Construction for de Bruijn Sequences with Large Orders *

Junwu Dong† Dingyi Pei ‡

Abstract

Sequences generated by maximum-period nonlinear feedback shift registers are known as de Bruijn sequences. The problem of designing de Bruijn sequences has received considerable attention. There is only one full cycle in the state graph of de Bruijn sequences. Most popular algorithms for generating de Bruijn sequences start from a nonsingular linear feedback shift register producing several shorter cycles in its state graph, then join them into one cycle. Unfortunately, the order n of the resulting de Bruijn sequence by using this kind of algorithms is small so far (usually $n \leq 40$). We introduce a new concept of correlated cycles between the cycles in the state graph of a LFSR. Based on this concept we present a algorithm for constructing de Bruijn sequences with large orders (such as $n = 128$). This is the first publication for designing de Bruijn sequences with such large orders.

Keywords de Bruijn sequence, state cycle, period of irreducible polynomial, conjugate states, t-correlated circles.

1 Introduction

Binary n-stage De Bruijn sequences are periodic sequences of period 2^n with every n-tuple of 0, 1 appears precisely once in a period. Since their period reach the maximal value 2^n, they must be nonlinear. de Bruijn proved in [1] that the number of binary n-stage de Bruijn sequences is $2^{2^{n-1}-n}$. Fredricksen gave a well survey in [2].

It has been well studied for many years, see for example [2, 10]. For small stage, all the de Bruijn sequences can be generated. The previous constructions can be divided into two classes:

(1) Constructing the n-stage de Bruijn sequence from two known $(n-1)$-stage de Bruijn sequences. In [3], Lempel provided the concept of D-homomorphism from the n-stage de Bruijn graph to the $(n-1)$-stage de Bruijn graph, the preimage of a $(n-1)$-stage de Bruijn sequence under the D-homomorphism is a pair of cycles C and $\overline{C}$ of length 2^{n-1}, by a pair of conjugate states on C and $\overline{C}$ respectively, one can join C and $\overline{C}$ resulting a n-stage de Bruijn sequence. In [4, 5], the authors consider the further construction of this method for 2-ary and q-ary de Bruijn sequences.

(2) Join cycles. From the state graph of special linear feedback shift register (LFSR), generating all the cycles, finding enough pairs of conjugate states, joining all the cycles, and then getting the de Bruijn sequence. In [6, 7, 8], the authors use this method to construct 2-ary and q-ary de Bruijn sequences.

Yet, the previous construction of de Bruijn sequences mainly based on the de Bruijn graph, depended heavily on the storing and calculating almost all the states of $\mathbb{F}_2^n$, whence can not generate de Bruijn sequences with large order, for example can not generate de Bruijn sequences with order 128.

In this paper, we use the second construction, select suitable polynomial $f(x) \in \mathbb{F}_2[x]$, generating all the cycles of LSFR with the feedback function $f(x)$, finding out enough pairs of conjugate states on distinct cycle, and joining all the cycles to a one full length cycle, i.e., resulting a de Bruijn sequence.

*This work was supported by the National Natural Science Foundation of China under Grant 11371106.

†J. Dong is with the department of mathematics and information Guangzhou university, Guangzhou, 510006, PRC Email: djunwu@163.com

‡D. Pei is with the department of mathematics and information Guangzhou university, Guangzhou, 510006, PRC Email: gztcdpei@scut.edu.cn

Our construction avoid the searching of all the states of $\mathbb{F}_2^n$, without storing all states, therefore can generate large stage de Bruijn sequences, such as $n = 128$.

2 Preliminaries

(1) Feedback Shift Register

The binary feedback shift register (FSR) consists of n storage registers and a feedback logic (a Boolean function $f(x_1, x_2, \cdots, x_n)$, where $x_i \in \mathbb{F}_2 = \{0, 1\}$). When a shift pulse is applied, the state $x = (x_1, x_2, \cdots, x_n)$ of the FSR is succeeded by the state $y = (y_1, y_2, \cdots, y_n)$, where

$$y_i = x_{i+1},\ i = 1, 2, \cdots, n-1,\ \text{and}\ \ y_n = f(x). \tag{1}$$

The Boolean function f is called the feedback function of the FSR. If $f(x_1, x_2, \cdots, x_n) = a_1x_1+a_2x_2+\cdots+a_nx_n$ is linear, the FSR is called linear feedback shift register (LFSR), in this case the feedback function is often expressed by a one indeterminate polynomial $f(x) = 1+a_1x+a_2x^2+\cdots+a_nx^n \in \mathbb{F}_2[x]$. Otherwise, i.e., if the polynomial f is not linear, the FSR is called nonlinear feedback shift register.

By equation (1), the feedback function f induces a mapping $T_f : \mathbb{F}_2^n \to \mathbb{F}_2^n$. The state graph of an FSR with feedback function f, or simply the state graph of f, denoted by G_f, is a direct graph (V, E), where $V = \mathbb{F}_2^n$ and $E = \{(x, y) \,|\, y = T_f(x), x \in V\}$. If the mapping T_f is one-to-one, the FSR or the feedback function f is called nonsingular. It is easy to see that an FSR is nonsingular if and only if its state graph G_f consists of branchless cycles. A cycle of length l (l-cycle) generated by s_0 in G_f, denoted by $< s_0 >$, is a closed sequence of l distinct states $\{s_0, s_1, \cdots, s_{l-1}\}$, such that $T_f(s_{l-1}) = s_0$, and $T_f(s_i) = s_{i+1}$ for $i = 0, 1, 2, \cdots, l-2$.

The following theorem gives the necessary and sufficient condition for an FSR to be nonsingular:

Theorem 2.1. *An FSR is nonsingular if and only if its feedback function $f(x)$ is of the form*

$$f(x_1, x_2, \cdots, x_n) = x_1 + g(x_2, x_3, \cdots, x_n)$$

where $g(x_2, x_3, \cdots, x_n)$ is an arbitrary Boolean function in the $n-1$ variables $x_2, x_3, \cdots, x_n$.

Let $x = (x_1, x_2, \cdots, x_n) \in \mathbb{F}_2^n$, we define $\widehat{x}$, the conjugate of x, by $\widehat{x} = (\overline{x}_1, x_2, \cdots, x_n)$, where $\overline{x}_1 = 1 \oplus x_1$ denotes the Boolean complement of x_1.

Two cycles Z_1 and Z_2 are said to be adjacent if they are disjoint and there exists a state s in Z_1 such that its conjugate state $\widehat{x}$ belongs to Z_2. For a given FSR, we define a relation $\to$ called the shift relation on the state set $\mathbb{F}_2^n$ by $x \to y$ iff $y = T_f(x)$. In the expression $x \to y$, we say that y is a successor of x, and that x is a predecessor of y. The following theorem is well known and we shall use in the sequel.

Theorem 2.2. *Let G_f be the state graph of a nonsingular FSR. If a cycle Z of G_f contains one pair of conjugate states x and $\widehat{x}$, then the cycle Z is split into two adjacent cycles when the successors of the conjugate pair states x and $\widehat{x}$ in Z are interchanged. Two adjacent cycles Z_1 and Z_2 of G_f, with x in Z_1 and $\widehat{x}$ in Z_2 are joined into a single cycle when the successors of x and $\widehat{x}$ are interchanged.*

Moreover, let $f(x_1, x_2, \cdots, x_n)$ be the feedback function of the FSR, and $x = (a_1, a_2, \cdots, a_n)$ and $\widehat{x} = (\overline{a}_1, a_2, \cdots, a_n)$ be the above conjugate pair of states, we define a Boolean function as follows:

$$h(x_1, x_2, \cdots, x_n) = f(x_1, x_2, \cdots, x_n) \oplus x_2^{a_2}x_3^{a_3}\cdots x_n^{a_n}$$

where x_i^1 and x_i^0 denote x_i and $\overline{x}_i$ (i.e., $1 \oplus x_i$), respectively. Then the feedback function of the FSR after interchanging the successors of the conjugate pair of states x and $\widehat{x}$, is $h(x_1, x_2, \cdots, x_n)$.

(2) Polynomial of Matrix.

Let $\mathbb{F} = \mathbb{F}_2 = \{0, 1\}$ be the finite field of order 2 (the following results are also true for general field, in this paper, we are interesting in this binary field), n be an positive integer, and $A = (a_{ij})_{n\times n}$ be a square matrix of order n over $\mathbb{F}$. The matrix A is called invertible if there exists a matrix B such that $AB = BA = I$, where I is the identity matrix.

Let $f(x) = a_0 + a_1x + \cdots + a_sx^s \in \mathbb{F}[x]$, define

$$f(A) = a_0I + a_1A + a_2A^2 + \cdots + a_sA^s.$$

$f(A)$ is called a polynomial matrix of A. Suppose that $f(x)$, $g(x) \in \mathbb{F}[x]$, for any square matrix A of order n, we have that

$$(f+g)(A) = f(A) + g(A), \quad (fg)(A) = f(A)g(A). \tag{2}$$

Given a square matrix A, define a set $\mathbb{F}[A]$ as follows:

$$\mathbb{F}[A] = \{f(A) \,|\, f(x) \in \mathbb{F}[x]\}$$

It is easy to see that $\mathbb{F}[A]$ form a ring under the addition and multiplication of matrix. By equation (2), the map

$$\begin{array}{rccc} \varphi: & \mathbb{F}[x] & \longrightarrow & \mathbb{F}[A] \\ & g(x) & \longmapsto & g(A) \end{array}$$

is a homomorphism from $\mathbb{F}[x]$ onto $\mathbb{F}[A]$.

If $f(x) = 1 + c_1x + c_2x^2 + \cdots + c_nx^n$ is an irreducible polynomial of degree n in $\mathbb{F}[x]$, the matrix

$$T = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & c_n \\ 1 & 0 & 0 & \cdots & 0 & c_{n-1} \\ 0 & 1 & 0 & \cdots & 0 & c_{n-2} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & 0 & 0 & \cdots & 1 & c_1 \end{pmatrix}$$

is called the shift register matrix of $f(x)$. In a LFSR with $f(x)$ as feedback function, if $s_i = (a_i, a_{i+1}, \cdots, a_{i+n-1})$ is a state, then the next state is $s_{i+1} = s_iT$. It is well known that, for any non-zero state $s_0 \in \mathbb{F}_2^n$, the sequence generated by s_0 is period, suppose that the period is l, then the cycle Z generated by s_0 can be represented as follows:

$$Z = < s_0 > = \{s_0, s_0T, s_0T^2, \cdots, s_0T^{l-1}\}.$$

The characteristic polynomial of T is

$$\det(xI - T) = x^n + c_1x^{n-1} + c_2x^{n-2} + \cdots + c_{n-1}x + c_n = x^nf(1/x) = f^*(x),$$

which is the reciprocal polynomial of $f(x)$. By Cayley-Hamilton Theorem, we have that $f^*(T) = 0$.

Since $f(x)$ is irreducible, it is easy to see that $f^*(x)$ is also irreducible. The ideal $J = (f^*(x)) = \{f^*(x)a(x) \,|\, a(x) \in \mathbb{F}[x]\}$ is a maximal ideal in the polynomial ring $\mathbb{F}[x]$. Suppose that θ is a root of $f^*(x)$ in some extension field of $\mathbb{F}$, then we have that $\mathbb{F}[\theta] = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \,|\, a_i \in \mathbb{F}\} \cong \mathbb{F}[x]/J$.

It is easy to see that the zero ideal of T is $\{g(x) \in \mathbb{F}[x] \,|\, g(T) = 0\} = J$, hence $\mathbb{F}[\theta] = \mathbb{F}_2[x]/J \cong \{a_0I + a_1T + a_2T^2 + \cdots + a_{n-1}T^{n-1} \,|\, a_i \in \mathbb{F}\} = \mathbb{F}[T]$, i.e., the ring $\mathbb{F}[\theta]$ and $\mathbb{F}[T]$ are isomorphic. Since $\mathbb{F}[\theta]$ is a field, so does $\mathbb{F}[T]$, whence every non-zero matrix of $\mathbb{F}[T]$ is invertible:

Theorem 2.3. *Suppose that $f(x) \in \mathbb{F}[x]$ is an irreducible polynomial, and T is the shift register matrix of $f(x)$. Then for any $g(x) \in \mathbb{F}[x]$, either $g(T) = 0$ or $g(T)$ is invertible.*

(3) Some Properties on the Reciprocal Polynomial.

Suppose that $f(x) \in \mathbb{F}[x]$ is a polynomial of degree n, we call $f^*(x) = x^nf(1/x)$ the reciprocal polynomial of $f(x)$. If $f^*(x) = f(x)$, then, $f(x)$ is called the auto-reciprocal polynomial. The following properties of reciprocal polynomials are useful:

Lemma 2.1. *If $f(x)|g(x)$, then $f^*(x)|g^*(x)$.*

Lemma 2.2. *Suppose that $f(x)|g(x)$, and $g(x)$ is auto-reciprocal, then $f^*(x)|g(x)$.*

Lemma 2.3. *If $f(x)$ is irreducible, then $f^*(x)$ is irreducible too, and conversely.*

(4) Some results on finite cyclic group.

Let $G =< a >$ be a cyclic group of order n, i.e., $G = \{1, a, a^2, \cdots, a^{n-1}\}$ with $a^n = 1$, where the identity element of G is denoted by 1. The following are useful:

Theorem 2.4. *Suppose G is a cyclic group of order n, and H is a subgroup of G, then H is also a cyclic group, and the order of H is a divisor of n.*

Theorem 2.5. *Suppose that G is a cyclic group of order n, and l is a divisor of n, then there exists only one subgroup H of G with order l.*

Theorem 2.6. *Suppose that G is a cyclic group of order n, and H is the subgroup of order l, then for every $b \in G$, the necessary and sufficient condition for b in H is that $b^l = 1$.*

Theorem 2.7. *Let $\mathbb{F}_q$ be a finite field, with q a prime power, then the set $\mathbb{F}_q^*$ of all nonzero elements of $\mathbb{F}_q$ form a cyclic group of order $q-1$ under the multiplication of $\mathbb{F}_q$.*

(5) The basic theory of LFSR.

Let n be a positive integer, and $f(x)$ be an irreducible polynomial of degree n in $\mathbb{F}_2[x]$. The period of $f(x)$ is defined to be the smallest positive integer l such that $f(x)|x^l + 1$. It is known that $l|2^n - 1$. Let $k = (2^n - 1)/l$. The state graph of the LFSR, whose feedback function is $f(x)$, consists of $k + 1$ cycles, one of which is the 1-cycle generated by the zero state (called zero cycle), and the other k cycles have the same length l.

Let T denote the shift register matrix of $f(x)$. If the period of $f(x)$ is l, then, l is the smallest positive integer such that $f(x)|x^l - 1$. Therefore $f^*(x)|x^l - 1$, we have $T^l = I$, i.e., the order of the matrix T is l. The group $< T >$ is the unique subgroup with order l in the multiplicative group $\mathbb{F}_2^*(\theta)$.

If $k = 1$, then $l = 2^n - 1$, and $f(x)$ is a primitive polynomial, the sequence generated by $f(x)$ is m-sequence. It is trivial to join the zero cycle and the $(2^n - 1)$-cycle, resulting a de Bruijn sequence. In the sequel, we always assume that $k > 1$.

The zero cycle $< 0 >$ and the cycle $< 1 >$ can be joined into one cycle by the conjugate states $s = 0 = (0, 0, \cdots, 0)$ and $\widehat{s} = 1 = (1, 0, \cdots, 0)$. From now on, we just consider all the k cycles of length l, which is denoted by $G(f)$.

Suppose that Z_1 and Z_2 are two l-cycles generated by s_0 and t_0 respectively,

$$Z_1 =< s_0 >= \{s_0, s_1, s_2, \cdots, s_{l-1}\}$$
$$Z_2 =< t_0 >= \{t_0, t_1, t_2, \cdots, t_{l-1}\}$$

If $s_0 \in Z_2$, then Z_1 and Z_2 are the same cycle.

3 The t-Correlated Cycles of $f(x)$

Let n and l be positive integers with $l|2^n - 1$, and let $k = (2^n - 1)/l$, $f(x)$ be an irreducible polynomial of degree n with period l. In order to generate all the cycles of $G(f)$ and find the conjugate pairs of states over different cycles, we introduce the following definition:

Definition 3.1. *Let n, $f(x)$, l, k be as above, T be the shift register matrix of $f(x)$, and $Z =< s_0 >$ be a cycle of $G(f)$ generated by s_0:*

$$Z =< s_0 >= \{s_0, s_0T, s_0T^2, \cdots, s_0T^{l-1}\} \in G(f).$$

Let t be a integer with $0 < t < l$, the 1th t-correlated cycle of Z, denoted by $D_{f,t}^{(1)}(Z)$, is the cycle generated by $s_0 \oplus s_0T^t$ (the symbol $\oplus$ denotes the addition of two points in $\mathbb{F}_2^n$), i.e.,

$$D_{f,t}^{(1)}(Z) =< s_0(I + T^t) >= \{s_0(I + T^t), s_0(I + T^t)T, s_0(I + T^t)T^2, \cdots, s_0(I + T^t)T^{l-1}\} \quad (3)$$

More generally, for any positive integer m, we define the mth t-correlated cycle of Z is the cycle generated by $s_0(I + T^t)^m$, and denote it by $D_{f,t}^{(m)}(Z)$. We call t the width of the correlated cycles. We regard $D_{f,t}^{(0)}(Z)$ as Z.

Definition 3.2. *Let $f(x)$, l be as above, and $0 < t < l$, m be a positive integer. The polynomial $h_{t,m}(x) = (1 + x^t)^m$ is called mth t-correlated polynomial.*

It is clear that the generated state of the mth t-correlated cycle $D^{(1)}_{f,t}(Z)$ of the cycle $Z =< s_0 >$ is $s_0 h_{t,m}(T)$.

We have the following properties about the t-correlated cycles.

Lemma 3.1. *Suppose that $f(x)$ is an irreducible polynomial of degree n with period l. For any positive integer t with $0 < t < l$, and m, the following map defined by the mth t-correlated cycle $D^{(m)}_{f,t}(Z)$:*

$$\begin{array}{rccc} \psi: & G(f) & \longrightarrow & G(f) \\ & Z & \longmapsto & D^{(m)}_{f,t}(Z) \end{array}$$

is a bijective map.

Proof. It is enough to prove the assertion for the case $m = 1$, since the product of two bijective maps is again a bijective map, and the mth t-correlated cycle can be regarded as the product of m 1th t-correlated cycles.

For every $Z \in G(f)$, and for every $0 < t < l$, the t-correlated cycle of Z $D^{(1)}_{f,t}(Z)$ is not the zero cycle, hence $D^{(1)}_{f,t}(Z) \in G(f)$, which means that ψ is a map from $G(f)$ to $G(f)$. As $G(f)$ is a finite set of k elements, it is enough to prove that ψ is injective, i.e., if $\psi(Z_1) = \psi(Z_2)$ implies $Z_1 = Z_2$ for any Z_1, $Z_2 \in G(f)$.

For any Z_1, $Z_2 \in G(f)$, generated by s_0 and u_0 respectively,

$$\begin{aligned} Z_1 =& \{s_0, s_1, s_2, \cdots, s_{l-1}\} \\ Z_2 =& \{u_0, u_1, u_2, \cdots, u_{l-1}\} \end{aligned}$$

where $s_i = s_0 T^i$, and $u_i = u_0 T^i$. If $D^{(1)}_{f,t}(Z_1) = D^{(1)}_{f,t}(Z_2)$, then there exists an integer i with $0 \le i < l$, such that $s_0 \oplus s_t = u_i \oplus u_{i+t}$, therefore, we have

$$s_j \oplus s_{j+t} = u_{i+j \pmod l} \oplus u_{i+j+t \pmod l}, \quad j = 0, 1, 2, \cdots, l-1 \tag{4}$$

let $v_j = s_j \oplus u_{i+j \pmod l}$, $(j = 0,\ 1,\ 2,\ \cdots,\ l-1)$, then the cycle generated by v_0

$$< v_0 >= \{v_0, v_1, v_2, \cdots, v_{l-1}\}$$

is also a cycle of $f(x)$. From (4), we have that $v_0 = v_t$. Since $0 < t < l$, v_0 and v_t lie in the same cycle, whence $< v_0 >$ is the zero cycle, i.e., $v_0 = v_1 = \cdots = v_{l-1} = 0$. So, we have $s_j = u_{i+j \pmod l}$ for all $j = 0,\ 1,\ 2,\ \cdots,\ l-1$, and hence $Z_1 = Z_2$, which means that ψ is injective. □

Lemma 3.2. *Suppose that $0 < t < l$. For any $Z \in G(f)$, there exists a positive integer d, such that $D^{(d)}_{f,t}(Z) = Z$.*

Proof. For any $Z \in G(f)$, we consider the following sequence:

$$Z = D^{(0)}_{f,t}(Z),\ D^{(1)}_{f,t}(Z),\ D^{(2)}_{f,t}(Z),\ \cdots,$$

Since $G(f)$ is a finite set, and $D^{(j)}_{f,t}(Z) \in G(f)$ for every $j = 0,\ 1,\ 2,\ \cdots$, there must exist two integer $0 \le i < j$ such that $D^{(i)}_{f,t}(Z) = D^{(j)}_{f,t}(Z)$. Let i_0 be the smallest integer satisfying the condition that there exists $d > i_0$ such that $D^{(i_0)}_{f,t}(Z) = D^{(d)}_{f,t}(Z)$, then we have $i_0 = 0$. Otherwise, we have $\psi(D^{(d-1)}_{f,t}(Z)) = D^{(d)}_{f,t}(Z) = D^{(i_0)}_{f,t}(Z) = \psi(D^{(i_0-1)}_{f,t}(Z))$, by Lemma 3.1, we get that $D^{(i_0-1)}_{f,t}(Z) = D^{(d-1)}_{f,t}(Z)$, which contradict with the minimality of i_0. Therefore, there exists an integer d such that $D^{(d)}_{f,t}(Z) = D^{(0)}_{f,t}(Z) = Z$, which completes the assertion. □

The following theorem shows that all the cycles $Z \in G(f)$ have the same value d.

Theorem 3.1. *Suppose $0 < t < l$. For every cycle $Z \in G(f)$, $D_{f,t}^{(d)}(Z) = Z$ if and only if*

$$h_{t,d}(x)^l \equiv 1 \pmod{f(x)}. \tag{5}$$

Proof. Suppose that $(h_{t,d}(x))^l = (1+x^t)^{dl} \equiv 1 \pmod{f(x)}$ holds, then $f(x)|(1+x^t)^{dl}-1$. Take $g(x) = (1+x^t)^{dl} - 1 - (x^{tdl}-1) = (1+x^t)^{dl} - x^{tdl}$. Since $f(x)|g(x)$, and $g^*(x) = (1+x^t)^{dl}-1$, by Lemma 2.1, we have

$$f^*(x)|(1+x^t)^{dl} - 1. \tag{6}$$

Since $f^*(T) = 0$, by (6), we have $(I+T^t)^{dl} = I$, whence $(I+T^t)^d \in < T >$, by Theorem 2.6. So, there exists a positive integer $0 \le i < l$, such that $h_{t,d}(T) = (I+T^t)^d = T^i$.

Let $Z =< s_0 >$ be any cycle of $G(f)$, where s_0 is a non-zero vector of $\mathbb{F}_2^n$, the initial state of the dth t-correlated cycle $D_{f,t}^{(d)}(Z)$ is $s_0^{(d)} = s_0 h_{t,d}(T) = s_0 T^i$, which means that $D_{f,t}^{(d)}(Z) = Z$.

Conversely, suppose that $Z =< s_0 >$ is a cycle of $G(f)$, such that $D_{f,t}^{(d)}(Z) = Z$. The initial state $s_0^{(d)} = s_0 h_{t,d}(T)$ of $D_{f,t}^{(d)}(Z)$ is in Z, then there exists an integer $0 \le i < l$ such that $s_0^{(d)} = s_0 T^i$, therefore, $s_0(h_{t,d}(T) - T^i) = 0$. Since $s_0 \neq 0$, by Theorem 2.3, we have $h_{t,d}(T) = T^i$, i.e., $(h_{t,d}(x))^l \equiv 1 \pmod{f^*(x)}$. By using the same way as above we can prove the assertion. □

So all the cycles Z in $G(f)$ have the same value d such that $D_{f,t}^{(d)}(Z) = Z$, the smallest positive integer d_t is called the t-correlated order of $f(x)$, and we denote it by $d_t = \mathrm{Ord}_t(f)$.

Two cycles Z_1 and Z_2 in $G(f)$ are called t-correlated, if there exists an integer i such that $Z_2 = D_{f,t}^{(i)}(Z_1)$. It is easy to see that this defines an equivalent relation in $G(f)$, each equivalent class has $d_t = \mathrm{Ord}_t(f)$ cycles. Since $G(f)$ has k cycles, we have thus proved the following corollary:

Corollary 3.1. *Suppose that $f(x)$, k, t are as above, then $\mathrm{Ord}_t(f)|k$.*

If k is a prime number, and $f(x)$ is an irreducible polynomial of degree n with period $l = (2^n-1)/k$, then for the integer $0 < t < l$ with $\mathrm{Ord}_t(f) \neq 1$, $\mathrm{Ord}_t(f)$ must be k. In this special case we can obtain all the cycles of $G(f)$ from any selected cycle Z from $G(f)$ by t-correlated cycles:

$$G(f) = \{Z = D_{f,t}^{(0)}(Z),\ D_{f,t}^{(1)}(Z),\ D_{f,t}^{(2)}(Z),\ \cdots,\ D_{f,t}^{(k-1)}(Z)\}.$$

4 Conjugate State Pair

Let n, k be positive integers such that $k|2^n-1$, and $f(x)$ be an irreducible polynomial in $\mathbb{F}_2[x]$ of degree n with period $l = (2^n-1)/k$. Let t be an positive integer with $0 < t < l$, such that $\mathrm{Ord}_t(f) = d > 1$, it is the same thing that $(1+x^t)^l \not\equiv 1 \pmod{f(x)}$, by Theorem 3.1. The set $G(f)$ is divided into k/d t-correlated classes, each of which has exactly d cycles. Now, we select a special state $\alpha_0 = 1 = (1, 0, 0, \cdots, 0)$, the cycle generated by α_0 is denoted by Z_0:

$$Z_0 = \{\alpha_0 = 1, \alpha_0 T, \alpha_0 T^2, \cdots, \alpha_0 T^{l-1}\}.$$

We are going to find the conjugate pairs of states that lie on Z_0 and the other cycles (which are belonged in the t-correlated class of Z_0) respectively.

Note that the mth t-correlated polynomial is $h_{t,m}(x) = (1+x^t)^m \in \mathbb{F}_2[x]$, then, for every $j = 0, 1, 2, \cdots$, the 2^jth t-correlated polynomial has the following special form:

$$h_{t,2^j}(x) = (1+x^t)^{2^j} = 1 + (x^t)^{2^j}.$$

The initial state of the 2^jth t-correlated cycle of Z_0 is

$$s = \alpha_0 h_{t,2^j}(T) = \alpha_0(1 + (T^t)^{2^j \pmod l}) = \alpha_0 \oplus \alpha_0 (T^t)^{2^j \pmod l} = 1 \oplus \alpha_{2^j t \pmod l},$$

the conjugate state $\widehat{s}$ of s is $\alpha_{2^j t \pmod l}$, thus, the conjugate pair of states $(s, \widehat{s})$ lies in two different state cycles of $G(f)$, where the state $\widehat{s}$ lies in the cycle Z_0, while the state s lies in the 2^jth t-correlated cycle $D_{f,t}^{(2^j)}(Z_0)$ of Z_0. By the corollary of theorem 3.1, $d|k$, so d is odd since k is odd, and $2^j \not\equiv 0 \pmod d$, this means that Z_0 and $D_{f,t}^{(2^j)}(Z_0)$ are different cycles in $G(f)$. By theorem 2.2, the conjugate pair of states s and s^* can join the cycles Z_0 and $D_{f,t}^{(2^j)}(Z_0)$ into one cycle.

Let r be the order of 2 mod $d = \mathrm{Ord}_t(f)$, i.e., r is the smallest positive integer such that $2^r \equiv 1 \pmod d$. The above method can join the cycle Z_0 with the following r distinct cycles:

$$\left\{D_{f,t}^{(2^0 \bmod d)}(Z_0), D_{f,t}^{(2^1 \bmod d)}(Z_0), D_{f,t}^{(2^2 \bmod d)}(Z_0), \cdots, D_{f,t}^{(2^{r-1} \bmod d)}(Z_0)\right\}. \tag{7}$$

If $r+1 = d$, then all the cycles in the t-correlated class of Z_0 can be joined into one cycle. Furthermore, if k is a prime number, and 2 is a primitive root mod k, then there is only one t-correlated class in $G(f)$, whence all the cycles of $G(f)$ can be joined into one full length cycle. However, if $r+1 \neq \mathrm{Ord}_t(f)$, this method can not join all the cycles in $G(f)$. To solve this problem, we study the relation of different t-correlated classes.

For any two elements a, $b \in \mathbb{Z}_l = \{0, 1, 2, \cdots, l-1\}$, we call a and b are conjugate mod l if there exists an integer j such that $b \equiv 2^j a \pmod l$. It is easy to see that it is an equivalent relation. Then the set $\mathbb{Z}_l$ are partitioned into several disjoint conjugate classes. For any $t \in \mathbb{Z}_l$, the conjugate class containing t is denoted by $[t]$, the class $[0]$ contains only the element 0. In the following, when we speak of class $[t]$, we always mean that $t \neq 0$. The conjugate class $[t]$ contains the following elements:

$$[t] = \{t, 2t \pmod l, 2^2 t \pmod l, \cdots, 2^{\gamma_t - 1} t \pmod l\},$$

where γ_t is a smallest positive integer such that $2^{\gamma_t} t \equiv t \pmod l$, γ_t is called the conjugate order of t mod l.

Let Z_0 denote the cycle of $G(f)$ generated by the state $\alpha_0 = (1, 0, \cdots, 0)$. Furthermore, we suppose that $d_t = \mathrm{Ord}_t(f) > 1$. Then, the cycle Z_0 has conjugate pairs of states with the following t-correlated cycles:

$$\Omega_t(Z_0) = \left\{D_{f,t}^{(2^0)}(Z_0), D_{f,t}^{(2^1)}(Z_0), \cdots, D_{f,t}^{(2^{\gamma_t - 1})}(Z_0)\right\}$$

In fact, the set $\Omega_t(Z_0)$ has exactly r_t cycles, where r_t is the order of 2 mod $d_t = \mathrm{Ord}_t(f)$. The set $\Omega_t(Z_0)$ coincides with the set of (7). By lemma 4.1 below, we will prove $r_t|\gamma_t$, the cycle Z_0 has γ_t/r_t pairs of conjugate states with each cycle of $\Omega_t(Z_0)$, so there are $(r_t)^{\gamma_t/r_t}$ ways to join the cycle Z_0 with all the cycles of $\Omega_t(Z_0)$.

Lemma 4.1. *Suppose that $0 < t < l$, be an integer such that $d_t = \mathrm{Ord}_t(f) > 1$, let γ_t be the conjugate order of t mod l, and r_t is the order of 2 mod d_t, then $r_t|\gamma_t$.*

Proof. Let D be an integer, it is easy to see that the equation $(1+x^t)^{Dl} \equiv 1 \pmod{f(x)}$ holds if and only if $d_t|D$, by Theorem 3.1. By the assumption that $2^{\gamma_t} t \equiv t \pmod l$, we have that $D_{f,t}^{(2^{\gamma_t})}(Z) = D_{f,t}^{(1)}(Z)$, where Z is any cycle of $G(Z)$. By lemma 3.1, we have that $D_{f,t}^{(2^{\gamma_t}-1)}(Z) = D_{f,t}^{(0)}(Z) = Z$, hence we obtain that,

$$2^{\gamma_t} \equiv 1 \pmod{d_t},$$

which completes the proof. □

Theorem 4.1. *For any two integers $1 \leq t_1, t_2 < l$, if $\Omega_{t_1}(Z_0)$ and $\Omega_{t_2}(Z_0)$ have a common element, then $\Omega_{t_1}(Z_0) = \Omega_{t_2}(Z_0)$.*

Proof. Let γ_1 and γ_2 be the conjugate order of t_1 and t_2 mod l respectively. By the assumption, there exists two integer i and j, with $0 \leq i < \gamma_1$ and $0 \leq j < \gamma_2$, such that $D_{f,t_1}^{(2^i)}(Z_0) = D_{f,t_2}^{(2^j)}(Z_0)$. The initial state $\alpha_0(1+T^{t_1})^{2^i}$ of $D_{f,t_1}^{(2^i)}(Z)$ is in the cycle $D_{f,t_2}^{(2^j)}(Z)$, there exists an integer u, with $0 \leq u < l$, such that

$$\alpha_0(1+T^{t_1})^{2^i} = \alpha_0(1+T^{t_2})^{2^j} T^u.$$

Since α_0 is not the zero state, and by theorem 2.3, we have that

$$(1+x^{t_1})^{2^i} \equiv (1+x^{t_2})^{2^j} x^u \pmod{f^*(x)}.$$

By taking $2^{\gamma_1 - i}$th powers on both sides, we have

$$(1+x^{t_1})^{2^{\gamma_1}} \equiv (1+x^{t_2})^{2^{j'}} x^{2^{j'}u} \pmod{f^*(x)}$$

where $j' = j + \gamma_1 - i \pmod{\gamma_2}$. Furthermore, by taking lth power on both sides, and noting that $x^l \equiv 1 \pmod{f^*(x)}$, and $(1+x^{t_1})^{2^{\gamma_1}} \equiv (1+x^{t_1}) \pmod{f^*(x)}$, we get that

$$(1+x^{t_1})^l \equiv (1+x^{t_2})^{2^{j'}l} \pmod{f^*(x)}. \tag{8}$$

Finally, by squaring on both sides of (8) step by step, we have that

$$(1+x^{t_1})^{2^i l} \equiv (1+x^{t_2})^{2^{j'+i}l} \pmod{f^*(x)}$$

So, we have proved that $D_{f,t_1}^{(2^i)}(Z_0) = D_{f,t_2}^{(2^{j'+i})}(Z_0)$ for $i = 1, 2, \cdots$, i.e., $\Omega_{t_1}(Z_0) \subset \Omega_{t_2}(Z_0)$. By the same way, we can prove that $\Omega_{t_2}(Z_0) \subset \Omega_{t_1}(Z_0)$, and the lemma is proved. □

Corollary 4.1. *Suppose that t_1 is conjugate with t_2 mod l, then $\Omega_{t_1}(Z_0) = \Omega_{t_2}(Z_0)$.*

Proof. By assumption, there exists an integer i, such that $t_1 \equiv 2^i t_2 \pmod{l}$, so that $T^{t_1} = T^{2^i t_2}$, and $\alpha_0(I+T^{t_1}) = \alpha_0(I+T^{t_2})^{2^i}$. Therefore, we have that $D_{f,t_1}^{(1)}(Z) =< \alpha_0(I+T^{t_1}) >=< \alpha_0(1+T^{t_2})^{2^i} >= D_{f,t_2}^{(2^i)}(Z) \in \Omega_{t_1}(Z) \cap \Omega_{t_2}(Z)$, by the Theorem 4.1, the corollary is proved. □

Corollary 4.2. *Let t_1 and t_2 be integers with $0 < t_1, t_2 < l$, and let γ_1 and γ_2 be the conjugate orders of t_1 and t_2 mod l respectively, then $\Omega_{t_1}(Z_0) = \Omega_{t_2}(Z_0)$ if and only if there exists an integer j with $0 \le j < \gamma_2$, such that*

$$(1+x^{t_1})^l \equiv (1+x^{t_2})^{2^j l} \pmod{f(x)} \tag{9}$$

Proof. If $\Omega_{t_1}(Z_0) = \Omega_{t_2}(Z_0)$, then there exists an integer j with $0 \le j < \gamma_2$, satisfying the equation (8). By using the properties of auto-reciprocal polynomial, it is easy to check that the equation (9) is also true.

Conversely, if the equation (9) holds, by the same way, we can prove that the equation (8) is true. By repeating the proof of Theorem 4.1, we can prove that $\Omega_{t_1}(Z_0) \cap \Omega_{t_2}(Z_0) \neq \emptyset$, hence $\Omega_{t_1}(Z_0) = \Omega_{t_2}(Z_0)$. □

The following example shows that when using different t_1 and t_2, both $\Omega_{t_1}(Z) = \Omega_{t_2}(Z)$ and $\Omega_{t_1}(Z) \cap \Omega_{t_2}(Z) = \emptyset$ can be happened.

Example 1. Let $n = 9$, then $2^9 - 1 = 7 \cdot 73$, let $k = 7$, so $l = (2^9-1)/k = 73$. It is easy to check that $f(x) = x^9 + x^8 + 1$ is an irreducible polynomial of degree 9 with period $l = 73$. There are 8 conjugate classes mod l in $\mathbb{Z}_l$ as follows: [1], [3], [5], [9], [11], [13], [17], and [25]. By equation (5), we can check that if $t \in [1] \cup [9]$, the corresponding t-correlated order of $f(x)$ is $d_t = \mathrm{Ord}_t(f) = 1$, while the corresponding of the t-correlated order of $f(x)$ is $d_t = \mathrm{Ord}_t(f) = 7$ for all t belong to all other 6 conjugate classes.

Let $\alpha_0 = (1, 0, 0, \cdots, 0)$, and $Z_0 =< \alpha_0 >$. Since $d_2 = \mathrm{Ord}_3(f) = 7 = k$, then we have

$$G(f) = \left\{ Z_0, D_{f,3}^{(1)}(Z_0), D_{f,3}^{(2)}(Z_0), D_{f,3}^{(3)}(Z_0), D_{f,3}^{(4)}(Z_0), D_{f,3}^{(5)}(Z_0), D_{f,3}^{(6)}(Z_0) \right\}$$

For simplicity, $D_{f,3}^{(j)}(Z_0)$ is denoted by Z_j for $j = 1, 2, \cdots, 6$, that is, $G(f) = \{Z_0, Z_1, Z_2, Z_3, Z_4, Z_5, Z_6\}$. We list all the cycles of $G(f)$ below (the state $(x_1, x_2, \cdots, x_9)$ is represented by the hexadecimal form of the integer $x_1 + 2x_2 + x^2x_3 + \cdots + 2^8 x_9$).

We will show that $\Omega_3(Z_0) = \Omega_5(Z_0)$, and $\Omega_3(Z_0) \cap \Omega_{11}(Z_0) = \emptyset$.

It is easy to check that the order r_3 of 2 mod $d_3 = 7$ is 3, so that

$$\Omega_3(Z_0) = \left\{D_{f,3}^{(2^0)}(Z_0), D_{f,3}^{(2^1)}(Z_0), D_{f,3}^{(2^2)}(Z_0)\right\} = \{Z_1, Z_2, Z_4\}.$$

If we take $t_2 = 5$, by calculating, it is easy to check that $(1 + x^3)^l \equiv (1 + x^5)^{2 \cdot l} \pmod{f(x)}$, so $\Omega_3(Z_0) = \Omega_5(Z_0)$ by corollary 4.2. In fact, we can check that $1 \oplus \alpha_5 = 011 \in Z_4$, which means that $D_{f,5}^{(2^0)}(Z_0) = Z_4 \in \Omega_3(Z_0)$, and that $1 \oplus \alpha_{10} = 181 \in Z_1$, which means that $D_{f,5}^{(2^1)}(Z_0) = Z_1 \in \Omega_3(Z_0)$, and that $1 \oplus \alpha_{20} = 0a1 \in Z_2$, which means that $D_{f,5}^{(2^2)}(Z_0) = Z_2 \in \Omega_3(Z_0)$.

Finally, we consider $t_3 = 11$. By calculation, we can check that for every $j = 0, 1, \cdots, 8$, $(1+x^3)^l \not\equiv (1+x^{11})^{2^j \cdot l} \pmod{f(x)}$, thus $\Omega_3(Z_0) \cap \Omega_{11}(Z_0) = \emptyset$ by corollary 4.2, whence $\Omega_{11}(Z_0) = \{Z_3, Z_5, Z_6\}$. In fact, we can check that $1 \oplus \alpha_{11} = 0c1 \in Z_6$, which means that $D_{f,11}^{(2^0)}(Z_0) = Z_6$, and that $1 \oplus \alpha_{22} = 029 \in Z_5$, means that $D_{f,11}^{(2^1)}(Z_0) = Z_5$, and that $1 \oplus \alpha_{44} = 063 \in Z_3$, means that $D_{f,11}^{(2^2)}(Z_0) = Z_3$.

$Z_0 =$ 001, 100, 080, 040, 020, 010, 008, 004, 002, 101, 180, 0c0, 060, 030, 018, 00c, 006, 103, 081, 140, 0a0, 050, 028, 014, 00a, 105, 182, 1c1, 1e0, 0f0, 078, 03c, 01e, 10f, 087, 043, 021, 110, 088, 044, 022, 111, 188, 0c4, 062, 131, 198, 0cc, 066, 133, 099, 14c, 0a6, 153, 0a9, 154, 0aa, 155, 1aa, 1d5, 1ea, 1f5, 1fa, 1fd, 1fe, 1ff, 0ff, 07f, 03f, 01f, 00f, 007, 003

$Z_1 =$ 041, 120, 090, 048, 024, 012, 109, 184, 0c2, 161, 1b0, 0d8, 06c, 036, 11b, 08d, 146, 1a3, 0d1, 168, 0b4, 05a, 12d, 196, 1cb, 0e5, 172, 1b9, 1dc, 0ee, 177, 0bb, 05d, 12e, 197, 0cb, 065, 132, 199, 1cc, 0e6, 173, 0b9, 15c, 0ae, 157, 0ab, 055, 12a, 195, 1ca, 1e5, 1f2, 1f9, 1fc, 0fe, 17f, 0bf, 05f, 02f, 017, 00b, 005, 102, 181, 1c0, 0e0, 070, 038, 01c, 00e, 107, 083

$Z_2 =$ 009, 104, 082, 141, 1a0, 0d0, 068, 034, 01a, 10d, 186, 1c3, 0e1, 170, 0b8, 05c, 02e, 117, 08b, 045, 122, 191, 1c8, 0e4, 072, 139, 19c, 0ce, 167, 0b3, 059, 12c, 096, 14b, 0a5, 152, 1a9, 1d4, 0ea, 175, 1ba, 1dd, 1ee, 1f7, 0fb, 07d, 13e, 19f, 0cf, 067, 033, 019, 10c, 086, 143, 0a1, 150, 0a8, 054, 02a, 115, 18a, 1c5, 1e2, 1f1, 1f8, 0fc, 07e, 13f, 09f, 04f, 027, 013

$Z_3 =$ 148, 0a4, 052, 129, 194, 0ca, 165, 1b2, 1d9, 1ec, 0f6, 17b, 0bd, 15e, 1af, 0d7, 06b, 035, 11a, 18d, 1c6, 1e3, 0f1, 178, 0bc, 05e, 12f, 097, 04b, 025, 112, 189, 1c4, 0e2, 171, 1b8, 0dc, 06e, 137, 09b, 04d, 126, 193, 0c9, 164, 0b2, 159, 1ac, 0d6, 16b, 0b5, 15a, 1ad, 1d6, 1eb, 0f5, 17a, 1bd, 1de, 1ef, 0f7, 07b, 03d, 11e, 18f, 0c7, 063, 031, 118, 08c, 046, 123, 091

$Z_4 =$ 061, 130, 098, 04c, 026, 113, 089, 144, 0a2, 151, 1a8, 0d4, 06a, 135, 19a, 1cd, 1e6, 1f3, 0f9, 17c, 0be, 15f, 0af, 057, 02b, 015, 10a, 185, 1c2, 1e1, 1f0, 0f8, 07c, 03e, 11f, 08f, 047, 023, 011, 108, 084, 042, 121, 190, 0c8, 064, 032, 119, 18c, 0c6, 163, 0b1, 158, 0ac, 056, 12b, 095, 14a, 1a5, 1d2, 1e9, 1f4, 0fa, 17d, 1be, 1df, 0ef, 077, 03b, 01d, 10e, 187, 0c3

$Z_5 =$ 02d, 116, 18b, 0c5, 162, 1b1, 1d8, 0ec, 076, 13b, 09d, 14e, 1a7, 0d3, 069, 134, 09a, 14d, 1a6, 1d3, 0e9, 174, 0ba, 15d, 1ae, 1d7, 0eb, 075, 13a, 19d, 1ce, 1e7, 0f3, 079, 13c, 09e, 14f, 0a7, 053, 029, 114, 08a, 145, 1a2, 1d1, 1e8, 0f4, 07a, 13d, 19e, 1cf, 0e7, 073, 039, 11c, 08e, 147, 0a3, 051, 128, 094, 04a, 125, 192, 1c9, 1e4, 0f2, 179, 1bc, 0de, 16f, 0b7, 05b

$Z_6 =$ 0e8, 074, 03a, 11d, 18e, 1c7, 0e3, 071, 138, 09c, 04e, 127, 093, 049, 124, 092, 149, 1a4, 0d2, 169, 1b4, 0da, 16d, 1b6, 1db, 0ed, 176, 1bb, 0dd, 16e, 1b7, 0db, 06d, 136, 19b, 0cd, 166, 1b3, 0d9, 16c, 0b6, 15b, 0ad, 156, 1ab, 0d5, 16a, 1b5, 1da, 1ed, 1f6, 1fb, 0fd, 17e, 1bf, 0df, 06f, 037, 01b, 00d, 106, 183, 0c1, 160, 0b0, 058, 02c, 016, 10b, 085, 142, 1a1, 1d0

5 The Choice of Polynomial

Given the positive integer n and k such that $k|2^n - 1$, let $l = (2^n - 1)/k$, the following lemma shows the condition that the irreducible polynomial $f(x)$ of degree n with period l exists.

Lemma 5.1. *Let n, k and l be as above, then, the necessary and sufficient condition that there exists an irreducible polynomial $f(x)$ of degree n with period l is that the order of 2 mod l is n.*

Proof. Suppose that $f(x)$ is an irreducible polynomial of degree n with period l, let β be a root of $f(x)$, we obtain a finite field $\mathbb{F}_{2^n} = \mathbb{F}_2[\beta]$. The order of β in the multiplicative group of all non-zero elements of $\mathbb{F}_{2^n}$ is l, i.e., l is the smallest positive integer such that $\beta^l = 1$. Since $f(x)$ is an irreducible polynomial, it has n distinct roots in $\mathbb{F}_{2^n}$, as following:

$$\{\beta, \beta^2, \beta^{2^2}, \cdots, \beta^{2^{n-1}}\}. \tag{10}$$

Since $l|2^n - 1$, we have that $2^n \equiv 1 \pmod{l}$. On the other hand, if the order s of 2 mod l is less than n, i.e., $s < n$, then, we have that $l|2^s - 1$, so that $\beta^{2^s} = \beta$, which contradicts with (10).

Conversely, let β be an element of order l in the finite field $\mathbb{F}_{2^n}$. Since the order of 2 mod l is n, the following elements

$$1, 2 \bmod l, 2^2 \bmod l, \cdots, 2^{n-1} \bmod l$$

are distinct, so that

$$\beta, \beta^2, \beta^{2^2}, \cdots, \beta^{2^{n-1}}$$

are distinct too. Let $f(x)$ be the minimal polynomial of β, then

$$f(x) = \prod_{i=0}^{n-1} (x - \beta^{2^i})$$

is an irreducible polynomial of degree n. The period of $f(x)$ is equal to the order l of β, and the assertion is proved. □

For the given positive integers n, k, and l, such that $l = (2^n - 1)/k$, and the order of 2 mod l is n, there are exactly $\varphi(l)$ elements of order l in the finite field $\mathbb{F}_{2^n}$, where $\varphi(\cdot)$ is the Euler function. The set of all elements of order l can be divided into $\varphi(l)/n$ conjugate classes, each class corresponds with an irreducible polynomial of degree n with period l respectively, so, there are $\varphi(l)/n$ irreducible polynomials of degree n with period l. For a given irreducible polynomial $f(x)$ of degree n with period l, if the t-correlated order of $f(x)$ is 1 for every $0 < t < l$, then, our method will not work, since we can not generate even one more cycle from Z_0. However, the following theorem shows that this case can not happen:

Theorem 5.1. *Suppose that $f(x)$ is an irreducible polynomial of degree n with period l, then there must exist a positive integer t with $0 < t < l$, such that* $\mathrm{Ord}_t(f) > 1$.

Proof. Suppose on the contrary that $\mathrm{Ord}_t(f) = 1$ for every positive integer $0 < t < l$. Let β be a root of $f(x)$, we get a finite field $\mathbb{F}_{2^n} = \mathbb{F}_2[\beta]$. By theorem 3.1, we have that

$$h_{t,1}^l(x) = (1 + x^t)^l \equiv 1 \pmod{f(x)}$$

for every t with $0 < t < l$. So, we have that $(1 + \beta^t)^l = 1$, for every $0 < t < l$. Consider the set

$$\sum = \{1\} \cup \{1 + \beta^t \,|\, 0 < t < l\}.$$

it is east to see that all the elements of $\sum$ are the roots of $x^l = 1$ in the finite field $\mathbb{F}_{2^n}$. Since the set $\mathbb{F}_{2^n}^*$ of all non-zero elements of $\mathbb{F}_{2^n}$ form a cyclic group of order $2^n - 1$, and $l|2^n - 1$, there exists only one subgroup H of order l. Since the order of β is l, we have that $H =< \beta >= \{1, \beta, \beta^2, \cdots, \beta^{l-1}\}$, also every element of H is a root of $x^l = 1$. Therefore, we get that

$$\begin{aligned} H &= \{1, 1 + \beta^1, 1 + \beta^2, \cdots, 1 + \beta^{l-1}\} \\ &= \{1, \beta, \beta^2, \cdots, \beta^{l-1}\}. \end{aligned}$$

The multiplication holds in H, as H is a group under the multiplication. Now, let $H' = H \cup \{0\}$. We are now going to prove that the addition law holds also in the set H'. It is clear that $1 + \beta^i \in H'$ for every $0 < i < l$. On the other hand, for every i, j with $0 < i < j < l$, we have that $\beta^i + \beta^j = \beta^i(1 + \beta^{j-i}) \in H'$. Thus, the set H' form a finite field under the addition and multiplication, there exists an integer $s \leq n$ such that $|H'| = 2^s$. If $s = n$, then $1 + l = |H'| = 2^n$, i.e., $l = 2^n - 1$, it is impossible since we have assumed that $k > 1$, so $s < n$. However, in this case, the condition that $1+l = 2^s$ means that the order of 2 mod l is less than $s < n$, which contradicts the assertion of lemma 5.1 (which says that the irreducible polynomial $f(x)$ of degree n with period l exists if and only if the order of 2 mod l is n), and the theorem is proved. □

6 Generating de Bruijn Sequences

Case 1. Let k be a prime number, such that 2 is a primitive root mod k, by theorem 5.1, there exists an integer t, such that $\mathrm{Ord}_t(f) = k$. Let $\alpha_0 = 1 = (1, 0, \cdots, 0)$ and let Z_0 be the cycle generated by α_0. Then, we have $\Omega_t(Z_0) = G(f) \setminus \{Z_0\}$, whence we can join all the cycles of $G(f)$ to generate de Bruijn sequences.

Example 2. Let $n = 128$, the factorization of $2^n - 1 = 2^{128} - 1$ is

$$2^{128} - 1 = 3 \cdot 5 \cdot 17 \cdot 257 \cdot 641 \cdot 65537 \cdot 274177 \cdot 6700417 \cdot 67280421310721.$$

If we take $k = 5$, then $l = (2^{128} - 1)/5$. It is easy to see that 2 is a primitive root mod $k = 5$. By calculation, we can choose $f(x)$ as

$$\begin{aligned} f(x) =& x^{128} + x^{88} + x^{83} + x^{62} + x^{57} + x^{52} + x^{48} + x^{43} \\ &+ x^{38} + x^{31} + x^{29} + x^{27} + x^{26} + x^2 + 1, \end{aligned}$$

which is an irreducible polynomial of degree $n = 128$ with period l. It is easy to check that $(1+x)^l \not\equiv 1 \pmod{f(x)}$, so let $t = 1$, the $t = 1$-order of polynomial $f(x)$ is $\mathrm{Ord}_1(f) = k = 5$. Therefore, we have that

$$\begin{aligned} G(f) &= \left\{Z_0, Z_0^{(1)}, Z_0^{(2)}, Z_0^{(3)}, Z_0^{(4)}\right\} \\ &= \left\{Z_0, Z_0^{(2^0)}, Z_0^{(2^1)}, Z_0^{(2^2)}, Z_0^{(2^3)} = Z_0^{(3)}\right\} \end{aligned}$$

By the shift register matrix T, we can find $k - 1 = 4$ states of the cycle Z_0 as follows:

$$\alpha_1 = \alpha_0 T,\ \alpha_2 = \alpha_0 T^2,\ \alpha_4 = \alpha_0 T^4,\ \alpha_8 = \alpha_0 T^8.$$

the conjugate states of which lie in all the cycles of $G(f)$ except for Z_0, hence we can join all these cycles of $G(f)$ and obtain a de Bruijn sequence of stage $n = 128$. We list these four pairs of conjugate states in the hexadecimal form as follows:

(80000000000000000000000000000000,80000000000000000000000000000001),
(40000000000000000000000000000000,40000000000000000000000000000001),
(50000000000000000000000000000000,50000000000000000000000000000001),
(55000000000000000000000000000000,55000000000000000000000000000001).

By theorem 2.2, we can write out the correspondent connective polynomial, we omit it to save space.

Since the conjugate order of 1 mod l is $\gamma_1 = 128$, and the order of 2 mod $d = \mathrm{Ord}_1(f) = 5$ is $r = 4$, there are $128/4 = 32$ pairs of conjugate states lying on Z_0 and each cycle of $\Omega_1(Z_0)$ respectively, therefore, we can generate $32^4 = 2^{20}$ distinct de Bruijn sequences of stage $n = 128$.

Case 2. In the case 1, k is a prime number, and 2 is a primitive root mod k, i.e., the order of 2 mod k is $k - 1$. Since $k|2^n - 1$, we have $2^n \equiv 1 \pmod{k}$, whence $k - 1 \leq n$, $k \leq n + 1$. So in this case, the number of cycles is relatively small.

However, we can select larger integer k, and use distinct t-correlated cycles to generate de Bruijn sequences.

Example 3. Let $n = 128$, and $k = 3 \cdot 5 \cdot 17 = 255$, $l = (2^{128} - 1)/255$. By calculation, the following polynomial $f(x)$ is an irreducible polynomial of degree $n = 128$ with period l.

$$\begin{aligned} f(x) =& 1 + x^2 + x^3 + x^9 + x^{10} + x^{13} + x^{15} + x^{16} + x^{17} + x^{18} + x^{19} + x^{21} \\ &+ x^{23} + x^{28} + x^{32} + x^{33} + x^{34} + x^{36} + x^{38} + x^{41} + x^{43} + x^{44} + x^{45} \\ &+ x^{47} + x^{48} + x^{50} + x^{53} + x^{57} + x^{59} + x^{60} + x^{66} + x^{67} + x^{74} + x^{75} \\ &+ x^{80} + x^{81} + x^{82} + x^{83} + x^{85} + x^{86} + x^{92} + x^{93} + x^{94} + x^{96} + x^{98} \\ &+ x^{99} + x^{101} + x^{103} + x^{104} + x^{106} + x^{109} + x^{110} + x^{111} + x^{112} \\ &+ x^{113} + x^{116} + x^{117} + x^{119} + x^{121} + x^{126} + x^{128} \end{aligned}$$

For $t = 1$, the 1-correlated order of $f(x)$ is $d_t = \mathrm{Ord}_t(f) = 255$, the order of 2 mod d_t is $r_t = 8$, the cycle Z_0 can join $r_t = 8$ cycles of $G(f)$, i.e., the subset $\Omega_1(Z_0) = \left\{ D_{f,1}^{(2^j)}(Z_0) \,|\, j = 0, 1, 2, \cdots, 7 \right\}$ of $G(f)$. The conjugate order of t mod l is $\gamma_t = 128$, the cycle Z_0 has $\gamma_t / r_t = 16$ pairs of conjugate states with each cycles of $\Omega_1(Z_0)$, so there are $16^8 = 2^{32}$ ways to join the cycle Z_0 with the cycles of $\Omega_t(Z_0)$. We should use many different values t to join all the cycles of $G(f)$. The following table list all the information about the selected t-correlated cycles: the width t, the t-correlated order $d_t = \mathrm{Ord}_t(f)$ of $f(x)$, the conjugate order γ_t of t mod l, the order r_t of 2 mod d_t, and the number $(\gamma_t / r_t)^{r_t}$, which means that how many ways we can join Z_0 with all the cycles of $\Omega_t(Z_0)$.

t	d_t	γ_t	r_t	number	t	d_t	γ_t	r_t	number
1	255	128	8	2^{32}	3	15	128	4	2^{20}
5	85	128	8	2^{32}	7	255	128	8	2^{32}
9	255	128	8	2^{32}	11	255	128	8	2^{32}
15	85	128	8	2^{32}	17	255	128	8	2^{32}
19	255	128	8	2^{32}	21	17	128	8	2^{32}
25	255	128	8	2^{32}	27	85	128	8	2^{32}
29	255	128	8	2^{32}	31	51	128	8	2^{32}
35	5	128	4	2^{20}	37	85	128	8	2^{32}
39	15	128	4	2^{20}	41	51	128	8	2^{32}
43	85	128	8	2^{32}	47	85	128	8	2^{32}
49	85	128	8	2^{32}	61	17	128	8	2^{32}
65	255	128	8	2^{32}	67	85	128	8	2^{32}
77	51	128	8	2^{32}	79	255	128	8	2^{32}
87	255	128	8	2^{32}	93	255	128	8	2^{32}
133	255	128	8	2^{32}	143	255	128	8	2^{32}
197	255	128	8	2^{32}	243	51	128	8	2^{32}
337	3	128	2	2^{12}	349	255	128	8	2^{32}

By this method, we can generate 2^{1032} (all the number in the last column are multiplied) distinct de Bruijn sequences.

7 Conclusion

In this paper, we propose a method, for a suitable irreducible polynomial, we can generate all the state cycles of $G(f)$, and find enough pairs of conjugate states, which can join all the cycles of $G(f)$ resulting a full length cycle. The basic idea is that we use the concept of correlated cycles to generate pairs of conjugate states, whose computation complexity is polynomial. Therefore, we can generate de Burijn sequences with such large orders as 128.

When we use different t-correlated cycles to join cycles, we hope that the number k of cycles in $G(f)$ should be large enough, so that the period of selected polynomial $f(x)$ will be small, and the resulting sequence will become more complex. However, as our method is to join one special cycle

Z_0 with all other cycles of $G(f)$, the period l of polynomial $f(x)$ can not be too small. Meanwhile, different t-correlated cycles may join the same cycles by lemma 4.1. To join all the cycles of $G(f)$, we need to search the width t until we can join all the cycles of $G(f)$. The further problem is to find some results on the choose of k, such that k is as large as possible.

References

[1] de Bruijn N, A combinatorial problem, Proc Nederlandse Akademie van Wetenschappen, vol. 49, pp. 758-764, 1946.

[2] Fredricksen H, A survey of full length nonlinear shift register cycle algorithms, SIAM Review, vol. 24, pp. 195-221, 1982. vol. 49, pp.758–764.

[3] Lempel A, On a homomorphism of the de Bruijn graph and its applications to the design of feedback shift registers, IEEE Trans. Comput. C19, pp. 1204-1209, 1970.

[4] Annexstein F S, Generating de Bruijn sequences: an efficient implementation, IEEE Trans. Comput. 46, pp. 198-200, 1997.

[5] Alhakim A, Akinwande M, A recursive construction of nonbinary de Bruijn sequences, Des. Codes and Crypto. 60, pp. 155-169, 2011.

[6] Etzion T, Lempel A, Algorithms for the generation of full-length shift-register sequences, IEEE Trans. Info. vol. 30, pp. 480-484, 1984.

[7] Jansen C J A, An efficient algorithm for the generation of de Bruijn cycles, IEEE trans. Info. vol. 37, pp. 1475-1478, 1991.

[8] Yang J H, Dai Z D, Construction of m-ary de Bruijn sequences, Advances in Cryptology-AUSCRYPT'92, LNCS 718, pp. 357-363, 1993.

[9] Richard A.Games, A generalized Recursive construction for de Bruijn sequence, Information Theory, IEEE Transactions on , Vol. 29(6), pp. 843-850, 1983

[10] Golomb S, Shift Register Sequences, Aegean Park Press, Laguna Hills, 1982.