文章编号:1671-4229(2022)03-0029-08

$k=2^m-1$ 阶分圆数的计算

董军武, 张晓磊, 余玉银
(广州大学 数学与信息科学学院, 广东 广州 510006)

摘 要: 令 $n=2m$ 是偶数,$k=2^m-1$,文章给出了有限域$\mathbb{F}_{2^n}$上所有 k 阶分圆数的计算公式,研究了这些分圆数的值分布规律。这些结果可用于构造一类 de Bruijn 序列,构造方式是对通过合并不可约线性移位寄存器的状态圈得到的,这类 de Brjijn 序列,合并的状态圈数是最多的。

关键词: 分圆类; 分圆数; 有限域; 迹; de Bruijn 序列
中图分类号: O 153.4 **文献标志码**: A

The cyclotomic numbers of order $k=2^m-1$

DONG Jun-wu, ZHANG Xiao-lei, YU Yu-yin
(School of Mathematics and Information Science, Guangzhou University, Guangzhou 510006, China)

Abstract: Let $n=2m$ be an even number, for $k=2^m-1$, we provide a method to calculate all the corresponding k-th cyclotomic numbers $a_{i,j}$ over the finite field $\mathbb{F}_{2^n}$, and study the value distribution of the k-th cyclotomic matrix. These results can be used to construct a class of de Bruijn sequences by jointing all the cycles of the graph state of the linear shift register with irreducible connective polynomials, and the number of cycles that are joined is as many as possible.

Key words: cyclotomic class; cyclotomic number; finite field; trace; de Bruijn sequence
CLC number: O 153.4 **Document code**: A

0 Introduction

The cyclotomic numbers have many applications in coding theory and combinatorial designs. In coding theory, for example, Delsarte et al.[1] used the cyclotomies to construct two-weight irreducible cyclic codes, which was called the "semi-primitive" case, i.e., $k|2^s+1$ and $2s|n$.

Cyclotomies can be used to construct difference sets[2-3], which is an important structure in combinatory designs. There are many results on the cyclotomic numbers for the case of prime finite fields[4-10].

A de Bruijn sequence of stage n is a binary sequence with period 2^n which contains all binary n-tuples. De Bruijn sequences can be generated by the cycle join method from a linear feedback shift register(LFSR), especially from irreducible codes[11-18].

In Ref.[19], the authors establish an isomorphism from the finite field $\mathbb{F}_{2^n}$ to stage space $\mathbb{F}_{2^n}=\{(a_1, a_2, \cdots, a_n)\,|\,a_i\in\mathbb{F}_2\}$, which maps cyclotomic classes to the cycles of the LFSR generated by the irreducible definition polynomial $f(x)$ of the finite field $\mathbb{F}_{2^n}$, and maps pairs $(\alpha, \alpha+1)$ to conjugate states, and hence the cyclotomic matrix can be used to calculate the number of de Bruijn sequences generated from the LFSR by the cycle join method.

From what we said above, we consider the cyclotomic numbers of the binary finite field $\mathbb{F}_{2^n}$. From the contribution of Delsarte et al., the semi-primitive case of cyclotomic

Foundation items: The NSF of China (61502113) and the Guangdong Provincial NSF (2015A030310174)
Biography: DONG Jun-wu(1971-), male, associate professor. E-mail: djunwu@163.com
Citation: DONG Jun-wu, ZHANG Xiao-lei, YU Yu-yin. The cyclotomic numbers of order $k=2^m-1$[J]. Journal of Guangzhou University (Natural Science Edition),2022,21(2):29-36.

numbers can be easily derived. In this paper, we consider the case $k=2^{\frac{n}{2}}-1$ for even field dimension n.

1 Preliminaries

We consider the binary finite field $\mathbb{F}_{2^n}$, let θ be the primitive element of this field. Suppose k divides 2^n-1, let $l=(2^n-1)/k$. For every $j=0, 1, 2, \cdots, k-1$, we call the subsets of the finite field $\mathbb{F}_{2^n}$

$$T_j=\{\theta^{u\cdot k+j}\mid u=0,1,2,\cdots,l-1\}$$

the k-th cyclotomic classes. So there are k cyclotomic classes $T_0, T_1, \cdots, T_{k-1}$. For each pair of cyclotomic classes T_i and T_j, the cyclotomic number, denoted by $(i,j)_k$ is defined to be the number of elements of the set

$$\{(\alpha, \alpha+1)\mid \alpha\in T_i, \alpha+1\in T_j\} \tag{1}$$

In the following, the number k is fixed, and we will write $a_{i,j}^k$ or $a_{i,j}$ instead of $(i,j)_k$. All the $k\times k$ cyclotomic numbers $a_{i,j}$ form a k-th square matrix $A=(a_{i,j})_{k\times k}$. We call $A=(a_{i,j})_{k\times k}$ the k-th binary cyclotomic matrix of the finite field $\mathbb{F}_{2^n}$.

Firstly, the following lemma and corollary can be easily derived form the basic arithmetics of the finite field $\mathbb{F}_{2^n}$:

Lemma 1 The k-th binary cyclotomic numbers $a_{i,j}$ processes the following relation:

(1) $a_{i,j}=a_{j,i}$;

(2) $a_{i,j}=a_{2i,2j}$;

(3) $a_{i,j}=a_{k-i,j-i}=a_{i-j,k-j}$;

all the operations on the subscripts are mod k.

(4) $\sum_{j=0}^{k-1}a_{0,j}=l-1$;

(5) $\sum_{j=0}^{k-1}a_{i,j}=l$ for all $i\neq 0$.

Corollary 1 For every $i=1, 2, \cdots, k-1$, $a_{0,i}=a_{i,0}=a_{-i,-i}$.

In Ref. [1], the authors calculate the weight-distributions of binary semi-primitive cyclic codes of even length: n is even and $2^n-1=kl$, there exists an integer s such that $k\mid 2^s+1$ and $s\mid n$. For each cyclotomic class

$$T_j=\{\theta^{uk+j}\mid u=0,1,2,\cdots, l-1\},$$

we define a define corresponding binary vector $S(T_j)$ of dimension n as follwing:

$$S(T_j)=\{Tr(\theta^j), Tr(\theta^{k+j}), Tr(\theta^{2k+j}), \cdots, Tr(\theta^{(l-1)k+j})\} \tag{2}$$

where $Tr(x)$ is the trace function of $\mathbb{F}_{2^n}$, defined by $Tr(x)=x+x^2+x^{2^2}+\cdots+x^{2^{n-1}}$ for all $x\in\mathbb{F}_{2^n}$.

Theorem 1[1] Let s be any divisor of 2^r+1, and let k be an even multiple of r, say $k=2mr$. Then the irreducible code of length $n=(2^k-1)/s$ and dimension k over $GF(2)$ has only two distinct weights w_0 and w_1 which are the unique solution of the following equations

$$\begin{aligned} w_0+(s-1)w_1&=2^{k-1}\\ w_0^2+(s-1)w_1^2&=(n+1)2^{k-2}\end{aligned} \tag{3}$$

From this result, and by using the method of exponent sum, we can easily get the following result:

Theorem 2 Let n, k be integers, such that there exists an integer s with $2s\mid n$ and $k\mid 2^s+1$, write $n=2ms$, set $x=\frac{2^{\frac{n}{2}}-(-1)^m}{k}$, then the k-th cyclotomic matrix of the finite field $\mathbb{F}_{2^n}$ has the following form:

$$\begin{pmatrix} a & b & b & \cdots & b & b\\ b & b & c & \cdots & c & c\\ b & c & b & \cdots & c & c\\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots\\ b & c & c & \cdots & b & c\\ b & c & c & \cdots & c & b\end{pmatrix}$$

that is, there are only three values in the matrix: ① $a_{0,0}$ denote a; ② except $a_{0,0}$, all the other elements of the first row, the first column and the diagram have the same value b; ③ all the other elements of the matrix have the same value c. Furthermore, we have that

$$\begin{aligned} a&=x(x+(-1)^m(3-k))-1,\\ b&=x(x+(-1)^m),\\ c&=x^2\end{aligned} \tag{4}$$

We consider the quadratic equation over finite field $\mathbb{F}_{2^n}$. The general quadratic equation over finite field $\mathbb{F}_{2^n}$ has the following form:

$$x^2+ax+b=0 \tag{5}$$

with $a, b\in\mathbb{F}_{2^n}$. If $a=0$, the Eq. (5) has only one root, since the map $x\mapsto x^2$ is an automorphism of $\mathbb{F}_{2^n}$. If $a\neq 0$, by dividing a^2 on both sides of Eq. (5), we get the following form:

$$z^2+z+c=0 \tag{6}$$

with $c=b/a^2\in\mathbb{F}_{2^n}$. The following Lemma 2 can be proven easily.

Lemma 2 If c is an element of $\mathbb{F}_{2^n}$, then the Eq. (6) has $2-2T$ solutions over $\mathbb{F}_{2^n}$, where $T=Tr(c)$. Furthermore, if z is one solution, then the other solution is $z+1$.

Corollary 2 If $a\neq 0$, then the quadratic Eq. (5) has

two solutions if and only $Tr(b/a^2)=0$.

2 The cyclotomic number of order $k=2^{\frac{n}{2}}-1$

In this section, we consider the case that $n=2m$ is an even integer, and $k=2^{\frac{n}{2}}-1=2^m-1$, then $l=(2^n-1)/k=2^m+1$. Firstly, we give some properties of such k-th cyclotomic classes.

In number theory, we have the following lemma:

Lemma 3 Suppose that G is a finite cyclic group, and H is a subgroup of G of order l, then for every $a\in G$, $a\in H$ if and only if $a^l=1$, where 1 denotes the identity element of the group G.

Since $n=2m$, the finite field $\mathbb{F}_{2^n}$ has a unique finite subfield $\mathbb{F}_{2^m}$. Let θ be a primitive element of $\mathbb{F}_{2^n}$. For every nonzero element $\alpha\in\mathbb{F}_{2^n}$, $\alpha\in\mathbb{F}_{2^m}$ if and only if $\alpha^{2^m-1}=1$, that is $\alpha^k=1$. Therefore $\mathbb{F}_{2^m}\setminus\{0\}=\{\theta^{jl}\mid j=0,1,2,\cdots,k-1\}$. Thus we have the following lemma:

Lemma 4 Suppose $n=2m$, $k=2^m-1$, and $l=2^m+1$, then in the finite field $\mathbb{F}_{2^n}$, all the elements θ^{jl} are distinct for all $j=0,1,2,\cdots,k-1$.

Furthermore, we have the following lemma:

Lemma 5 Each k-th cyclotomic class T_i contains only one element of the form θ^{jl}.

Proof From $k=2^m-1$ and $l=2^m+1$, we know that k and l are coprime, so the congruent equation $uk+i\equiv 0\pmod l$ has only one solution u. That is, the k-th cyclotomic class T_i contains only one element θ^{uk+i} which has the form of θ^{jl}. Since all the k-th cyclotomic classes are disjoint, each cyclotomic class T_i contains only one nonzero element of the subfield $\mathbb{F}_{2^m}$. □

In the following, we use the symbol $T_1(\alpha)$ to denote the trace function over the subfield $\mathbb{F}_{2^m}$ of $\mathbb{F}_{2^n}$, that is, for every $\alpha\in\mathbb{F}_{2^m}$ (i.e., for every element $\alpha\in\mathbb{F}_{2^n}$ of the form θ^{jl}), $T_1(\alpha)=\alpha+\alpha^2+\alpha^{2^2}+\cdots+\alpha^{2^{m-1}}$.

Now, we will prove the following lemma, which gives the bound of all the k-th cyclotomic number:

Lemma 6 For every $i,j=0,1,2,\cdots,k-1$, the k-th cyclotomic number $a_{i,j}\leqslant 2$.

Proof Let G be the multiplicative group of all the nonzero elements of the finite field $\mathbb{F}_{2^n}$, and θ be the primitive element, then G is a cyclic group of order 2^n-1. The cyclotomic class T_0 is the unique subgroup of order l generated by the element θ^k, in the following, we use H instead of T_0 for simplicity. The other cyclotomic classes T_j are just the left cosets θ^jH of H in G.

For any given $i,j=0,1,2,\cdots,k-1$, if $a_{i,j}=0$, the assertion is true. Now assume that $a_{i,j}>0$. Then there exist an element $\alpha=\theta^{uk+i}\in T_i=\theta^iH$, such that $1+\alpha\in T_j=\theta^jH$. Therefore $(1+\alpha)\theta^{-j}=(1+\theta^{uk+i})\theta^{-j}\in H$, and by Lemma 3, we have that $(1+\theta^{uk+i})^l\theta^{-lj}=1$, it is the same thing as

$$(1+\theta^{uk+i})^l=\theta^{jl}\tag{7}$$

We calculate the left side of Eq. (7) as following:

$$\begin{aligned}(1+\theta^{uk+i})^l&=(1+\theta^{uk+i})^{2^m+1}=\\&(1+\theta^{uk+i})^{2^m}(1+\theta^{uk+i})=\\&(1+\theta^{2^m(uk+i)})(1+\theta^{uk+i})=\\&1+\theta^{2^m(uk+i)}+\theta^{uk+i}+\theta^{il}\end{aligned}$$

where $\theta^{2^m(uk+i)}\theta^{uk+i}=\theta^{(2^m+1)(uk+i)}=\theta^{l(uk+i)}=\theta^{il}$. Since $k=2^m-1$, then $2^m(uk+i)=2^muk+(2^m-1)i+i=(2^mu+i)k+i$. Let u_1 be the remainder of l that divides 2^mu+i, that is, there exist 5 an integer q such that $2^mu+i=ql+u_1$, with $0\leqslant u_1<l$, then we have that

$$\theta^{2^m(uk+i)}=\theta^{(2^mu+i)k+i}=\theta^{qlk+u_1k+i}=\theta^{u_1k+i}\in T_i.$$

Now, the Eq. (7) becomes

$$\theta^{uk+i}+\theta^{u_1k+i}=1+\theta^{il}+\theta^{jl}\tag{8}$$

Set $\xi=1+\theta^{il}+\theta^{jl}$, then both $\alpha=\theta^{uk+i}$ and $\alpha_1=\theta^{u_1k+i}$ in T_i are the roots of the following equation in the finite field $\mathbb{F}_{2^n}$:

$$x^2+\xi x+\theta^{il}=0\tag{9}$$

Let i,j be given as above, we define the set $\Gamma_{i,j}=\{\gamma\in T_i\mid 1+\gamma\in T_j\}$. Notice that the Eq. (9) is only related to i and j, all the element of $\Gamma_{i,j}$ are the solutions of the Eq. (9). Since the quadratic equation over any field has at most two roots, we have that $a_{i,j}=|\Gamma_{i,j}|\leqslant 2$ for this i and j. Therefore, the assertion of Lemma 6 is true. □

Now, we can prove the following result:

Theorem 3 Suppose that $n=2m$, and $k=2^m-1$, $l=2^m+1$. Let θ be a primitive element of the finite field $\mathbb{F}_{2^n}$, then we have that

(1) $a_{i,j}=1$ if and only if $1+\theta^{il}+\theta^{jl}=0$.

(2) For all the $i,j=0,1,2,\cdots,k-1$, such that $\xi=1+\theta^{il}+\theta^{jl}\neq 0$, then

$$a_{i,j}=\begin{cases}2, & \text{if } T_1(\theta^{il}/\xi^2)=1\\0, & \text{if } T_1(\theta^{il}/\xi^2)=0\end{cases}$$

Proof Notice that the coefficients $\xi=1+\theta^{il}+\theta^{jl}$ and θ^{jl} of the Eq. (9) belong to the subfield $\mathbb{F}_{2^m}$. We will con-

sider the general quadratic Eq. (9) of all $i, j = 0, 1, 2, \cdots, k-1$.

If $\xi = 1 + \theta^{il} + \theta^{jl} = 0$, then the quadratic Eq. (9) becomes

$$x^2 = \theta^{il}$$

which has only one solution. Therefore, $a_{i,j} = 1$. In this case, the corresponding element $\alpha \in T_i$ belongs to the subfield $\mathbb{F}_{2^m}$. On the other hand, if $a_{i,j} = 1$, then there exists only one element $a \in T_i$ such that $1 + \alpha \in T_j$, since α is the solution of the Eq. (9), then ξ must be zero, otherwise, this quadratic equation would have two solutions in T_i, contrary to the condition that $a_{i,j} = 1$.

If $\xi = 1 + \theta^{il} + \theta^{jl} \neq 0$, set $\eta = \theta^{il}/\xi^2$. By dividing both sides of Eq. (9), we get the following quadratic equation

$$z^2 + z + \eta = 0 \qquad (10)$$

If the trace function $T_1(\eta)$ of the subfield $\mathbb{F}_{2^m}$ is zero, then the quadratic Eq. (10) has two solutions in $\mathbb{F}_{2^m}$, in this case, the corresponding k-th cyclotomic number $a_{i,j}$ must be zero. Otherwise, the k-th cyclotomic class T_i would contain two solutions of the quadratic Eq. (9), which belong to the subfield $\mathbb{F}_{2^m}$, contrary to the Lemma 5.

If the trace function $T_1(\eta)$ of the subfield $\mathbb{F}_{2^m}$ is one, we will prove that the corresponding k-th cyclotomic number $a_{i,j} = 2$. In this case, the quadratic equation of the form Eq. (9) has no solution in the subfield $\mathbb{F}_{2^m}$, i. e., it is irreducible over $\mathbb{F}_{2^m}$, and it has two solutions in the large field $\mathbb{F}_{2^n}$. Let α be one of its solution, then, α must belong to one of the k-th cyclotomic class, say T_r. By the process of the proof of Lemma 6, α is a solution of the following quadratic equation:

$$x^2 + (1 + \theta^{rl} + \theta^{jl})x + \theta^{rl} = 0.$$

We know that, any two different irreducible polynomial over any field can not contain a common solution, therefore $\theta^{rl} = \theta^{il}$, and $r = i$, that is, the quadratic Eq. (9) has two solutions in the k-th cyclotomic class T_i. Hence the corresponding k-th cyclotomic number $a_{i,j} = 2$, which completes the proof. □

The following example illustrates the idea in the proof of Theorem 3:

Example 1 It is easy to verify that $f(x) = x^6 + x + 1$ is a primitive polynomial of degree $n = 6$ over the finite field $\mathbb{F}_2$. Let θ be a root of $f(x)$, then each element of the finite field $\mathbb{F}_{2^6}$ has a unique form $c_5\theta^5 + c_4\theta^4 + c_3\theta^3 + c_2\theta^2 + c_1\theta + c_0$ with each $c_i \in \mathbb{F}_2 = \{0, 1\}$, the binary 0 − 1 string $c_5c_4c_3c_2c_1c_0$ of length 6 can be used to represent the field element of $\mathbb{F}_{2^6}$, yet we would like to use the corresponding hexadecimal form for short. For example, the binary form of the field element $\theta^5 + \theta^3 + \theta^2 + 1$ is 101101, and the corresponding hexadecimal form is $2d$.

Let $k = 7$, $l = 9$, then the 7-th cyclotommic classes are listed as follows:

$T_0 = \{1, \theta^7, \theta^{14}, \theta^{21}, \theta^{28}, \theta^{35}, \theta^{42}, \theta^{49}, \theta^{56}\} = \{01, 06, 14, 3b, 1c, 0b, 3a, 1a, 1f\}$,

$T_1 = \{\theta, \theta^8, \theta^{15}, \theta^{22}, \theta^{29}, \theta^{36}, \theta^{43}, \theta^{50}, \theta^{57}\} = \{02, 0c, 28, 35, 38, 16, 37, 34, 3e\}$,

$T_2 = \{\theta^2, \theta^9, \theta^{16}, \theta^{23}, \theta^{30}, \theta^{37}, \theta^{44}, \theta^{51}, \theta^{58}\} = \{04, 18, 13, 29, 33, 2c, 2d, 2b, 3f\}$,

$T_3 = \{\theta^3, \theta^{10}, \theta^{17}, \theta^{24}, \theta^{31}, \theta^{38}, \theta^{45}, \theta^{52}, \theta^{59}\} = \{08, 30, 26, 11, 25, 1b, 19, 15, 3d\}$,

$T_4 = \{\theta^4, \theta^{11}, \theta^{18}, \theta^{25}, \theta^{32}, \theta^{39}, \theta^{46}, \theta^{53}, \theta^{60}\} = \{10, 23, 0f, 22, 09, 36, 32, 2a, 39\}$,

$T_5 = \{\theta^5, \theta^{12}, \theta^{19}, \theta^{26}, \theta^{33}, \theta^{40}, \theta^{47}, \theta^{54}, \theta^{61}\} = \{20, 05, 1e, 07, 12, 2f, 27, 17, 31\}$,

$T_6 = \{\theta^6, \theta^{13}, \theta^{20}, \theta^{27}, \theta^{34}, \theta^{41}, \theta^{48}, \theta^{55}, \theta^{62}\} = \{03, 0a, 3c, 0e, 24, 1d, 0d, 2e, 21\}$.

From this, we can calculate easily the 7-th cyclotomic matrix of $\mathbb{F}_{2^6}$ as follows:

$$A_7 = \begin{pmatrix} 2 & 0 & 0 & 2 & 0 & 2 & 2 \\ 0 & 2 & 2 & 0 & 2 & 1 & 2 \\ 0 & 2 & 2 & 1 & 2 & 2 & 0 \\ 2 & 0 & 1 & 0 & 2 & 2 & 2 \\ 0 & 2 & 2 & 2 & 2 & 0 & 1 \\ 2 & 1 & 2 & 2 & 0 & 0 & 2 \\ 2 & 2 & 0 & 2 & 1 & 2 & 0 \end{pmatrix}.$$

The subfield $\mathbb{F}_{2^3} = \{0, 1, \theta^9, \theta^{18}, \theta^{27}, \theta^{36}, \theta^{45}, \theta^{54}\}$, with $1 \in T_0$, $\theta^9 \in T_2$, $\theta^{18} \in T_4$, $\theta^{27} \in T_6$, $\theta^{36} \in T_1$, $\theta^{45} \in T_3$, and $\theta^{54} \in T_5$.

We calculate the trace function $T_1(x)$ of the subfield $\mathbb{F}_{2^3}$ for all $x \in \mathbb{F}_{2^3}$ as following:

$T_1(0) = 0$,

$T_1(1) = 1 + 1 + 1 = 1$,

$T_1(\theta^9) = \theta^9 + \theta^{18} + \theta^{36} = 18 + 0f + 16 = 1 = T_1(\theta^{18}) = T_1(\theta^{36})$,

$T_1(\alpha^{27}) = \theta^{27} + \theta^{54} + \theta^{45} = 0e + 17 + 19 = 0 = T_1(\theta^{54}) = T_1(\theta^{45})$.

It is easy to check that $1 + \theta^{2l} + \theta^{3l} = 1 + 0f + 0e = 1$, so the cyclotomic number $a_{2,3} = 1$.

To compute the cyclotomic number $a_{3,6}$, let $\xi = 1 + \theta^{3l}$

$+\theta^{6l}=1+\theta^{27}+\theta^{54}=01+0e+17=18=\theta^9$, then $\theta^{il}/\xi^2=\theta^{3l}/\theta^{2l}=\theta^9$, since $T_1(\theta^{il}/\xi^2)=T_1(\theta^9)=1$, we have $a_{3,6}=2$ by Theorem 3.

To compute the cyclotomic number $a_{4,5}$, let $\xi=1+\theta^{4l}+\theta^{5l}=1+\theta^{36}+\theta^{45}=01+16+19=0e=\theta^{27}=\theta^{3l}$, then $\theta^{il}/\xi^2=\theta^{4l}/\theta^{6l}=\theta^{5l}$, since $T_1(\theta^{il}/\xi^2)=T_1(\theta^{5l})=0$, we have $a_{4,5}=0$ by Theorem 3.

In fact, the proof of Lemma 6 provides another method to calculate the cyclotomic number $a_{i,j}$ as following:

Now, we can show that the cyclotomic class T_i can be partitioned into subsets of the form $\{\theta^{uk+i}, \theta^{u_1k+i}\}$, where u_1 is the remainder of l divides 2^mu+i as above. Since $2^mu_1+i\equiv 2^{2m}u+2^mi+i=(2^n-1)u+(2^m+1)i+u=lku+li+u\equiv u \pmod l$, u is the remainder of l divides 2^mu_1+i. Furthermore, if $0\leqslant v<l$ is an integer such that $v\neq u$, and $v\neq u_1$, let v_1 be the remainder of l divides 2^mv+i, we have that $v_1\neq u$ and $v_1\neq u_1$. In fact, if $v_1=u$, then v is the remainder of l divides 2^mv_1+i, and also the remainder of l divides 2^mu+i, and hence $v=u_1$ a contradiction. Similarly, $v_1\neq u_1$. So, the sets $\{\theta^{uk+i}, \theta^{u_1k+i}\}$ and $\{\theta^{vk+i}, \theta^{v_1k+i}\}$ are disjointed. If $u=-k^{-1}i \pmod l$, then $u\equiv 2^mu+i \pmod l$, in this case, $\theta^{uk+i}=\theta^{u_1k+i}$, and the set $\{\theta^{uk+i}, \theta^{u_1k+i}\}$ contains only one element.

For each subset $\{\theta^{uk+i}, \theta^{u_1k+i}\}$, from the relation (8), we can obtain a unique j, and then the corresponding cyclotomic number $a_{i,j}$ equals the cardinal number of the subset $\{\theta^{uk+i}, \theta^{u_1k+i}\}$.

Example 2 Let $n=6$, $k=7$, $l=9$, we consider the finite field $\mathbb{F}_{2^6}$ as in Example 1. We take $i=3$ as an example to illustrate the idea used in the above statement:

Let $u=0$, then $u_1\equiv 2^mu+i=2^3\cdot 0+3\equiv 3 \pmod 9$, we have the subset $\{\theta^3, \theta^{3k+3}=\theta^{24}\}$. By Eq. (8), we shall compute the unique value j with $0\leqslant j<k=7$ satisfying $\theta^3+\theta^{24}=1+\theta^{il}+\theta^{jl}$. Since $\theta^3+\theta^{24}=19$, and $1+\theta^{il}=1+\theta^{27}=0f$, so $\theta^{jl}=19+0f=16=\theta^{36}$. Therefore we have that $j=4$, and $a_{3,4}=2$. In fact, $1+\theta^3=09\in T_4$ and $1+\theta^{24}=10\in T_4$.

Let $u=1$, then $u_1\equiv 2^mu+i=2^3\cdot 1+3\equiv 2 \pmod 9$, we get the subset $\{\theta^{10}, \theta^{17}\}$. By the similarly calculation, we have that $j=5$, and thus $a_{3,5}=2$.

Let $u=4$, then $u_1\equiv 2^mu+i=2^3\cdot 4+3\equiv 8 \pmod 9$, we get the subset $\{\theta^{31}, \theta^{59}\}$. By the similarly calculation, we have that $j=6$, and thus $a_{3,6}=2$.

Let $u=5$, then $u_1\equiv 2^mu+i=2^3\cdot 5+3\equiv 7 \pmod 9$, we get the subset $\{\theta^{38}, \theta^{52}\}$. By the similarly calculation, we have that $j=0$, and thus $a_{3,0}=2$.

Let $u=6$, then $u_1\equiv 2^mu+i=2^3\cdot 6+3\equiv 6 \pmod 9$, we get the subset $\{\theta^{45}\}$, which contains only one element. Since $\theta^{jl}=1+\theta^{il}=1+\theta^{27}=0f=\theta^{18}$, we have that $j=2$, and thus $a_{3,2}=1$.

3 The value distribution of the (2^m-1)-th cyclotomic matrix

The result of Theorem 3 just provides a method to compute each $a_{i,j}$, and can not give any global information of the whole k-th cyclotomic matrix $A=(a_{i,j})_{k\times k}$. In this section, we study the value distribution of this cyclotomic matrix. Let $\mathbb{F}_{2^m}$ be any finite field, for each $\alpha\in\mathbb{F}_{2^m}$ with $\alpha\neq 0$, we define a map $\psi_\alpha(x)$ parameterized by α:

$$\psi_\alpha(x)=\begin{cases}\dfrac{\alpha}{1+\alpha^2+x^2}, & \text{if } x\neq 1+\alpha\\ 0, & \text{if } x=1+\alpha\end{cases} \tag{11}$$

The following Lemma 7 shows that the map $\psi_\alpha(x)$ is a one-to-one map from the finite field $\mathbb{F}_{2^m}$ into itself for every nonzero element $\alpha\in\mathbb{F}_{2^m}$:

Lemma 7 For every nonzero $\alpha\in\mathbb{F}_{2^m}$, the map $\psi_\alpha(x)$ defined by Map (11) is a one-to-one map.

Proof It is necessary to show that this map is onto, since the set $\mathbb{F}_{2^m}$ is finite. For every $y\in\mathbb{F}_{2^m}$, if $y=0$, then $\psi_\alpha(1+\alpha)=y$ by definition of the Map (11). If $y\neq 0$, we can solve x form $\dfrac{\alpha}{1+\alpha^2+x^2}=y$, i. e. $x=\sqrt{1+\alpha^2+\alpha y^{-1}}$. □

Lemma 8 For every nonzero $\alpha\in\mathbb{F}_{2^m}$, we have that $Tr(\dfrac{\alpha}{1+\alpha^2})=0$, where $Tr(x)$ is the trace function of the finite field $\mathbb{F}_{2^m}$.

Proof For every nonzero element $\alpha\in\mathbb{F}_{2^m}$, we consider the following quadratic equation over the finite field $\mathbb{F}_{2^m}$:

$$x^2+(1+\alpha)x+\alpha=0.$$

It is easy to check that α and 1 are the solutions of this equation, we have that $Tr(\dfrac{\alpha}{1+\alpha^2})=0$ by Corollary 2. Thus the assertion is hold. □

Theorem 4 Suppose $n=2m$ is an even integer, let $k=2^m-1$, and $l=2^m+1$, then the k-th cyclotomic matrix A

$=(a_{i,j})_{k\times k}$ of finite field $\mathbb{F}_{2^n}$ processes the following properties:

(1) $a_{0,0}=0$, if m is even, and $a_{0,0}=2$, if m is odd.

(2) In the first row, there are 2^{m-1} elements taking value 2, and the other $2^{m-1}-1$ elements taking value 0.

(3) In each of the other rows, there are 2^{m-1} elements taking value 2, only one element taking value 1, and all the other $2^{m-1}-2$ elements taking value 0.

Proof (1) If $i=0$, $j=0$, then the corresponding $\xi=1+\theta^{il}+\theta^{il}=1$, and $\theta^{il}/\xi^2=1$, and hence $T_1(\theta^{il}/\xi^2)=T_1(1)=m \pmod 2$. By the (2) of Theorem 11, we have that $a_{0,0}=2$ if and only if m is odd.

For each $i=0, 1, 2, \cdots, k-1$, let $\alpha=\theta^{il}$. By Lemma 7, the map $\psi_\alpha(x)$ is one-to-one over the subfield $\mathbb{F}_{2^m}$. For the special value $x_0=\theta^{il}$ such that $1+\theta^{il}+\theta^{il}=0$, the corresponding value $\psi_\alpha(x_0)=0$. Let $\sum_i=\mathbb{F}_{2^m}\setminus\{0=\psi_\alpha(x_0), \psi_\alpha(0)\}$. By the part (2) of Theorem 3, the whole elements of the i-th row of the matrix A that taking values 0 or 2 are exactly the $\{T_1(x)\mid x\in\sum_i\}$. Since the trace function $T_1(x)$ of the subfield $\mathbb{F}_{2^m}$ taking value 0 for half elements of $\mathbb{F}_{2^m}$ and value 1 for the other half elements of $\mathbb{F}_{2^m}$, and $T_1(0)=0$, $T_1(\psi_\alpha(0))=0$ by Lemma 8, there are 2^{m-1} elements of $\sum_i$ that taking 1 as the trace function value of $\mathbb{F}_{2^m}$, thus there are 2^{m-1} elements of the i-th row of the matrix A that taking value 2.

If $i=0$, then the element 1 belongs to the cyclotomic class T_0, and $1+1=0$ does not appear in any cyclotomic classes, therefore in the first row of the matrix A, no element can take value 1, therefore the part (2) of this theorem is held.

If $i\neq 0$, then there exists only value j such that $1+\theta^{il}+\theta^{il}=0$, and by part (1) of Theorem 3, the corresponding $a_{i,j}=1$, and part (3) of this theorem is held. □

4 Application

In this section, we will use our results to construct a class of de Bruijn sequences of stage n. Let $p(x)$ be a primitive polynomial of degree $n=2m$ over $\mathbb{F}_2$, with θ being one of its primitive roots. Let $k=2^m-1$ and $l=2^m+1$ as above. Now, we take $\alpha=\theta^k$, and $f_1(x)$ be the minimal polynomial of α over the finite field $\mathbb{F}_2$. Consider the set $\{\alpha, \alpha^2, \alpha^{2^2}, \cdots, \alpha^{2^{d-1}}\}$, with $\alpha^{2^d}=\alpha$. Then, we have that

$$f_1(x)=(x-\alpha)(x-\alpha^2)(x-\alpha^{2^2})\cdots(x-\alpha^{2^{d-1}}),$$

and $f_1(x)$ is an irreducible polynomial of degree d over $\mathbb{F}_2$. The following Lemma 9 shows that the degree d of $f_1(x)$ is n:

Lemma 9 Let $n=2m$, $k=2^m-1$, $l=2^m+1$, and d be as above, then $d=n$.

Proof We know that d is the minimal integer such that $\alpha^{2^d}=\alpha$, i.e., $\theta^{2^d k}=\theta^k$. Since the multiplicative order of θ in the finite field $\mathbb{F}_{2^n}$ is $2^n-1=kl$, we have that $2^d k\equiv k \pmod{kl}$, that is, $2^d\equiv 1 \pmod l$. Thus d is the multiplicative order of 2 mod l. By $2^n\equiv 1 \pmod l$, we have that $d\mid n$.

On the contrary, if we suppose that $d<n$, then we will get a contradiction. Let $n=n_1 d$, with $n_1>1$. By $2^d\equiv 1 \pmod l$, we can say that $2^d-1=ls$, with $s\geqslant 1$. Then

$$\begin{aligned} kl=2^n-1=2^{n_1 d}-1=&\\ (2^d-1)(1+2^d+2^{2d}+\cdots+2^{(n_1-1)d})=&\\ ls(1+2^d+2^{2d}+\cdots+2^{(n_1-1)d}).& \end{aligned}$$

Thus, we have that $2^m-1=k=s(1+2^d+2^{2d}+\cdots+2^{(n_1-1)d})\geqslant 1+2^d>2^d-1>l=2^m+1$, a contradiction. □

Let $f(x)=x^n f_1(1/x)$ be the reciprocal polynomial of $f_1(x)$, then $f(x)$ is the minimal polynomial of α^{-1}. Since both the multiplicative order of α^{-1} and α are equal, the period of $f(x)$, i.e., the smallest integer l such that $f(x)^l\equiv 1 \pmod{f(x)}$, is $l=(2^n-1)/k=2^m+1$.

If we take $f(x)$ as the feedback polynomial of a linear feedback shift register (LFSR), then stage graph $G(f)$ of the resulting LFSR 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.

Two state $x=(x_1, x_2, \cdots, x_n)$ and $y=(y_1, y_2, \cdots, y_n)\in\mathbb{F}_2^n$ are called conjugate states if $y_1=x_1+1$, and $y_i=x_i$ for $i=2, 3, \cdots, n$. If a pair of conjugate states lies on two distinct cycles then these two cycles can be joined into one cycle by adding a suitable monomial to the feedback polynomial $F(x_1, x_2, \cdots, x_n)$. The cycle-joint method of constructing de Bruijn sequences is to find enough pairs of conjugate states such that one can joins all the cycles into a full cycle.

If $f(x)=1+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}+x^n$ is an irreducible polynomial of degree n in $\mathbb{F}_2[x]$ with period $l=2^m+1$, then the matrix

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

is called the shift register matrix of $f(x)$. In a LFSR with $f(x)$ as a 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 $s\in\mathbb{F}_2^n$, the cycle generated by s is periodic, with period l, and the cycle Z generated by s can be represented as follows:

$$Z=\langle s\rangle=\{s, sT, sT^2, \cdots, sT^{l-1}\}.$$

The characteristic polynomial of T is

$$\det(xI-T)=x^nf(1/x)=f^*(x)=f_1(x),$$

which is the reciprocal polynomial of $f(x)$. By Cayley-Hamilton Theorem, we have that $f_1(T)=0$.

Then there is an field isomorphism ψ form the finite field $\mathbb{F}_{2^n}=\mathbb{F}_2[\alpha]$ to the set $\mathbb{F}_2[T]=\{a_0I_n+a_1T+a_2T^2+\cdots+a_{n-1}T^{n-1}\mid a_i\in\mathbb{F}_2\}$, by sending α to T. All nonzero matrices of $\mathbb{F}_2[T]$ form a multiplicative cyclic group of order 2^n-1, and the subgroup $H_0=\{I, T, T^2, \cdots, T^{l-1}\}$ is of order l. There exist $k-1$ matrices $g_i(T)\in\mathbb{F}_2[T]$ $(i=1, 2, \cdots, k-1)$ such that all the other left cosets of H_0 are of the following form:

$$H_i=g_i(T)H_0=\{g_i(T), g_i(T)T, g_i(T)T^2, \cdots, g_i(T)T^{l-1}\}.$$

Let $s_0=(1, 0, \cdots, 0)$ be a fixed vector. Then the map ϕ from $\mathbb{F}_2[T]$ to the vector space $\mathbb{F}_2^n$ by sending $g(T)$ of $\mathbb{F}_2[T]$ to $s_0g(T)$, is a one-to-one map. This map also sends each coset H_i into the corresponding state cycle $Z_i=\langle s_0g_i(T)\rangle$. If two state vectors $x=s_0g(T)$ and $y=s_0h(T)$ are conjugate, then, by $x+y=s_0$, we have that $g(T)+h(T)=I_n$. Through the isomorphism ψ, we can get a one-to-one map ψ from the finite field $\mathbb{F}_{2^n}=\mathbb{F}_2[\alpha]$ to the vector space $\mathbb{F}_2^n$, by sending $g(\alpha)$ to $s_0g(T)$. In the multiplicative cyclic group $\mathbb{F}_2[\alpha]\setminus\{0\}$, there is a unique cyclic subgroup $W_0=\{1, \alpha, \alpha^2, \cdots, \alpha^{l-1}\}$ of order l. There exist $k-1$ element $g_i(\alpha)\in\mathbb{F}_2[\alpha]\setminus\{0\}$ $(i=1, 2, \cdots, k-1)$ such that all the other left cosets of W_0 are of the following form

$$W_i=g_i(\alpha)W_0=\{g_i(\alpha), g_i(\alpha)\alpha, g_i(\alpha)\alpha^2, \cdots, g_i(\alpha)\alpha^{l-1}\}.$$

The map ψ sends each coset W_i into the corresponding state cycle $Z_i=\langle s_0g_i(T)\rangle$. Two state vectors $x=s_0g(T)$ and $y=s_0h(T)$ are conjugate if and only if $g(\alpha)+h(\alpha)=1$.

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

The adjacent matrix $B=(b_{i,j})_{k\times k}$ of the LFSR generated by $f(x)$ is defined as following:

$b_{i,j}$ = the pairs of conjugate states that lie in Z_i and Z_j respectively.

The adjacent matrix can be used to calculate the number of de Bruijn sequences that the cycle-join method can generate. Next, we will show that by suitable chosen $g_i(\alpha)$, the cosets W_i of $\mathbb{F}_2[\alpha]$ equals the cyclotomic T_i respectively.

Since $\mathbb{F}_2[\theta]=\mathbb{F}_2[\alpha]$, where $\alpha=\theta^k$, we have that

$$W_0=\{1,\alpha,\alpha^2,\cdots,\alpha^{l-1}\}=\{1,\theta^k, \theta^{2k}, \cdots, \theta^{(l-1)k}\}=T_0$$

for each $i=1, 2, \cdots, k-1$, set $g_i(\alpha)=\theta^i$, then, we have that

$$W_i=\{\theta^i,\theta^i\alpha, \theta^i\alpha^2, \cdots, \theta^i\alpha^{l-1}=\{\theta^{uk+i}\mid u=0,1, 2,\cdots, l-1\}=T_i.$$

Thus, by suitable labeling the state cycles, the adjacent matrix is exactly the k-th cyclotomic matrix. From the adjacent matrix $A_k=(a_{i,j})_{k\times k}$, we let $M=(m_{i,j})_{k\times k}$ as following:

$$m_{i,j}=\begin{cases}-a_{i,j}, & \text{if } i\neq j\\ \sum\limits_{t\neq i}a_{i,t}, & \text{if } i=j\end{cases}\qquad(12)$$

The BEST theorem shows that the number of de Bruijn sequences generated by cycle-join method is equal to the minor of any element of M. The following theorem shows that the cycle-join method does work for our case, that is, for $n=2m$, $k=2^m-1$.

Theorem 5 Suppose that n, k, l, and $f(x)$ as above, then we can find enough pairs of conjugate states that can join all the cycles of the $G(f)$ into a full cycle.

Proof Since the zero cycle (0) can be joined with $Z_0=\langle s_0\rangle$ as above. We just consider how to join all the k cycles $Z_0, Z_1, \cdots, Z_{k-1}$.

Firstly, consider the cycle Z_0. Let $\sum_1=\{Z_i\mid a_{0,i}=2, 0<i<k\}$, we have that $|\sum_1|=2^{m-1}$ or $2^{m-1}-1$ according to m being even or being odd. Thus, there are either 2^{m-1} cycles or $2^{m-1}-1$ cycles, which share two pairs of conjugate states. Let $\sum_2=\{T_i\mid a_{0,i}=0, 1\leqslant i<k\}$,

then cycles in $\sum_2$ can not be joined with T_0, i.e., there are at most $2^{m-1}-1$ cycles, that can not be joined with T_0.

For each $Z_j \in \sum_2$, that is, Z_j can not be joined with Z_0 directly. We shall show that there exists at least one $Z_i \in \sum_1$ such that $a_{i,j}=2$. For otherwise, there are at least 2^{m-1} cycles such $a_{i,j}=0$ in the j-th row of the k-th cycotomic matrix. However, there are exactly $2^{m-1}-2$ cycles such that $a_{j,i}=0$ by (3) of Theorem 4, a contridication. That is, the cycle Z_j can be joined with the cycle Z_i, and Z_i can be joined with the cycle Z_0, thus all the cycles can be joined with the cycle Z_0. □

Example 3 Let $n=6$, $k=7$, $l=9$ as before. It is easy to check that the polynomial $f(x)=x^6+x^3+1$ is irreducible with period $l=9$. By suitable labeling, the adjacent matrix of the state graph is equal the 7-th cyclotomic matrix $A=(a_{i,j})_{7\times 7}$ as in Example 1.

In this case, $\sum_1=\{Z_3, Z_5, Z_6\}$, that is, the cycles Z_3, Z_5 and Z_6 can be joined with Z_0, and $\sum_2=\{Z_1, Z_2, Z_4\}$, none of which can not be joined with Z_0.

For the state cycle Z_1, consider the 1-th column of the matrix A, since there are only two elements $a_{j,1}$ taking value 0, i.e., $a_{0,1}=0$ and $a_{3,1}=0$. Thus there must exist state cycle Z_j such that $a_{j,i}=2$, in fact $a_{5,1}=2$, and Z_1 can be joined with T_5.

For the state cycle Z_2, we can find that $a_{3,2}=1$ and $a_{5,2}=2$, then the cycle Z_2 can be joined with Z_3 or Z_5 of the set $\sum_1$.

For the state cycle Z_4, we can find that $a_{3,4}=2$ and $a_{6,4}=1$, then the cycle Z_4 can be joined with Z_3 or Z_6 of the set $\sum_1$.

All the cycles of $G(f)$ are joined into a full cycle.

It seems difficult to calculate any one minor of the matrix defined by Eq. (12) to get the number of de Bruijn sequences generated by the cycle-join method. In the following, we list, in the following Table 1, some experimental data of the number of de Bruijn sequences for small dimension n:

Table 1 The number of de Bruijn sequences that can be generated

n	Number
4	8
6	$2^{11}\cdot 3^3$
8	$2^{34}\cdot 3^6\cdot 5^4$
10	$2^{77}\cdot 3^{25}\cdot 5^5\cdot 7^5\cdot 11$
12	$2^{184}\cdot 3^{30}\cdot 5^{15}\cdot 7^7\cdot 13^6\cdot 17^6\cdot 19^8$
14	$2^{380}\cdot 3^{91}\cdot 5^{35}\cdot 7^{21}\cdot 11^{21}\cdot 17^7\cdot 29^8\cdot 31^7\cdot 37^7$

References:

[1] Delsarte P, Goethals J M. Irreducible binary cyclic codes of even dimension[C]//Proceedings of the Second Chapel Hill Conference on Combinatorial Mathematics and its Applications. Chapel Hill: University of North Carolina Press, 1970: 100-113.

[2] Storer T. Cyclotomy and difference sets[M]. Chicage: Markham Publishing Company, 1967.

[3] Baumert L D. Cyclic difference sets[M]. Berlin, Heidelberg: Splinger-Verlag, 1971.

[4] Dickson L E. Cyclotomy, higher congruences and warings problem[J]. American Journal of Mathematics, 1935, 57(2): 391-424.

[5] Lehmer E. On the number of solutions $u^k+D\equiv w^2 \pmod p$[J]. Pacific Journal of Mathematics, 1953(5): 425-432.

[6] Muskat J B. The cyclotomic numbers of order fourteen[J]. Acta Arithmetica, 1966, 11(3): 263-279.

[7] Whiteman A L. The cyclotomic numbers of order sixteen[J]. Transactions of the American Mathematical Society, 1957, 86(2): 401-413.

[8] Whiteman A L. The cyclotomic numbers of order ten[J]. Acta Arithmetica, 1960, 6(6): 95-111.

[9] Whiteman A L. The cyclotomic numbers of order twelve[J]. Acta Arithmetica, 1960, 6(1): 53-76.

[10] Baumert L D, Fredricksen H. The cyclotomic numbers of order eighteen with applications to difference sets[J]. Mathematics of Computation, 1967, 21(98): 204-219.

[11] Fredricksen H. A survey of full length nonlinear shift register cycle algorithms[J]. Siam Review, 1982, 24: 195-221.

[12] Dong J W, Pei D Y. Construction for de Bruijn sequences with large stage[J]. Designs, Codes and Cryptography, 2017, 85(2): 343-358.

[13] Fredricksen H. A class of nonlinear de Bruijn cycles[J]. Journal of Combinatorial Theory Series A, 1975, 19: 192-199.

(下转第54页)