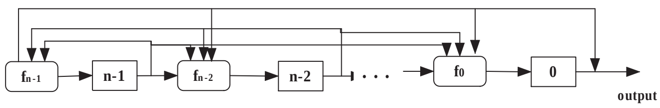

Fig. 1. The uniform Galois NLFSR

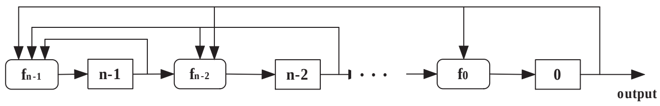

Fig. 2. The Galois NLFSR

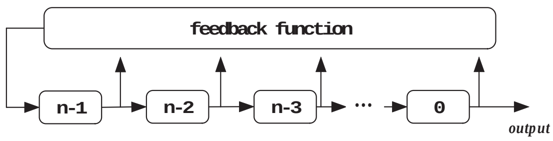

Fig. 3. The Fibonacci NLFSR

- N : the set of all integers.

2.1 Semi-Tensor Product of matrices

In this subsection, we give the definition of STP of matrices.

Definition 1 ? *Let $A \in \mathbb{R}^{n\times m}$, $B \in \mathbb{R}^{p\times q}$. The semi-tensor product of A and B is defined as:*

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

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

Obviously, if $m = p$ in Definition 1, then the STP of A and B is reduced to their conventional matrix product AB.

We identify $\Delta_2 \sim \mathcal{D}$ i.e ($\delta_2^1 \sim 1, \delta_2^2 \sim 0$), and $\delta_2^1(\delta_2^2)$ is called the vector form of logical value 1(0).

Lemma 1 ? *Any Boolean function $f(x_1, x_2, ..., x_n)$ with variables $x_1, x_2, ..., x_n \in \Delta_2$ can be expressed as a multi-linear form:*

$$f(x_1, x_2, ..., x_n) = Fx_1 \ltimes x_2 \ltimes ... \ltimes x_n. \tag{2}$$

where $F \in \mathcal{L}_{2\times 2^n}$ is called the structure matrix of f, and F can be uniquely expressed as

$$F = \begin{bmatrix} s_1 & s_2 & ... & s_{2^n} \\ 1-s_1 & 1-s_2 & ... & 1-s_{2^n} \end{bmatrix} \tag{3}$$

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

In the following, we omit the symbol $\ltimes$ for simplicity.

2.2 Galois NLFSR and Fibonacci NLFSR

An NLFSR consists of n binary memory devices, which is called bits. The output of a NLFSR is the value of the 0-th bit.
An n-bit Galois NLFSR can be described by a system of n nonlinear equations:

$$\begin{cases} y_0(t+1) = f_0(y_0(t), y_1(t), ..., y_{n-1}(t)), \\ y_1(t+1) = f_1(y_0(t), y_1(t), ..., y_{n-1}(t)), \\ \vdots \\ y_{n-1}(t+1) = f_{n-1}(y_0(t), y_1(t), ..., y_{n-1}(t)), \end{cases} \tag{4}$$

where $f_i : \mathcal{D}^n \to \mathcal{D}, i \in \{0, 1, 2..., n-1\}$ is logical function, and $y_i \in \mathcal{D}, i \in \{0, 1, 2, ..., n-1\}$. Let $(y_0(t), y_1(t), ..., y_{n-1}(t))$ denote the state of the Galois NLFSR at time t.

By means of STP and Lemma 1, the logical system (4) can be expressed in an algebraic form. Let $y(t) = y_0(t) \ltimes y_1(t) \ltimes ... \ltimes y_{n-1}(t)$, then we can express the system (4) as follows:

$$\begin{cases} y_0(t+1) = F_0 y(t), \\ y_1(t+1) = F_1 y(t), \\ \vdots \\ y_{n-1}(t+1) = F_{n-1} y(t). \end{cases} \tag{5}$$

where $F_0, F_1, ..., F_{n-1} \in \mathcal{L}_{2\times 2^n}$. Moreover, (5) can further be converted into the following form:

$$y(t+1) = L_G y(t) \tag{6}$$

where $L_G \in \mathcal{L}_{2^n \times 2^n}$. Equation (6) is called the algebraic representation of Galois NLFSR (4).

Lemma 2 ? *Let (6) be the algebraic representation of Galois NLFSR, and let F_i be the structure matrix of f_i, for $i = 0, 1, ..., n-1$. Then*

$$F_i = S_i L_G, i = 0, ..., n-1 \tag{7}$$

where $S_i = 1_{2^i} \otimes I_2 \otimes 1_{2^{n-i-1}}$ for each i.

An n-bit Fibonacci NLFSR can be described as follows:

$$\begin{cases} x_0(t+1) = x_1(t), \\ x_1(t+1) = x_2(t), \\ \vdots \\ x_{n-2}(t+1) = x_{n-1}(t), \\ x_{n-1}(t+1) = f(x_0(t), x_1(t), ..., x_{n-1}(t)). \end{cases} \tag{8}$$

where $x_i \in \mathcal{D}, i = 1, 2, ..., 2^n$, $f : \mathcal{D}^n \to \mathcal{D}$ is a logical function. Let $x(t) = x_0(t)x_1(t)...x_{n-1}(t)$ denote the state of Fibonacci NLFSR (8). We can convert system (8) into the following form:

$$x(t+1) = L_F x(t), \tag{9}$$

where $L_F \in \mathcal{L}_{2^n \times 2^n}$, $x(t) \in \Delta_{2^n}$. Clearly, the Fibonacci NLFSR is a special cases of Galois NLFSR.

Lemma 3 ? *Assume that the truth table of feedback function f in (8) is [ζ_1, ζ_2, ...,ζ_{2^n}], and the algebraic representation of Fibonacci NLFSR (8) is (9). Then L_F satisfies*

$$L_F = \delta_{2^n} \left[q_1 \; ... \; q_{2^{n-1}} \; q_{2^{n-1}+1} \; ... \; q_{2^n} \right] \tag{10}$$

where

$$q_i = 2i - \zeta_i, \tag{11}$$
$$q_{2^{n-1}+i} = 2i - \zeta_{2^{n-1}+i}, \tag{12}$$

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

Let $\mathcal{F}_{2^n \times 2^n}$ denote the set of all $2^n \times 2^n$ logic matrix satisfying conditions (10), (11) and (12).

Let $x_{n-1}(t+1) = x_0(t+n)$, $x_{n-1}(t) = x_0(t+n-1)$, $x_{n-2}(t) = x_0(t+n-2)$, $x_{n-3}(t) = x_0(t+n-3)$, ..., $x_1(t) = x_0(t+1)$, and substituting them into $x_{n-1}(t+1) = f(x_0(t), x_1(t), ..., x_{n-1}(t))$ in system (8), one can obtain

$$x_0(t+n) = f(x_0(t), x_0(t+1), ..., x_0(t+n-1)), \tag{13}$$

which is called *nonlinear recurrence* of order n describing the output sequences of Fibonacci NLFSR.

Definition 2 *An* n*-bit NLFSR is* $uniform$ *if the NLFSR has nonlinear recurrence of order* n *describing the output sequence.*

Remark 1 *An arbitrary Fibonacci NLFSR is uniform.*

Definition 3 *Consider a NLFSR* N *with directed state transition graph being* G_N*, and with its structure matrix being* L*. We define the state transition graph as follows:*

- *the vertex set* $V(G_N)$ *is the set* $\{(i_0, i_1, ..., i_{n-1}) \sim \delta_{2^n}^i | i_0, i_1, ..., i_{n-1} \in \mathcal{D}\}$.
- *the directed edge set* $E(G_N)$ *is defined as follows: there is a 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 a NLFSR, the state which has two *predecessors* is called a *branch state*. The state without *predecessor* is called *starting state*.

Definition 4 *A state* $x_0 \in \Delta_{2^n}$ *is called a equilibrium state of system (6) or (9), if* $L_G x_0 = x_0$ *or* $L_F x_0 = x_0$.

Example 1 *Given an 3-bit NLFSR* N_1 *with the following equation:*

$$\begin{cases} x_0(t+1) = x_1(t) \oplus x_0(t), \\ x_1(t+1) = x_2(t), \\ x_2(t+1) = x_2(t) \oplus x_1(t). \end{cases} \tag{14}$$

The state transition graph of NLFSR N_1 *is shown in Fig. 4.* 000 *and* 100 *are equilibrium states.*

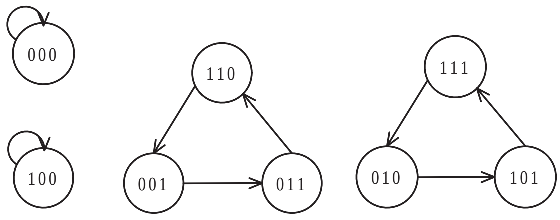

Fig. 4. State transition graph of N_1 in Example 1

For an arbitrary edge $e \in E(G)$, there are vertexes u and v, such that $\psi_G(e) = uv$.

Definition 5 *Two graphs* G *and* H *are isomorphic, written* $G \cong H$*, if there are bijections* 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 Fig. 5, the mapping* θ *and* ϕ *are defined by*

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

then $G \cong H$.

Definition 6 *Let* S_0 *denote the set of states* $\{(0, x_1, x_2, ..., x_{n-1}) | x_1,$ $\mathcal{D}\}$*, and let* S_1 *denote the set of states* $\{(1, x_1, x_2, ..., x_{n-1}) | x_1, x_2, ..., x$ $\mathcal{D}\}$.

Definition 7 *Two NLFSRs are equivalent if the sets of their output sequences are the same, and two equivalent NLFSRs are called absolutely equivalent if their state transition graphs are isomorphic.*

In the following, only the absolutely equivalence of NLFSR will be considered. In order to avoid ambiguity, an NLFSR is a arbitrary type of NLFSR without special declarations.

3 Unified synchronization criterion

In this section, some interesting properties of uniform NLFSR are firstly obtained. Then, two algorithms are

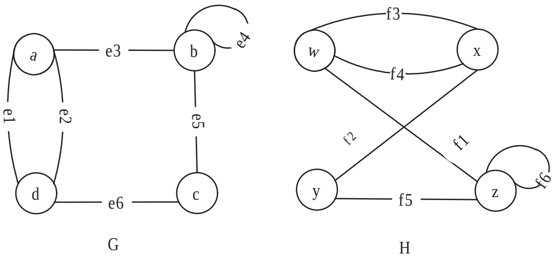

Fig. 5. Isomorphic graphs in Example 2

provided to achieve the transformation between Galois NLFSR and Fibonacci NLFSR.

Property 1 ? *Given an n-bit uniform NLFSR N_1. If the nonlinear recurrence of order n describing the output sequence of N_1 is*

$$x_0(t+n) = f(x_0(t), x_0(t+1), ..., x_0(t+n-1)).(15)$$

One can replace $x_0(t+i)$ with $x_i(t)$, $(0 \leq i \leq n-1)$ in (15), then we can obtain

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

which is a Fibonacci NLFSR.

Lemma 4 ? *If two n-bit NLFSRs have same nonlinear recurrence of order n, then these two n-bit NLFSRs are equivalent to each other.*

Lemma 5 ? *If two n-bit NLFSRs (NLFSR N_1 and NLFSR N_2) have same nonlinear recurrence of order n, then there exists a bijection Φ between the initial states of NLFSR N_1 and NLFSR N_2, such that the initial states $\delta_{2^n}^i$ in N_1 and $\Phi(\delta_{2^n}^i)$ in N_2 have same output sequence.*

Theorem 1 *If two n-bit uniform NLFSRs (NLFSR N_1 and NLFSR N_2) have same nonlinear recurrence of order n, then these two n-bit NLFSRs are absolutely equivalent.*

Proof. From Lemma 4, we can know that these two n-bit NLFSRs are equivalent. Hence, in the following, we only need to prove that the state transition graphs of these two NLFSRs are isomorphic.

From Lemma 5, one can conclude that there is a bijection Φ between these initial states of two NLFSRs, such that the initial states $\delta_{2^n}^i$ in NLFSR N_1 and $\Phi(\delta_{2^n}^i)$ in NLFSR N_2 have the same output sequence. Now, we only need to prove that

$$\Phi(L_1\delta_{2^n}^i) = L_2\Phi(\delta_{2^n}^i),$$

where L_1 and L_2 are structure matrices of NLFSR N_1 and NLFSR N_2 respectively.

Let $l_i = i_1, i_2, i_3, ...$ denote the output sequence of initial state $\delta_{2^n}^i$.

- For NLFSR N_1, if $L_1\delta_{2^n}^i = \delta_{2^n}^j$, then l_j is the subsequence of l_i and $i_2 = j_1, i_3 = j_2, ...$ If $\Phi(\delta_{2^n}^i) = \delta_{2^n}^p$, then $\delta_{2^n}^p$ is initial state of NLFSR N_2, then one can obtain that l_i is equal to l_p (i.e. $i_1 = p_1, i_2 = p_2, ...$).
- For NLFSR N_2, if $L_2\Phi(\delta_{2^n}^i) = L_2\delta_{2^n}^p = \delta_{2^n}^q$, then l_q is the sub-sequence of l_p, and $p_2 = q_1, p_3 = q_2, ...$
- Hence, we can conclude that output sequence l_j is equal to l_q, which means that $\Phi\delta_{2^n}^j = \delta_{2^n}^q$ (i.e. $\Phi(L_1\delta_{2^n}^i) = L_2\Phi(\delta_{2^n}^i)$). So the state transition graphs of NLFSR N_1 and NLFSR N_2 are isomorphic.

□

From Property 1, Lemma 5 and Theorem 1, we can derive the following Corollary.

Corollary 1 *A uniform Galois NLFSR can be transformed to an absolutely equivalent Fibonacci NLFSR.*

Lemma 6 ? *The number of branch states of a Fibonacci NLFSR is equal to the number of starting states.*

From definition of uniform NLFSR and Corollary 1, we can derive following properties of uniform NLFSR.

Property 2 *The number of branch states of an uniform NLFSR is equal to the number of starting states.*

Property 3 *Every state of an uniform NLFSR has at most two predecessors, and $|col(L_G)| \geq 2^{n-1}$.*

Proof. If every state $\delta_{2^n}^i \in col(L_G)$ in uniform 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 both equal to $\delta_{2^n}^i$. Hence, we have $|col(L_G)| \geq 2^{n-1}$. □

Property 4 *For an arbitrary uniform NLFSR N_1, there are at most two equilibrium states of NLFSR N_1. If the NLFSR N_1 has two equilibrium states e_1, e_2, then $e_1 \in S_0$ and $e_2 \in S_1$.*

Proof. From Theorem 1 and Corollary 1, N_1 can be transformed to an absolutely equivalent Fibonacci NLFSR N_2. Hence the state transition graph $G_{N_1} \cong G_{N_2}$, and the set of output sequences of NLFSR N_1 and NLFSR N_2 are equal. Since every state of NLFSR N_2 has two predecessors at most, NLFSR N_1 must have the same property (i.e. for every state of NLFSR N_1 has at most two predecessors).

For NLFSR N_2, the equilibrium states can only be 000... or 111.... The output sequences of initial states 000... and 111... are 000... and 111... respectively. Considering the fact that the output sequences of equilibrium states of two absolutely NLFSRs are equal, we can conclude that if NLFSR N_1 have two equilibrium states e_1, e_2, then $e_1 \in S_0$ and $e_2 \in S_1$. □

Theorem 2 *Given an n-bit NLFSR N_1 with its structure matrix being L_1. Then there exists another different*

n-bit Galois NLFSR N_2 with structure matrix being L_2, such that NLFSR N_1 and NLFSR N_2 are absolutely equivalent.

Proof. First, we need to construct a bijection $\Phi : \Delta_{2^n} \to \Delta_{2^n}$, which is a one-to-one mapping from states of NLFSR N_1 to that of NLFSR N_2.

The constructing method of the bijection Φ named CM is given as follows:

- ***Initialization*** Set $i := 0$, set $Re := \Delta_{2^n}$, state transition graph of N_2 is $G_{N_2} := (V, E), V = \emptyset, E = \emptyset$.
- ***Recursive step*** Set $i = i + 1$, $\delta_{2^n}^i \sim (i_0, i_1, ... i_{n-1})$ 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 $(1, j_1, ... j_{n-1}) \sim \delta_{2^n}^j \in Re$.
  Do $V = V \cup \delta_{2^n}^j$, and set $\Phi(\delta_{2^n}^i) = \delta_{2^n}^j$, $Re = Re \setminus \delta_{2^n}^j$.
  $E = \{\Phi(u)\Phi(v) | u, v \in V(G_{N_1}), uv = e \in E(G_{N_1})\}$, and the matrix L_2 satisfies the following property:
  $\{col_i(L_2) = \delta_{2^n}^j | u = \delta_{2^n}^i \sim (i_0, i_1, ..., i_{n-1}), v = \delta_{2^n}^j \sim (j_0, j_1, ..., j_{n-1}), \Phi^{-1}(u)\Phi^{-1}(v) \in E(G_{N_1})\}$.

From the process of CM, we can easily conclude that NLFSR N_2 and NLFSR N_1 are absolutely equivalent. □

From the process of constructing method CM, one can also derive the following result.

Corollary 2 *If an arbitrary type of NLFSR N_1 is equivalent to a Galois NLFSR N_2 which is constructed by CM, then the states in sets S_0 of NLFSR N_1 and NLFSR N_2 are one-to-one mapping, and further the states in sets S_1 of NLFSR N_1 and NLFSR N_2 are also one-to-one mapping.*

Theorem 3 *Given an arbitrary n-bit uniform Galois NLFSR GN with its state transition matrix being L_G, there exist a matrix $L_F \in \mathcal{F}_{2^n \times 2^n}$ and a permutation matrix $M_\Phi = [M_{\Phi_1}, M_{\Phi_2}] \in \mathcal{L}_{2^n \times 2^n}$, $M_{\Phi_1} \in \mathcal{L}_{2^n \times 2^{n-1}}$, $M_{\Phi_2} \in \mathcal{L}_{2^n \times 2^{n-1}}$, $col(M_{\Phi_1}) \subseteq \{\delta_{2^n}^1, \delta_{2^n}^2, ..., \delta_{2^n}^{2^{n-1}}\}$, $col(M_{\Phi_2}) \subseteq \{\delta_{2^n}^{2^{n-1}+1}, \delta_{2^n}^{2^{n-1}+2}, ..., \delta_{2^n}^{2^n}\}$) such that*

$$L_G = M_\Phi^{-1} L_F M_\Phi. \tag{16}$$

Proof. From Theorem 1 and Corollary 1, the NLFSR GN is absolutely equivalent to a Fibonacci NLFSR FN with structure matrix being L_F. Then there exists a bijection Φ between the initial states of NLFSR GN and NLFSR FN. Hence, for any state $\delta_{2^n}^i$ of NLFSR GN, we have

$$M_\Phi L_G \delta_{2^n}^i = L_F M_\Phi \delta_{2^n}^i, \tag{17}$$

where M_Φ is the structure matrix of bijection Φ, and M_Φ is a permutation matrix. To ensure that the output sequences of $\delta_{2^n}^i$ and $M_\Phi \delta_{2^n}^i$ are equal, we need the implementation of that $\delta_{2^n}^i \sim (0, i_1, ... i_{n-1})$, which implies that $M_\Phi \delta_{2^n}^i = \delta_{2^n}^j \sim (0, i_1, ... i_{n-1})$. Hence $col(M_{\Phi_1}) \subseteq \{\delta_{2^n}^1, \delta_{2^n}^2, ..., \delta_{2^n}^{2^{n-1}}\}$, $col(M_{\Phi_2}) \subseteq \{\delta_{2^n}^{2^{n-1}+1}, \delta_{2^n}^{2^{n-1}+2}, ..., \delta_{2^n}^{2^n}\}$).

On the contrary, if $M_\Phi L_G \delta_{2^n}^i \neq L_F M_\Phi \delta_{2^n}^i$, we know that the output sequences of initial state $M_\Phi L_G \delta_{2^n}^i$ in NLFSR GN and initial state $L_F M_\Phi \delta_{2^n}^i$ in NLFSR FN are not equal, which contradicts with Theorem 1. Hence, proof of Theorem 3 is completed. □ Following Theorem 2 and Theorem 3, we can derive the following theorem to describe the relationship between structure matrices of Fibonacci NLFSR and Galois NLFSR.

Theorem 4 *An arbitrary Fibonacci NLFSR FN can be transformed to an absolutely equivalent Galois NLFSR GN by using CM, and the structure matrix M_Ψ of bijection Ψ between the initial states in NLFSR FN and NLFSR GN satisfies that $M_\Psi = [M_{\Psi_1}, M_{\Psi_2}]$, $M_{\Psi_1} \in \mathcal{L}_{2^n \times 2^{n-1}}$, $M_{\Psi_2} \in \mathcal{L}_{2^n \times 2^{n-1}}$, $col(M_{\Psi_1}) \subseteq \{\delta_{2^n}^1, \delta_{2^n}^2, ..., \delta_{2^n}^{2^{n-1}}\}$, $col(M_{\Psi_2}) \subseteq \{\delta_{2^n}^{2^{n-1}+1}, \delta_{2^n}^{2^{n-1}+2}, ..., \delta_{2^n}^{2^n}\}$). The structure matrices L_F of NLFSR GN and L_G of NLFSR FN satisfy*

$$L_F = M_\Psi^{-1} L_G M_\Psi. \tag{18}$$

In the following, we provide an algorithm to achieve the transformation from a uniform Galois NLFSR to an absolutely equivalent Fibonacci NLFSR. Suppose that the structure matrix of Galois NLFSR is $L_G = \delta_{2^n}[p_1 \; p_2 \; ... \; p_{2^n}]$. For any initial state $\delta_{2^n}^i$, it has an output sequence l_i. In this algorithm, the first n bits of l_i are written as $(y_1, y_2, ..., y_n) \sim \delta_{2^n}^{j_i}$. Now we provide an algorithm to calculate the structure matrix M_Φ of transform function Φ and the structure matrix of NLFSR N_2. In following algorithm, at first, we judge whether the Galois NLFSR is a uniform Galois NLFSR. If the Galois NLFSR is a uniform Galois NLFSR, the Galois NLFSR can be transformed into an absolutely equivalent Fibonacci NLFSR. Otherwise the algorithm is ended.

Remark 2 *According to Algorithm 1, one can obtain the structure matrix M_Φ, and $M_\Phi = [M_{\Phi_1} \; M_{\Phi_2}] \in \mathrm{L}_{2^n \times 2^n}$, $M_{\Phi_1} \in \mathrm{L}_{2^n \times 2^{n-1}}$, $M_{\Phi_2} \in \mathrm{L}_{2^n \times 2^{n-1}}$, $col(M_{\Phi_1}) \subseteq \{\delta_{2^n}^1, \delta_{2^n}^2, ..., \delta_{2^n}^{2^{n-1}}\}$, $col(M_{\Phi_2}) \subseteq \{\delta_{2^n}^{2^{n-1}+1}, \delta_{2^n}^{2^{n-1}+2}, ..., \delta_{2^n}^{2^n}\}$.*

The transformation from a Fibonacci NLFSR to an absolutely equivalent Galois NLFSR can be achieved according to the following Algorithm 2. In the transformation from a Fibonacci NLFSR to an equivalent Galois

Algorithm 1. Calculation of matrix L_F.
[1] initial set $\Delta = \{1, 2, ..., 2^n\}$ $i = 1$ to 2^n $j_i \in \Delta$ $\Phi(i) = j_i$ $col_i(M_\Phi) = \delta_{2^n}^{j_i}$ $\Delta \setminus j_i$ the algorithm is ended.
$M_\Phi^{-1} = M_\Phi^T$ $L_F = M_\Phi L_G M_\Phi^{-1}$

NLFSR, one only need to construct a bijection Ψ from Galois NLFSR to Fibonacci NLFSR. The structure matrix of bijection Ψ is denoted by M_Ψ. For every initial state $\delta_{2^n}^i$ in Fibonacci NLFSR, if $\delta_{2^n}^i \in S_0$ ($\delta_{2^n}^i \in S_1$), then we can choose an $\delta_{2^n}^{j_i} \in S_0$ ($\delta_{2^n}^{j_i} \in S_1$), such that $\Psi(\delta_{2^n}^i) = \delta_{2^n}^{j_i} \in S_0$ ($\Psi(\delta_{2^n}^i) = \delta_{2^n}^{j_i} \in S_1$). The algorithm is presented as follows.

4 EXAMPLES

In this section, we give two examples to illustrate the effectiveness of the algorithms and our theoretical results obtained in this paper.

Example 3 *Consider an 4-bit Galois NLFSR with following equation:*

$$\begin{cases} x_0(t+1) = x_1(t) \oplus x_0(t), \\ x_1(t+1) = x_2(t), \\ x_2(t+1) = x_3(t), \\ x_3(t+1) = x_0(t) \oplus x_2(t)x_3(t)). \end{cases} \tag{19}$$

By simple computations, we can obtain its structure matrix L_G:

$$L_G = \delta_{16}[10\ 11\ 13\ 15\ 2\ 3\ 5\ 7\ 1\ 4\ 6\ 8\ 9\ 12\ 14\ 16].$$

Also we can easily obtain the state transition graph as shown in Fig. 6 By using Algorithm 1, we can obtain the bijection Φ and the structure matrix of Φ as follows.

$$M_\Phi = \delta_{16}[6\ 5\ 7\ 8\ 3\ 4\ 2\ 1\ 11\ 12\ 10\ 9\ 14\ 13\ 15\ 16]$$

Algorithm 2. Calculation of matrix L_F.
[2] $\Omega_1 = \{1, 2, ..., 2^{n-1}\}$,$\Omega_2 = \{2^{n-1}+1, 2^{n-1}+2, ..., 2^n\}$ $i = 1$ to 2^{n-1} $\Psi(i) = j_i \in \Omega_1$ $\Omega_1 = \Omega_1 \setminus j_i$ $col_i(M_\Psi) = \delta_{2^n}^{j_i}$ $i = 2^{n-1}$ to 2^n $\Psi(i) = j_i \in \Omega_2$ $\Omega_2 = \Omega_2 \setminus j_i$ $col_i(M_\Psi) = \delta_{2^n}^{j_i}$ $M_\Psi^{-1} = M_\Psi^T$ $L_G = M_\Psi L_F M_\Psi^{-1}$

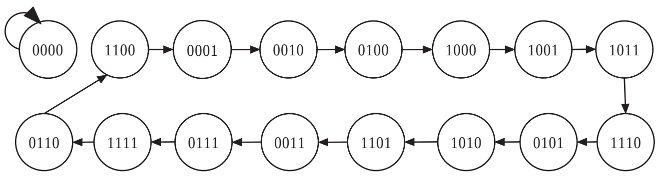

Fig. 6. State transition graph of Galois NLFSR in Example 3

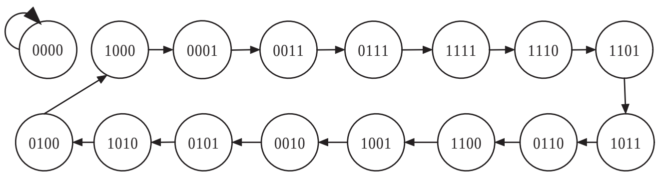

Fig. 7. State transition graph of Fibonacci NLFSR in Example 3

Also we can obtain the structure matrix L_F of the equivalent Fibonacci NLFSR:

$$L_F = \delta_{16}[2\ 3\ 5\ 7\ 10\ 12\ 14\ 15\ 1\ 4\ 10\ 6\ 8\ 9\ 13\ 16]$$

From the state transition graph of the Galois NLFSR, we know that the Galois NLFSR is a uniform Galois NLFSR.

By using Lemma 3, the absolutely equivalent Fibonacci NLFSR is :

$$\begin{cases} y_0(t+1) = y_1(t), \\ y_1(t+1) = y_2(t), \\ y_2(t+1) = y_3(t), \\ y_3(t+1) = y_0(t) \oplus y_2(t) \oplus y_3(t) \oplus y_1(t)y_2(t) \oplus \\ \qquad\qquad y_1(t)y_3(t) \oplus y_2(t)y_3(t). \end{cases} \tag{20}$$

The state transition graph of NLFSR (20) is shown in Fig.7. This example verifies Theorem 3 and Algorithm 1. The Fibonacci NLFSR (20) is obtained by using Algorithm 1 are absolutely equivalent to Galois NLFSR (19). From the state transition graph of Galois NLFSR (19) and Fibonacci NLFSR (20), we can know that the set of output sequences of NLFSR (20) and NLFSR (19) are the same.

Example 4 *Consider an 3-bit Fibonacci NLFSR*

$$\begin{cases} x_0(t+1) = x_1(t) \\ x_1(t+1) = x_2(t), \\ x_2(t+1) = x_0(t) \oplus x_1(t)x_2(t). \end{cases} \tag{21}$$

By simple computations, we can obtain the structure matrix of (21) as $L_F = \delta_8[2\ 3\ 5\ 7\ 1\ 4\ 6\ 8]$. Then we can obtain the state transition graph of Fibonacci NLFSR (21) shown in Fig.8. By using Algorithm 2, the structure matrix of bijection Ψ from Fibonacci NLFSR to Galois NLFSR is $M_\Psi = \delta_8[2\ 1\ 4\ 3\ 6\ 5\ 8\ 7]$. Let $L_G = M_\Psi L_F M_\Psi^{-1}$, so the structure matrix of Galois NLFSR is $L_G = \delta_8[4\ 1\ 8\ 6\ 3\ 2\ 7\ 5]$.

By Lemma 2, we can conclude that the equation of Gaolis NLFSR is given as follows:

$$\begin{cases} y_0(t+1) = y_1(t)\neg y_2(t) \oplus y_1(t)y_2(t) \\ y_1(t+1) = \neg y_2(t), \\ y_2(t+1) = y_0(t) \oplus \neg y_1(t) \oplus y_1(t)y_2(t). \end{cases} \tag{22}$$

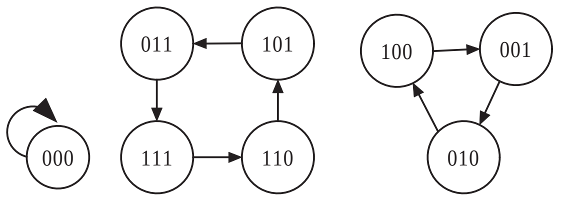

Fig. 8. State transition graph of Fibonacci NLFSR in Example 4

The state transition graph of Galois NLFSR is shown in Fig. 9. One can know that the set of the output sequences of Fibonacci NLFSR and Galois NLFSR are same. This example verifies that Algorithm 2 is efficient to achieve the transformation from Fibonacci NLFSR to Galois NLFSR.

5 Conclusion and future work

In this paper, a detailed analysis has been presented for the synchronization of complex dynamical networks with impulsive coupling. By utilizing the new concept of *average impulsive interval*, a *unified* synchronization criterion is derived for directed impulsive dynamical networks, which takes into account two types of impulses *simultaneously*. According to theoretical analysis and numerical examples, our result has been proved to be less conservative. Moreover, simulations are given to confirm that the result can be applied to large-scale impulsive dynamical networks.

In this paper, the impulsive strength is assumed to be invariable. However, in reality, the strength of impulsive signal can be different at different instants. Therefore, it would be of great interest to study unified synchronization criterion for networks with time-varying impulsive strength. Some good results have been obtained in this issue (Guan *et al.* (2005)Guan *et al.* (2006)). Moreover, unified synchronization criterion for impulsive networks with non-identical nodes will also be considered in the near future by using the concept of tolerant error.

Acknowledgement

We wish to thank Mr. Chi Huang for his helpful discussion throughout the development of this research. The authors thank the referee and the editor for their valuable comments and constructive suggestions.

References

Arenas, A., A. Díaz-Guilera, J. Kurths, Y. Moreno and C.S. Zhou (2008). 'Synchronization in complex networks'. *Physics Reports* **469**(3), 93–153.

Bainov, D. and P.S. Simeonov (1989). *Systems with Impulsive Effect: Stability Theory and Applications.* Ellis Horwood Limited, Chichester, UK.

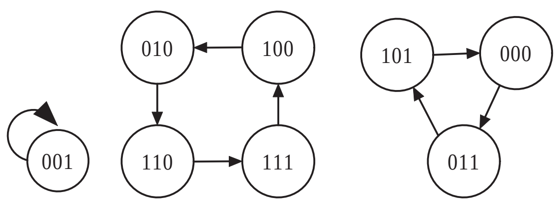

Fig. 9. State transition graph of Galois NLFSR in Example 4

Barabási, A. and R. Albert (1999). 'Emergence of scaling in random networks'. *Science* **286**(5439), 509–512.

Cai, S., J. Zhou, L. Xiang and Z.R. Liu (2008). 'Robust impulsive synchronization of complex delayed dynamical networks'. *Physics Letters A* **372**(30), 4990–4995.

Chen, W. and W.X. Zheng (2009*a*). 'Input-to-state stability and integral input-to-state stability of nonlinear impulsive systems with delays'. *Automatica* **45**(6), 1481–1488.

Chen, W.-H. and W. X. Zheng (2009*b*). 'Global exponential stability of impulsive neural networks with variable delay: An lmi approach'. *IEEE Transactions on Circuits and Systems-I* **56**(6), 1248–1259.

Chung, F. (1997). *Spectral Graph Theory.* American Mathematical Society.

Gao, H., J. Lam and G.R. Chen (2006). 'New criteria for synchronization stability of general complex dynamical networks with coupling delays'. *Physics Letters A* **360**(2), 263–273.

Guan, Z., D.J. Hill and J. Yao (2006). 'A hybrid impulsive and switching control strategy for synchronization of nonlinear systems and application to Chua's chaotic circuit'. *International Journal of Bifurcation and Chaos* **16**, 229–238.

Guan, Z., D.J. Hill and X. Shen (2005). 'On hybrid impulsive and switching systems and application to nonlinear control'. *IEEE Transactions on Automatic Control* **50**(7), 1058–1062.

Hespanha, J. and A.S. Morse (1999). 'Stability of switched systems with average dwell-time'. *38th Proc. IEEE Conf. Decision Control* **3**, 2655–2660.

Hespanha, J., D. Liberzon and A.R. Teel (2005). 'On input-to-state stability of impulsive systems'. *44th Proc. IEEE Conf. Decision Control* pp. 3992–3997.

Hoppensteadt, F. and E.M. Izhikevich (2000). 'Pattern recognition via synchronization in phase-locked loop neural networks'. *IEEE Transactions on Neural Networks* **11**(3), 734–738.

Horn, R. and C.R. Johnson (1990). *Matrix Analysis.* Cambridge University Press.

Krinsky, V., V.N. Biktashev and I.R. Efimov (1991). 'Autowave principles for parallel image processing'. *Physica D* **49**(1-2), 247–253.

Li, Z. and G.R. Chen (2006). 'Global synchronization and asymptotic stability of complex dynamical networks'. *IEEE Transactions on Circuits and Systems-II* **53**(1), 28–33.

Liberzon, D. (2003). *Switching in Systems and Control.* Springer.

Liu, B. and D.J. Hill (2007). Robust stability of complex impulsive dynamical systems. In '46th Proc. IEEE Conf. Decision Control'. pp. 103–108.

Liu, B., K.L. Teo and X. Liu (2008*a*). 'Robust exponential stabilization for large-scale uncertain impulsive systems with coupling time-delays'. *Nonlinear Analysis* **68**(5), 1169–1183.

Liu, B., X.Z. Liu, G.R. Chen and H.Y. Wang (2005). 'Robust impulsive synchronization of uncertain dynamical networks'. *IEEE Transactions on Circuits and*

Systems-I **52**(7), 1431–1441.

Liu, Y., Z. Wang, J. Liang and X. Liu (2008*b*). 'Synchronization and state estimation for discrete-time complex networks with distributed delays'. *IEEE Transactions on Systems, Man and Cybernetics, Part B* **38**(5), 1314–1325.

Lu, J. and D.W.C. Ho (2010). 'Globally exponential synchronization and synchronizability for general dynamical networks '. *IEEE Transactions on Systems, Man and Cybernetics, Part B* **40**(2), 350–361.

Lu, J., D.W.C. Ho and L.G. Wu (2009*a*). 'Exponential stabilization in switched stochastic dynamical networks'. *Nonlinearity* **22**, 889–911.

Lu, J., D.W.C. Ho and Z.D. Wang (2009*b*). 'Pinning stabilization of linearly coupled stochastic neural networks via minimum number of controllers '. *IEEE Transactions on Neural Networks* **20**, 1617–1629.

Lu, W. and T. Chen (2006). 'New approach to synchronization analysis of linearly coupled ordinary differential systems'. *Physica D* **213**(2), 214–230.

Newman, M. and D.J. Watts (1999). 'Scaling and percolation in the small-world network model'. *Physical Review E* **60**(6), 7332–7342.

Pecora, L. and T.L. Carroll (1998). 'Master stability functions for synchronized coupled systems'. *Physical Review Letters* **80**(10), 2109–2112.

Wang, X. and G.R. Chen (2002). 'Synchronization in scale-free dynamical networks: robustness and fragility'. *IEEE Transactions on Circuits and Systems-I* **49**(1), 54–62.

Wang, Y., H.O. Wang, J.W. Xiao and Z.H. Guan (2010). 'Synchronization of complex dynamical networks under recoverable attacks'. *Automatica* **46**, 197–203.

Wu, C. (2005). 'Synchronization in networks of nonlinear dynamical systems coupled via a directed graph'. *Nonlinearity* **18**(3), 1057–1064.

Wu, C. (2007). *Synchronization in Complex Networks of Nonlinear Dynamical Systems.* World Scientific Publishing Company.

Yang, T. (2001). *Impulsive Systems and Control: Theory and Application.* New York: Nova Science.

Yang, Z. and D. Xu (2005). 'Stability analysis of delay neural networks with impulsive effects'. *IEEE Transactions on Circuits and Systems-II* **52**(8), 517–521.

Yao, J., Z.H. Guan and D.J. Hill (2009). 'Passivity-based control and synchronizationnext term of general complex dynamical networks'. *Automatica* **45**(9), 2107–2113.

Yu, W., G.R. Chen and J.H. Lü (2009). 'On pinning synchronization of complex dynamical networks'. *Automatica* **45**, 429–435.

Zhang, G., Z. Liu and Z. Ma (2007). 'Synchronization of complex dynamical networks via impulsive control'. *Chaos* **17**, 043126.

Zhang, H., Z.H. Guan and D.W.C. Ho (2006). 'On synchronization of hybrid switching and impulsive networks'. *45th Proc. IEEE Conf. Decision Control* pp. 2765–2770.

Zhang, H., Z.H. Guan and G. Feng (2008). 'Reliable dissipative control for stochastic impulsive systems'. *Automatica* **44**(4), 1004–1010.

Zhang, Q. and J.A. Lu (2009). 'Impulsively control complex networks with different dynamical nodes to its trivial equilibrium'. *Computers and Mathematics with Applications* **57**, 1073–1079.

Zhou, J., L. Xiang and Z. Liu (2007). 'Synchronization in complex delayed dynamical networks with impulsive effects'. *Physica A* **384**(2), 684–692.

Zou, F. and J.A. Nossek (1993). 'Bifurcation and chaos in cellular neural networks'. *IEEE Transactions on Circuits and Systems-I* **40**(3), 166–173.

Appendix

Example 5 *This example is devoted to the discussion of non-uniformly distributed impulses. A specific example is given to show that lower bound or upper bound of impulsive intervals, which has been widely used in literature, can not precisely describe the occurrence frequency of impulses.*

We give a specific impulsive signal as $\bar{\zeta} = \{\epsilon, 2\epsilon, ..., (N_0-1)\epsilon, N_0T_a, N_0T_a + \epsilon, N_0T_a + 2\epsilon, ..., N_0T_a + (N_0-1)\epsilon, 2N_0T_a, ...\}$, *where* ϵ *and* T_a *are positive numbers satisfies* $\epsilon < T_a$, *and* N_0 *is a positive integer. The impulsive signal* $\bar{\zeta} = \{t_1, t_2, t_3, ...\}$ *can also be re-written in the following form:*

$$t_k - t_{k-1} = \begin{cases} \epsilon, & \text{if } mod(k, N_0) \neq 0, \\ N_0(T_a-\epsilon)+\epsilon, & \text{if } mod(k, N_0) = 0. \end{cases} \quad (23)$$

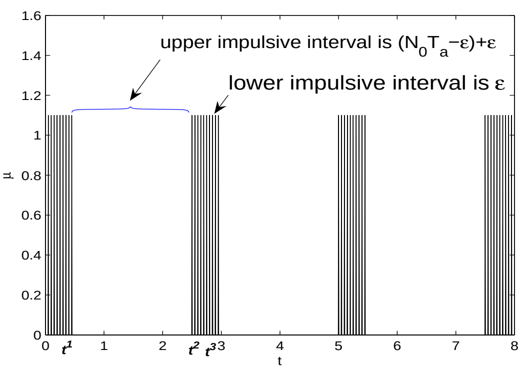

Fig. 10. Example of a specific impulsive sequence described in (23) with $\epsilon = 0.05$, $N_0 = 10$ and $T_a = 0.5$. Such an impulsive sequence simultaneously owns small lower bound and large upper bound of impulsive intervals.

From the structure of the impulsive signal $\bar{\zeta}$, *we can obtain that* $\inf_{k\in\mathbb{N}^+}\{t_k - t_{k-1}\} = \epsilon$ *and* $\sup_{k\in\mathbb{N}^+}\{t_k - t_{k-1}\} = N_0(T_a-\epsilon)+\epsilon$. *Figure 10 represents such an impulsive signal with* $\epsilon = 0.05$, $N_0 = 10$ *and* $T_a = 0.5$. *It can be observed from Figure 10 that impulses occur frequently in* (t^2, t^3), *whereas they seldom occur in* (t^1, t^2).

When ϵ is sufficiently small and N_0 is sufficiently large, the quantity $\inf_{k\in\mathbb{N}^+}\{t_k - t_{k-1}\} = \epsilon$ will be very small, and the quantity $\sup_{k\in\mathbb{N}^+}\{t_k - t_{k-1}\} = N_0(T_a - \epsilon) + \epsilon$ will be very big. Under such circumstance, the results in (Zhou et al. *(2007); Yang and Xu (2005); Zhang and Lu (2009); Zhang* et al. *(2006); Liu* et al. *(2008*a, *2005); Zhang* et al. *(2007); Cai* et al. *(2008)), would not be applicable.*