SOME PROPERTIES OF THE CYCLE DECOMPOSITION OF
WG-NLFSR

Yujuan Li, Huaifu Wang, Peipei Zhou and Guoshuang Zhang

Abstract. In this paper, we give some properties of the cycle decomposition of a nonlinear feedback shift register called WG-NLFSR which was presented by Mandal and Gong recently. First we give the parity of the state transition transformation of WG-NLFSR and then by the relation of the parity of a permutation and its number of cycles given in Theorem 2 in Section 1, we show that the number of cycles in the cycle decomposition of WG-NLFSR is even. Second we study the properties of the cycle decomposition of WG-NLFSR when the coefficients of the characteristic polynomial belong to the proper subfields of the finite field on which the WG-NLFSR is defined. Finally, we give some properties of the cycle decomposition of the filtering WG7-NLFSR.

1. Introduction

Let $t$ be a positive integer with $t > 1$, $t \mod 3 \neq 0$ and $3k \equiv 1 \mod t$ for some integer $k$. Let $\mathbb{F}_{2^{t}}$ be the finite field with $2^{t}$ elements and let $\mathbb{F}_{2}$ be the finite field of two elements. Let $h(x) = x + x^{q_{1}} + x^{q_{2}} + x^{q_{3}}$ be a function from $\mathbb{F}_{2^{t}}$ to $\mathbb{F}_{2^{t}}$ and the exponents are given by $q_{1} = 2^{k} + 1$, $q_{2} = 2^{2k} + 2^{k} + 1$, $q_{3} = 2^{2k} - 2^{k} + 1$, $q_{4} = 2^{2k} + 2^{k} - 1$. Then the function

$$WGP(x) = h(x + 1) + 1$$

is called the WG permutation in [5, 8]. The condition $t > 1$, $t \mod 3 \neq 0$ and $3k \equiv 1 \mod t$ for some integer $k$ is to make sure $WGP(x)$ is a permutation from $\mathbb{F}_{2^{t}}$ to $\mathbb{F}_{2^{t}}$, for more details one can refer to [3]. Let $Tr(x) = x + x^{2} + x^{4} + \cdots + x^{2^{t-1}}$ be the trace function mapping from $\mathbb{F}_{2^{t}}$ to $\mathbb{F}_{2}$. Then the function from $\mathbb{F}_{2^{t}}$ to $\mathbb{F}_{2}$ defined by

$$WG(x) = Tr(WGP(x))$$

is called the WG transformation in [5, 8].

Let $n$ be a positive integer greater than 1. Let $c_{0}, \ldots, c_{n-1} \in \mathbb{F}_{2^{t}}$ and let $\{a_{i}\}_{i \geq 0}$, $a_{i} \in \mathbb{F}_{2^{t}}$ be a sequence generated by the $n$-stage nonlinear recurrence relation, which is defined as

$$a_{n+k} = c_{0}a_{k} + c_{1}a_{k+1} + \cdots + c_{n-1}a_{n-1+k} + WGP(a_{n-1+k}), k \geq 0, \quad (1)$$

2010 Mathematics Subject Classification: 94A55, 94A60.
Key words and phrases: Permutation, WG-NLFSR, cycle decomposition.
* Corresponding author.
where WGP(x) is the WG permutation and \((a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_2^n\) is the initial state. Let \(p(x) = c_0 + c_1x + \cdots + c_{n-1}x^{n-1} + x^n\). The polynomial \(p(x)\) is called the characteristic polynomial of relation (1) and the nonlinear recurrence relation (1) is called the WG-NLFSR recurrence relation in [8]. An architecture of the WG-NLFSR is shown in Figure 1.

\[
\begin{align*}
\text{WG} & \quad a_{n-1} \\
\downarrow & \quad \downarrow \\
\oplus & \quad \oplus \\
a_{n-2} & \quad c_{n-2} \\
\downarrow & \quad \downarrow \\
\oplus & \quad \oplus \\
c_{n-1} & \quad c_{n-1} \\
\end{align*}
\]

**Figure 1. An Architecture of the WG-NLFSR**

The filtering WG-NLFSR consists of the WG-NLFSR and a WG transformation. The filtering WG-NLFSR sequence \(\{b_i\}_{i \geq 0}\) is defined by \(b_i = \text{WG}(a_i)\), where WG(x) is the WG transformation. For \((a_0, \cdots, a_{n-1}) \in \mathbb{F}_2^n\), let

\[
T(a_0, \cdots, a_{n-1}) = (a_1, \cdots, a_{n-1}, c_0a_0 + \cdots + c_{n-1}a_{n-1} + \text{WGP}(a_{n-1})).
\]

Then one can check that \(T\) is a permutation from \(\mathbb{F}_2^n\) to \(\mathbb{F}_2^n\) if and only if \(c_0 \neq 0\). We call \(T\) the state transition transformation of the WG-NLFSR. In this paper, from now on, we suppose that \(c_0 \neq 0\), and then \(T\) is a permutation from \(\mathbb{F}_2^n\) to \(\mathbb{F}_2^n\).

The filtering WG-NLFSR was presented by Mandal and Gong in their paper [8]. They investigated the periodicity of a sequence generated by the filtering WG-NLFSR by considering the model WG-NLFSR. They first performed the cycle decomposition of WG-NLFSR recurrence relations over different finite fields by computer simulations using different characteristic polynomials and a fixed WG permutation. Secondly, they conducted an empirical study on the period distribution of the sequences generated by the WG-NLFSR.

**Remark 1.** The period of \(\{b_i\}_{i \geq 0}\) produced by the filtering WG-NLFSR is a factor of the period of \(\{a_i\}_{i \geq 0}\), so analyzing the period of the sequence \(\{a_i\}_{i \geq 0}\) can help us analyze the period of the sequence \(\{b_i\}_{i \geq 0}\). Since the state transition transformation \(T\) of the WG-NLFSR is a permutation when \(c_0 \neq 0\), analyzing the period of the sequence \(\{a_i\}_{i \geq 0}\) is equivalent to analyzing the cycle decomposition of the state transition transformation \(T\) of the WG-NLFSR. Sometimes we call the cycle decomposition of the state transition transformation of a NLFSR the cycle decomposition of the NLFSR for short.

As we know the cycle decomposition of a general NLFSR is not well understood [6]. It is hard to determine the number of cycles and the lengths of the cycles in a cycle decomposition of an NLFSR. In the theory of NLFSRs, the property of the cycle decomposition of NLFSRs is an important property to look at first, since each cycle can be considered as a sequence and the length of the cycle determines the period of the sequence. For more details on the study results of the cycle decomposition of NLFSRs, one can refer to [2, 4, 6, 7, 9, 10].
In this paper, we give some properties of the cycle decomposition of WG-NLFSR in theory. First we mainly investigate the parity of the state transition transformation of WG-NLFSR and the parity of the number of the cycles in the cycle decomposition of the state transition transformation of WG-NLFSR and we get the following Theorem 1, Theorem 2 and Theorem 3.

In the following Theorem 1, Theorem 3 and Theorem 4, we always suppose that $t$ is a positive integer with $t > 1$, $t \mod 3 \neq 0$ and $3k \equiv 1 \mod t$ for some integer $k$ and $n$ is a positive integer greater than 1.

**Theorem 1.** The state transition transformation $T$ of the $n$-stage WG-NLFSR over $\mathbb{F}_{2^t}$ is an even permutation of $\mathbb{F}_{2^n}^n$.

**Theorem 2** Let $\Omega$ be an arbitrary nonempty finite set and let $\pi$ be an arbitrary permutation of $\Omega$. Let $|\Omega|$ be the number of elements of the set $\Omega$, $\pi_p$ be the parity of the permutation $\pi$ ($\pi_p = 0$ or 1, where 0 represents the even permutation, 1 represents the odd permutation), and $N_\pi$ be the number of cycles in the cycle decomposition of $\pi$. Then $N_\pi \equiv (|\Omega| + \pi_p) \mod 2$.

Using Theorem 1 and Theorem 2, we can deduce the following Theorem 3 and by the method to prove Theorem 1 and the result of Theorem 2 we give another proof of a well-known theorem given by Golomb[4].

**Theorem 3** The number of cycles in the cycle decomposition of the state transition transformation $T$ of the WG-NLFSR is even.

Second we study the properties of the cycle decomposition of the WG-NLFSR when the coefficients of the characteristic polynomial belong to a proper subfield of $\mathbb{F}_{2^t}$, and we get the following results.

**Theorem 4** Let $\mathbb{F}_{2^s}$ be a proper subfield of $\mathbb{F}_{2^t}$. If all the coefficients of the characteristic polynomial belong to $\mathbb{F}_{2^s}$, then the period of the sequence generated by the $n$-stage WG-NLFSR with initial state in $\mathbb{F}_{2^s}^n$ will be less than or equal to $2^{sn} - 1$.

For Theorem 1 and Theorem 3, we want to point out that it is still true if one uses any other permutation over $\mathbb{F}_{2^t}(t > 1)$ instead of the WG permutation. One can see this from Lemma 1 and the explanations after the proof of Lemma 1. In fact in the proof of Theorem 1 and Theorem 3, we only use the conditions that the WGP$(x)$ is a permutation, $c_0 \neq 0$ and $n, t$ are positive integers greater than 1. In [8], they performed computer simulations over finite fields $\mathbb{F}_{2^5}$ and $\mathbb{F}_{2^7}$ for investigating the cycle decomposition of the WG-NLFSR. One can check that their experimental results in Tables 1-4 on the number of cycles in the cycle decomposition of the WG-NLFSR are consistent with Theorem 3. Note that they didn’t provide all the cycles in the cycle decompositions. For Theorem 2, it is a general result and is true for any nonempty finite set and any permutation of it. For Theorem 4, it is proven based on our observation of the expression of the WG permutation.

The remainder of the paper is organized as follows. In Section 2, we mainly prove Theorem 1. In Section 3, we prove Theorem 2 and Theorem 3. In Section 4, we give the proof of Theorem 4. In Section 5, we give some properties of the cycle decomposition of the filtering WG7-NLFSR using the results given in Section 3. Finally, in Section 6, we conclude the paper.

2. The Parity of the State Transition Transformation of WG-NLFSR

In this section, we mainly use the basic knowledge of permutations to prove Theorem 1. First we recall some knowledge of permutations used in this paper and for more information one can refer to [1]. Let $q$ be a positive integer greater than 1.

---

**Some properties of the cycle decomposition of WG-NLFSR**
By group theory, it is well known that each permutation $\sigma$ in the symmetric group $S_q$ can be written as a product of disjoint cycles. Suppose that the decomposition of $\sigma$ into a product of pairwise disjoint cycles consists of $k_1$ 1-cycles, $k_2$ 2-cycles, $\cdots$, and $k_m$ $m$-cycles, where $1 \leq m \leq q$ and $k_i(i = 1, \cdots, m)$ are non-negative integers. Then $\sum_{i=1}^m ik_i = q$ and the number of cycles of $\sigma$ is $\sum_{i=1}^m k_i$. A permutation is called an even (odd) permutation if it can be written as a product of 2-cycles of even (odd) number. For example, if $i$ is even, then the $i$-cycle is an odd permutation otherwise it is an even permutation. The product of two even (odd) permutations is an even permutation. The product of an even and an odd permutation is an odd permutation. Two permutations $\sigma$ and $\xi$ in the symmetric group $S_q$ are called conjugate if there exits a permutation $\tau$ in $S_q$ such that $\sigma = \tau^{-1} \xi \tau$. A permutation has the same parity as all its conjugate permutations.

We define some permutations of the $n$-dimensional vector space $F^{n}_{2^t}$ over $F_{2^t}$, where $t$ is a positive integer with $t > 1$, $t \mod 3 \neq 0$ and $3k \equiv 1 \mod t$ for some integer $k$ and $n$ is a positive integer greater than 1. For $(a_0, \cdots, a_{n-1}) \in F^{n}_{2^t}$, let

$$L_1(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-2}, a_{n-1} + a_{n-2}).$$

$$T_{WGP}(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-3}, WGP(a_{n-2}), a_{n-1}).$$

Let $c_0, \cdots, c_{n-1} \in F_{2^t}$, $c_0 \neq 0$.

$$L(a_0, a_1, \cdots, a_{n-1}) = (a_1, a_2, \cdots, a_{n-1}, c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1}).$$

It is easy to see that $L_1$ and $T_{WGP}$ are permutations of $F^{n}_{2^t}$. Since $c_0 \neq 0$, $L$ is a permutation of $F^{n}_{2^t}$. Now we can write $T$ as the composition of the permutations defined above.

**Lemma 1.** The state transition transformation $T$ of the WG-NLFSR is the composition of $T^{-1}_{WGP}, L_1, T_{WGP}$ and $L$, i.e., $T = T^{-1}_{WGP} \circ L_1 \circ T_{WGP} \circ L$, where $\circ$ denotes the composition of maps.

**Proof.** Let $(a_0, a_1, \cdots, a_{n-2}, a_{n-1}) \in F^{n}_{2^t}$ be an arbitrary $n$-tuple. Note that $T_{WGP}(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-3}, WGP^{-1}(a_{n-2}), a_{n-1})$. Then

$$T^{-1}_{WGP} \circ L_1 \circ T_{WGP} \circ L(a_0, a_1, \cdots, a_{n-1})$$

$$= T^{-1}_{WGP} \circ L_1 \circ T_{WGP}(a_0, a_1, \cdots, a_{n-1}, c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1})$$

$$= T^{-1}_{WGP} \circ L_1(a_1, a_2, \cdots, a_{n-2}, WGP(a_{n-1}), c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1})$$

$$= T^{-1}_{WGP}(a_1, a_2, \cdots, a_{n-2}, WGP(a_{n-1}), c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1})$$

$$= (a_1, a_2, \cdots, a_{n-2}, c_0a_0 + c_1a_1 + \cdots + c_{n-1}a_{n-1} + WGP(a_{n-1}))$$

$$= T(a_0, a_1, \cdots, a_{n-1}).$$

Hence, $T = T^{-1}_{WGP} \circ L_1 \circ T_{WGP} \circ L$. This completes the proof of Lemma 1.

Since a permutation has the same parity as all its conjugate permutations, by Lemma 1, to prove $T$ is even, we only need to prove that both $L_1$ and $L$ are even. First for $(a_0, \cdots, a_{n-1}) \in F^{n}_{2^t}$, we let

$$L_2(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-2}, a_{n-1} + c_1a_0 + \cdots + c_{n-1}a_{n-2}).$$

Then we have

**Lemma 2.** Let $n$ and $t$ be positive integers greater than 1. Then $L_2$ is an even permutation of $F^{n}_{2^t}$. 
Proof. Let \( h = \#\{i | c_i \neq 0, 1 \leq i \leq n - 1\} \). If \( h = 0 \), then \( L_2 \) is the identity mapping, then \( L_2 \) is even. If \( h \neq 0 \), it does not lose the generality to suppose that \( c_{n-1} \neq 0 \). Let \( \mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_2^n \) be an arbitrary \( n \)-tuple. Then one can see that \( L_2 \mathbf{a} = \mathbf{a} \) if and only if \( a_{n-2} = c_{n-1}^{-1} \sum_{i=1}^{n-2} c_i a_{i-1} \). So all the fixed points of \( L_2 \) are the \( n \)-tuples with \( a_{n-2} = c_{n-1}^{-1} \sum_{i=1}^{n-2} c_i a_{i-1} \). Then \( L_2 \) has \( (2^t)^{n-1} \) fixed points. If \( a_{n-2} \neq c_{n-1}^{-1} \sum_{i=1}^{n-2} c_i a_{i-1} \), then \( L_2^2 \mathbf{a} = \mathbf{a} \) and \( L_2 \mathbf{a} \neq \mathbf{a} \). So \( L_2 \) is the composition of \( \frac{1}{2}((2^t)^n - (2^t)^{n-1}) \) transpositions. Obviously, \( \frac{1}{2}((2^t)^n - (2^t)^{n-1}) \) is even when \( n > 1 \) and \( t > 1 \). So \( L_2 \) is an even permutation. This completes the proof of Lemma 2.

One can see that \( L_1 \) is a special case of \( L_2 \). So by Lemma 2, we can directly have the following corollary.

**Corollary 1.** Let \( n \) and \( t \) be positive integers greater than 1. Then \( L_1 \) is an even permutation of \( \mathbb{F}_2^n \).

For \( (a_0, \cdots, a_{n-1}) \in \mathbb{F}_2^n \), let

\[
C_0(a_0, a_1, \cdots, a_{n-1}) = (a_0, a_1, \cdots, a_{n-2}, c_0 a_{n-1}).
\]

And let

\[
\tau(a_0, a_1, \cdots, a_{n-1}) = (a_1, a_2, \cdots, a_{n-1}, a_0).
\]

One can check that \( C_0 \) and \( \tau \) are all permutations of \( \mathbb{F}_2^n \) and \( L = L_2 \circ C_0 \circ \tau \). In the following, we will prove that \( C_0 \) and \( \tau \) are even permutations. Then we can deduce that \( L \) is also an even permutation.

**Lemma 3.** Let \( n \) and \( t \) be positive integers greater than 1. Then \( C_0 \) is an even permutation of \( \mathbb{F}_2^n \).

**Proof.** If \( c_0 = 1 \), then \( C_0 \) is the identity mapping. If \( c_0 \neq 1 \), then the order of \( c_0 \) is not equal to 1. Denote the order of \( c_0 \) is \( r \), i.e., \( r \) is a positive integer greater than 1. Let \( \mathbf{a} = (a_0, a_1, \cdots, a_{n-1}) \in \mathbb{F}_2^n \) be an arbitrary \( n \)-tuple. Then \( C_0 \mathbf{a} = \mathbf{a} \) if and only if \( a_{n-1} = 0 \). So all the fixed points of \( C_0 \) are the \( n \)-tuples with \( a_{n-1} = 0 \). Thus \( C_0 \) has \( (2^t)^{n-1} \) fixed points. If \( a_{n-1} \neq 0 \), then \( C_0^r \mathbf{a} = \mathbf{a} \) and \( C_0^r \mathbf{a} \neq \mathbf{a} \) for every positive integer \( s, 1 \leq s < r \). So \( C_0 \) is the composition of \( 2^t(n-1) \left( \frac{2^t}{r} - 1 \right) \) \( r \)-cycles. Since \( r \) is the order of \( c_0 \), \( c_0 \in \mathbb{F}_2^r, c_0 \neq 1 \) and \( t > 1 \), then \( r \) can divide \( 2^t - 1 \), so \( r \) is odd and thus each \( r \)-cycle is an even permutation. Hence \( C_0 \) is an even permutation. This completes the proof of Lemma 3.

Note that \( \tau \) is the so-called pure circulation. In the following, we first extend some results of the \( n \)-stage pure cycling register (\( PCR_n \)) over \( \mathbb{F}_2 \) to the general finite field of characteristic 2. And then prove that the pure circulation \( \tau \) is an even permutation when \( t \) and \( n \) are positive integers greater than 1.

**Theorem 5**[4] Let \( n \) be a positive integer greater than 1. Then the length of each cycle in the decomposition of the pure circulation of \( \mathbb{F}_2^n \) is a factor of \( n \). Let \( d \) be a positive factor of \( n \). Then the number of cycles of length \( d \) in the decomposition of the pure circulation is

\[
M(d) = \frac{1}{d} \sum_{d' | d} \mu(d') 2^{d'/d}
\]

where the sum takes over all the positive factors of \( d \), and \( \mu(d) \) is the Möbius function, then the number of cycles in the cycle decomposition of the pure circulation of
Let \( \mathbb{F}_2 \) be

\[ Z(n) = \frac{1}{n} \sum_{d|n} \phi(d)2^{n/d} \]

where the sum takes over all the positive factors of \( n \), and \( \phi(d) \) is Euler function. If \( n \neq 2 \), then \( Z(n) \) is even.

Theorem 5 is on the result of the decomposition of the pure circulation over \( \mathbb{F}_2 \).

For \( \mathbb{F}_2 \), one can check that \( M(d) \) may not be even, but for \( \mathbb{F}_2 \) (\( t > 1 \)), we will prove in the following theorem that \( M(d) \) is always even.

**Theorem 6** Let \( t > 1 \). Then the length of each cycle in the decomposition of the pure circulation is a factor of \( n \). Let \( d \) be a positive factor of \( n \). Then the number of cycles of length \( d \) in the decomposition of the pure circulation is

\[ M(d) = \frac{1}{d} \sum_{d'|d} \mu(d')(2^t)^{d/d'} \]

where the sum takes over all positive factors of \( d \), and \( \mu(d) \) is the Möbius function. Furthermore \( M(d) \) is even.

**Proof.** Let \( i \geq 0 \) and \( (a_1, a_{i+1}, \cdots, a_{i+n-1}) \) be an arbitrary state of the pure circulation. Then by the definition of the pure circulation, we have

\[ \tau^n(a_1, a_{i+1}, \cdots, a_{i+n-1}) = (a_i, a_{i+1}, \cdots, a_{i+n-1}). \]

This proves that the length of each cycle in the decomposition of the pure circulation is a factor of \( n \).

Let \( d \) be a positive factor of \( n \). Let \( (a_1, a_2, \cdots, a_n) \) be a state of \( \tau \) and the period of it be a factor of \( d \), then \( (a_1, a_2, \cdots, a_n) = (a_{d+1}, a_{d+2}, \cdots, a_n, a_1, a_2, \cdots, a_d) \). So

\[ a_j = a_{j+d} = a_{2d+j} = \cdots = a_{(n/d-1)d+i}, j = 1, 2, \cdots, d. \]

That is,

\[ (a_1, a_2, \cdots, a_n) = (a_1, a_2, \cdots, a_d, a_1, a_2, \cdots, a_d, \cdots, a_1, a_2, \cdots, a_d). \]

On the contrary, if \( (a_1, a_2, \cdots, a_d) \) is an arbitrary \( d \)-tuple, then the period of the state \( (a_1, a_2, \cdots, a_n) = (a_1, a_2, \cdots, a_d, a_1, a_2, \cdots, a_d, \cdots, a_1, a_2, \cdots, a_d) \) is a factor of \( d \). Hence \( \tau \) has \((2^t)^d\) states whose periods are factors of \( d \). On the other side, the number of the states whose periods are factors of \( d \) is

\[ \sum_{d'|d} d'M(d'), \]

where the sum takes over all positive factors of \( d \). Thus

\[ \sum_{d'|d} d'M(d') = (2^t)^d. \]

By the Möbius inversion formula, we have

\[ M(d) = \frac{1}{d} \sum_{d'|d} \mu(d')(2^t)^{d/d'}. \]

In the following we will prove that \( M(d) \) is even. If \( d \) is odd, then by the above formula, we have

\[ dM(d) = \sum_{d'|d} \mu(d')(2^t)^{d/d'}. \]
So $M(d)$ is even. If $d = 2^k$, $k > 0$, then
\[ M(2^k) = \frac{1}{2^k} \sum_{d' | 2^k} \mu(d')(2^k/d') = \frac{1}{2^k}((2^k)^2k - (2^k)^2k-1), \]
so $M(d)$ is even since $k > 0$, $t > 1$. If $d = 2^km$, $(k > 0)$, gcd$(m, 2) = 1$, then
\[ M(2^km) = \frac{1}{2^km} \sum_{d' | 2^km} \mu(d')(2^km/d') \]
(2) \[ = \frac{1}{m} \sum_{d' | 2^km} \mu(d')2^{kmt/d'} - k. \]
(3) If $k = 1$, then $2^km/d' - k = 2mt/d' - 1 \geq t - 1 \geq 1$. So $2^{(2^km/d')-k}$ is even. If $k \geq 2$, let $d' = 2^ml$, where $m | m, l \leq k$. If $l \geq 2$, then $\mu(d') = 0$. If $l \leq 1$, then
\[ 2^km/d' - k = 2^{k-1}mt/m' - k \geq 2^{k-1}t - k \geq 2^{k-1}t - k \geq 2^k - k > 1. \]
So $2^{(2^km/d')-k}$ is also even. Hence, the numerator of the right part of equation (3) is always even while the denominator is odd, so $M(d)$ is even. This completes the proof of Theorem 6.

**Corollary 2** Let $t$ and $n$ be positive integers greater than 1. Then the pure circulation $\tau$ is an even permutation of $\mathbb{F}_2^n$.

**Proof.** By Theorem 6, the length of each cycle of the permutation $\tau$ is a factor of $n$. Let $d$ be a positive factor of $n$. If $d$ is even, then all the $d$-cycles are even permutations. If $d$ is even, then all the $d$-cycle are odd permutation. However, according to Theorem 6, the number of the cycles with length $d$ is always even. So $\tau$ is an even permutation following from the basic knowledge of group theory that the product of two even (odd) permutations is an even permutation. This completes the proof of Corollary 2.

**Corollary 3** Let $n$ and $t$ be positive integers greater than 1. Then $L$ is an even permutation of $\mathbb{F}_2^n$.

**Proof.** Since $t$ and $n$ are positive integers greater than 1, by Lemma 2, we know $L_2$ is an even permutation. By Lemma 3, we know $C_0$ is an even permutation. And by Corollary 2, we know $\tau$ is an even permutation. By the definition of $L, L_2, C_0$ and $\tau$, we have known that $L = L_2 \circ C_0 \circ \tau$. So $L$ is an even permutation following from the product of two even (odd) permutations is an even permutation. This completes the proof of Corollary 3.

We want to point out that $L$ in fact is the state transition transformation of a linear feedback shift register over $\mathbb{F}_2^n$. From Corollary 3, we know that all state transition transformations of the linear feedback shift registers over a general finite field $\mathbb{F}_2^t (t > 1)$ are even permutations.

Applying the above lemmas and corollaries, we can give the proof of our first main result.

**Proof of Theorem 1.** By Lemma 1, we have $T = T^{-1}_{WGP} \circ L_1 \circ T_{WGP} \circ L$. Since $t$ is a positive integer with $t > 1, t \mod 3 \neq 0$ and $3k \equiv 1 \mod t$ for some integer $k$ and $n$ is a positive integer greater than 1, $T_{WGP}$ is a permutation and by Corollary 1, $L_1$ is an even permutation of $\mathbb{F}_2^n$. So $T^{-1}_{WGP} \circ L_1 \circ T_{WGP}$ is an even permutation of $\mathbb{F}_2^n$. By Corollary 3, $L$ is an even permutation of $\mathbb{F}_2^n$. So $T$ is an even permutation of $\mathbb{F}_2^n$. This completes the proof of Theorem 1.
3. The parity of the number of cycles in the cycle decomposition of WG-NLFSR

In this section, we first give the proof of Theorem 2 and then using Theorem 1 and Theorem 2 we prove Theorem 3. Finally, we use our method to give another proof of a theorem given by Golomb[4].

Proof of Theorem 2. Suppose that the decomposition of $\pi$ into a product of pairwise disjoint cycles consists of $k_1$ 1-cycles, $k_2$ 2-cycles, $\cdots$, and $k_m$ $m$-cycles, where $1 \leq m \leq |\Omega|$ and $k_i (i = 1, \cdots, m)$ are non-negative integers. Then the number of cycles of $\pi$ is equal to $m \sum_{i=1}^{\infty} k_i$, i.e., $N_\pi = m \sum_{i=1}^{\infty} k_i$.

Let $N_1 = k_1 + k_3 + \cdots + k_{m_1}$, where $m_1$ is the largest odd integer such that $m_1 \leq m$ and let $N_2 = k_2 + k_4 + \cdots + k_{m_2}$, where $m_2$ is the largest even integer such that $m_2 \leq m$. Then

$$N_\pi = N_1 + N_2.$$ 

Since $\pi$ is a permutation of $\Omega$, we have $k_1 + 2k_2 + \cdots + m \cdot k_m = |\Omega|$. Then

$$|\Omega| \equiv N_1 \mod 2.$$ 

If $\pi_p = 0$, i.e., $\pi$ is an even permutation, note that all cycles with odd lengths are even permutations, then the number of all cycles with even lengths is even, i.e., $N_2$ is even, hence

$$N_\pi = N_1 + N_2 \equiv N_1 \mod 2.$$ 

So according to (4), $N_\pi \equiv |\Omega| \mod 2$.

If $\pi_p = 1$, i.e., $\pi$ is an odd permutation, the same note that all cycles with odd lengths are even permutations, then the number of all cycles with even lengths is odd, i.e. $N_2$ is odd, hence

$$N_\pi = N_1 + N_2 \equiv N_1 + 1 \mod 2.$$ 

So the same according to (4), $N_\pi \equiv |\Omega| + 1 \mod 2$. This completes the proof of Theorem 2.

By Theorem 2, we can directly have the following corollaries.

**Corollary 4** Let $n$ and $t$ be positive integers. Then for every even permutation of $\mathbb{F}_2^n$, the number of cycles in its cycle decomposition is even.

**Proof.** Let $\pi$ denote an even permutation of $\mathbb{F}_2^n$ and let $\pi_p$ denote the parity of $\pi$. Let $N_\pi$ denote the number of all cycles in the cycle decomposition of $\pi$. By Theorem 2, we have

$$N_\pi \equiv (|\mathbb{F}_2^n| + \pi_p) \mod 2.$$ 

Since $\pi$ is an even permutation of $\mathbb{F}_2^n$ and $|\mathbb{F}_2^n| = 2^{nt}$ is even, we have $N_\pi \equiv 0 \mod 2$, i.e., the number of all cycles in the cycle decomposition of $\pi$ is even. This completes the proof of Corollary 4.

**Corollary 5** Let $t$ and $n$ be positive integers greater than 1. Then the number of cycles in the cycle decomposition of $L$ is even.

**Proof.** Since $t$ and $n$ are positive integers greater than 1, by Corollary 3, $L$ is an even permutation of $\mathbb{F}_2^n$. Then by Corollary 4, the number of cycles in the cycle decomposition of $L$ is even. This completes the proof of Corollary 5.

From Corollary 5, we know that the number of cycles in the cycle decomposition of the state transition transformation of a linear feedback shift register over $\mathbb{F}_2(t > 1)$ is even.
**Proof of Theorem 3.** Since $t$ is a positive integer with $t > 1$, $t \mod 3 \neq 0$ and $3k \equiv 1 \mod t$ for some integer $k$ and $n$ is a positive integer greater than 1, by Theorem 1, $T$ is an even permutation of $F_{2^n}$. Then by Corollary 4, the number of cycles in the cycle decomposition of $T$ is even. This completes the proof of Theorem 3.

In 1967, Golomb [4] gave the parity of the number of cycles of a shift register over $F_2$. In detail, they gave and proved the following Theorem 7. It should be noted that their result and proof are only over $F_2$ and can not be extended to general finite fields. Using our method and Theorem 2, we can give another proof of Theorem 7. This shows that our method is more general.

**Theorem 7** [4] For $n > 2$, let $T_2(x_0, x_1, \ldots, x_{n-1}) = (x_1, \ldots, x_{n-1}, x_0 + f(x_1, \ldots, x_{n-1}))$ be the transition transformation of a shift register of $F_{2^n}$. Then the number of cycles of $T_2$ is even or odd according to whether the number of 1’s in the truth table of $f(x_1, \ldots, x_{n-1})$ is even or odd.

**Proof.** Firstly, let $T_1(x_0, \ldots, x_{n-1}) = (x_0 + f(x_1, \ldots, x_{n-1}), x_1, \ldots, x_{n-1})$ and let $\tau(x_0, \ldots, x_{n-1}) = (x_1, x_2, \ldots, x_{n-1}, x_0)$. Then one can check that $T_2 = \tau \circ T_1$. For the pure circulation $\tau$ of $F_2^n$, by Theorem 5, we know that for $n > 2$ the total number of cycles in the cycle decomposition of the pure circulation of $F_2^n$ is even. Since the number of elements in $F_2^n$ is even, then by Theorem 2, we can deduce that the pure circulation $\tau$ of $F_2^n$ is an even permutation. For $T_1$, let $X = (x_0, \ldots, x_{n-1}) \in F_2^n$.

If $f(x_1, \ldots, x_{n-1}) = 0$, then $T_1X = X$ otherwise $T_2X = X$ and $T_1X \neq X$. So $T_1$ has only fixed points and 2-cycles in its cycle decomposition. Let $\omega(f)$ denote the number of 1’s in the truth table of $f(x_1, \ldots, x_{n-1})$. Then $T_1$ has $2(2^n - \omega(f))$ fixed points and $\omega(f)$ ones 2-cycle in the cycle decomposition of $T_1$. So $T_1$ is even or odd according to whether $\omega(f)$ is even or odd. Since $T_2 = \tau \circ T_1$ and $\tau$ is an even permutation, we have $T_2$ is even or odd according to whether $\omega(f)$ is even or odd. Secondly, since the number of elements in $F_2^n$ is even, by Corollary 4, we can deduce that the number of cycles of $T_2$ is even or odd according to whether $T_2$ is even or odd, and this is according to whether the number of 1’s in the truth table of $f(x_1, \ldots, x_{n-1})$ is even or odd. This completes the proof of Theorem 7.

4. **The case that the coefficients of characteristic polynomial belong to a proper subfield of $F_{2^s}$**

In this section, we mainly give the proof of Theorem 4. First we give a property of the WG permutation.

**Property 1** Let $F_{2^s}$ be a proper subfield of $F_{2^t}$. Then the WG permutation satisfies $WGP(F_{2^s}) \subseteq F_{2^s}$.

**Proof.** Let $a \in F_{2^t}$. Since $F_{2^s}$ is a proper subfield of $F_{2^t}$, $a + 1 \in F_{2^s}$. Then

$$WGP(a) = h(a + 1) + 1 = a + 1 + (a + 1)^{q_1} + (a + 1)^{q_2} + (a + 1)^{q_3} + (a + 1)^{q_4} + 1 \in F_{2^s}.$$

Thus we can have $WGP(F_{2^s}) \subseteq F_{2^s}$. This completes the proof of Property 1.

**Proof of Theorem 4.** Let $(a_0, a_1, \ldots, a_{n-1}) \in F_2^n$ be the initial state of a sequence $\{a_k\}_{k \geq 0}$ generated by the $n$-stage WG-NLFSR. Since all the coefficients of the characteristic polynomial belong to $F_2$, and Property 1, we have

$$a_{n+k} = c_0a_k + c_1a_{k+1} + \cdots + c_{n-1}a_{n+k} + WGP(a_{n-1+k}) \in F_2^n, k \geq 0,$$

If $(a_0, a_1, \ldots, a_{n-1}) = 0$, note that $WGP(0) = 0$, then $a_{n+k} = 0, k \geq 0$, and the period of the zero sequence is 1. If $(a_0, a_1, \ldots, a_{n-1}) \neq 0$, then each state
\( (a_k, a_{k+1}, \ldots, a_{k+n-1}) (k \geq 0) \) generated by the \( n \)-stage WG-NLFSR belongs to \( \mathbb{F}_2^n \) and is not equal to \( 0 \), thus the period of the sequence will be less than or equal to \( 2^{2n} - 1 \). This completes the proof of Theorem 4.

5. The filtering WG7-NLFSR

The filtering WG7-NLFSR is composed of a nonlinear feedback shift register of length 23 and the WG transformation over the finite field \( \mathbb{F}_{2^7} \). The finite field \( \mathbb{F}_{2^7} \) is defined by the primitive polynomial \( t(x) = x^7 + x + 1 \) over \( \mathbb{F}_2 \).

Let \( h(x) = x + x^{33} + x^{39} + x^{41} + x^{104} \) and the WG permutation \( \text{WG7}(x) = h(x + 1) + 1 \). The nonlinear WG permutation with decimation 3, from \( \mathbb{F}_{2^7} \) to \( \mathbb{F}_{2^7} \), is defined by \( \text{WG7}(x^3) = h(x^3 + 1) + 1 \), and the WG transformation over \( \mathbb{F}_{2^7} \) is defined as

\[
\text{WG7}(x) = \text{Tr}(\text{WG7}(x^3)) = \text{Tr}(x^3 + x^9 + x^{21} + x^{57} + x^{87}), x \in \mathbb{F}_{2^7},
\]

where \( \text{Tr}(x) = x + x^2 + x^4 + x^8 + x^{16} + x^{32} + x^{64} \) is the trace mapping from \( \mathbb{F}_{2^7} \) to \( \mathbb{F}_2 \). We denote by \( \{a_i\} \) the sequence generated by the following NLFSR, which is defined as

\[
a_{i+23} = \gamma a_i + a_{i+11} + \text{WG7}(a_{i+22}), a_i \in \mathbb{F}_{2^7},
\]

where \( p(x) = x^{23} + x^{11} + \gamma \) is a primitive polynomial over \( \mathbb{F}_{2^7} \) and \( t(\gamma) = 0 \). A binary filtering WG-NLFSR sequence \( \{s_i\} \) is produced by filtering through the WG transformation \( \text{WG7} \), i.e., \( s_i = \text{WG7}(a_i), i \geq 0 \). The readers can refer to [8] for more details.

Set \( q = 2^3 \). Recall that

\[
T(a_0, a_1, \ldots, a_{22}) = (a_1, a_2, \ldots, a_{22}, \gamma a_0 + a_{11} + \text{WG7}(a_{22})).
\]

In this section, we give some properties of the decomposition of the state transition transformation of WG7-NLFSR.

Lemma 4 The state transition transformation of WG7-NLFSR has only two fixed points and one 2-cycle. One of the two fixed points is zero, and the other one is non-zero. The sum of the two elements in the 2-cycle is equal to the non-zero fixed point.

Proof. If \( T(a_0, a_1, \ldots, a_{22}) = (a_0, a_1, \ldots, a_{22}) \), then \( a_0 = a_1 = \cdots = a_{22} \) and \( a_0 = \gamma a_0 = \text{WG7}(a_0) \). Since \( \text{WG7}(x) = h(x + 1) + 1 \) and \( h(x) = x + x^{33} + x^{39} + x^{41} + x^{104} \), by solving the following equation (6) over \( \mathbb{F}_{2^7} \), we can deduce that \( (0, \cdots, 0, a_0) \) and \( (a_0, \cdots, a_0) \) where \( a_0 = \gamma^6 + \gamma^5 + \gamma^2 + \gamma \) are the fixed points of \( T \). Hence the WG7-NLFSR has only two fixed points.

\[
(6) \quad \gamma x = x + (x + 1)^{33} + (x + 1)^{39} + (x + 1)^{41} + (x + 1)^{104}
\]

Using the similar method, we can deduce that

\[
((0, a_0, 0, a_0, \cdots, 0, a_0, 0), (a_0, 0, a_0, 0, \cdots, a_0, 0, a_0))
\]

is the unique 2-cycle. Since \( (0, a_0, 0, a_0, \cdots, 0, a_0, 0) + (a_0, 0, a_0, 0, \cdots, a_0, 0, a_0) = (a_0, \cdots, a_0) \), the sum of the elements in the 2-cycle is equal to the non-zero fixed point. This completes the proof of Lemma 4.

Theorem 8 The number of cycles in the cycle decomposition of WG7-NLFSR is even and at least 4. The period of the sequences generated by WG7-NLFSR is less than or equal to \( 2^{161} - 4 \).
Proof. First note that WG7-NLFSR is a special case of the WG-NLFSR, the properties of WG-NLFSR are also true for WG7-NLFSR. Hence by Theorem 3, the number of cycles in the cycle decomposition of WG7-NLFSR is even. By Lemma 4, WG7-NLFSR has two fixed points and one 2-cycle, hence there are at least 4 cycles in the cycle decomposition of $T$. And since the number of all states are $(2^7)^{23} = 2^{161}$, the length of the longest cycle in the cycle decomposition of WG7-NLFSR is less than or equal to $2^{161} - 4$. So the period of the sequences generated by WG7-NLFSR is less than or equal to $2^{161} - 4$. This completes the proof of Theorem 8.

Remark 2. In fact we can prove that there are no cycles of length 3, 4, 5, 6, 11 and 12 in the cycle decomposition of WG7-NLFSR at present.

6. Conclusions

In this paper, we give some properties of the cycle decomposition of the WG-NLFSR. In fact, from our proof, one can see that the method to prove Theorem 1 and Theorem 3 can also be used to analyze the parity of any permutation and the number of cycles in the decomposition of any permutation of any finite nonempty set. We hope that it will be useful when we study the nonlinear feedback shift registers.

References

[1] P. B. Bhattacharya, S. K. Jain and S. R. Nagpaul, Basic Abstract Algebra, 2nd Edition, Cambridge University Press, Cambridge, 1994.
[2] U. Cheng, On the cycle structure of certain classes of nonlinear shift registers, Journal of Combinatorial Theory, 37 (1984), 61–68.
[3] H. Dobbertin, Kasami power functions, permutation polynomials and cyclic difference sets, Difference Sets, Sequences and Their Correlation Properties (Bad Windsheim, 1998), NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Kluwer Acad. Publ., Dordrecht, 542 (1999), 133–158.
[4] S. W. Golomb, Shift Register Sequences, Holden-Day, San Francisco, Calif.-Cambridge-Amsterdam, 1967.
[5] G. Gong and A. M. Youssef, Cryptographic properties of the Welch-Gong transformation sequence generators, IEEE Transactions on Information Theory, 48 (2002), 2837–2846.
[6] T. Helleseth, Nonlinear shift registers - A survey and challenges, Algebraic Curves and Finite Fields, Radon Ser. Comput. Appl. Math., De Gruyter, Berlin, 16 (2014), 121–144.
[7] K. Kjeldsen, On the cycle structure of a set of nonlinear shift registers with symmetric feedback functions, Journal of Combinatorial Theory Ser. A, 20 (1976), 154–169.
[8] K. Mandal and G. Gong, Filtering nonlinear feedback shift registers using Welch-Gong transformations for securing RFID applications, ICST Trans. Security Safety, 3 (2016), e3.
[9] J. Mykkeltveit, M. K. Siu and P. Tong, On the cycle structure of some nonlinear shift register sequences, Information and Control, 43 (1979), 202–215.
[10] Z. X. Wan and Z. D. Dai, Nonlinear Feedback Shift Registers, Science Press, Beijing, 1975.

Received December 2018; 1st revision April 2019; final revision September 2019.

E-mail address: liyj@amss.ac.cn
E-mail address: wanghf@mmrc.iss.ac.cn
E-mail address: zhoupeipei08@mails.gucas.ac.cn
E-mail address: zhangguoshuang@iie.ac.cn