THE UNIT GROUP OF THE RING OF NEGA-CIRCULANT MATRICES OVER FINITE FIELDS

By
MR. Prarinya NAKSING

A Thesis Submitted in Partial Fulfillment of the Requirements
for Master of Science MATHEMATICS
Department of MATHEMATICS
Silpakorn University
Academic Year 2024

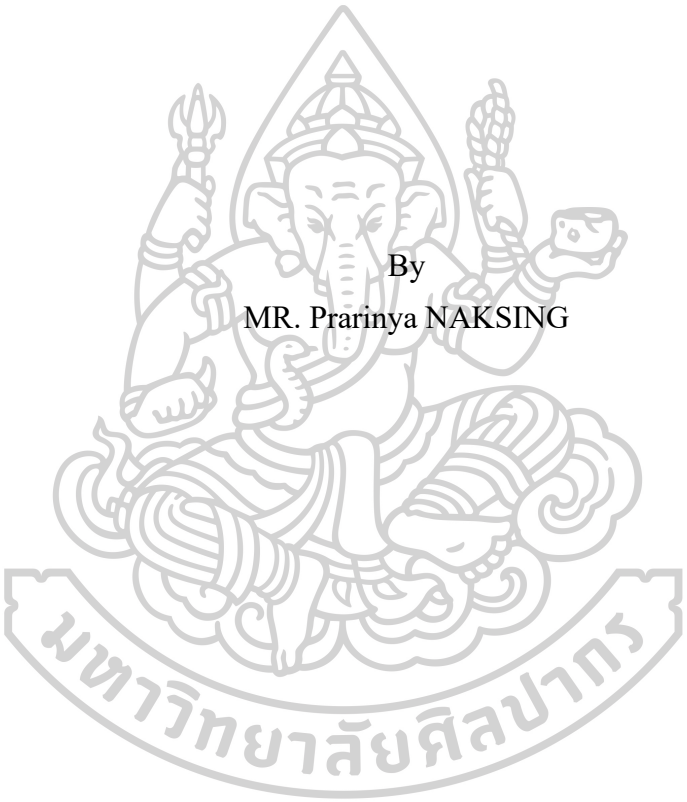
กรุปยูนิตของริงของเมทริกซ์วัฏจักรเชิงลบบนฟิลด์จำกัด

โดย
นายปริญญา นาคสิงห์

วิทยานิพนธ์นี้เป็นส่วนหนึ่งของการศึกษาตามหลักสูตรวิทยาศาสตรมหาบัณฑิต
สาขาวิชาคณิตศาสตร์ แผน ก แบบ ก 2
ภาควิชาคณิตศาสตร์
มหาวิทยาลัยศิลปากร
ปีการศึกษา 2567

THE UNIT GROUP OF THE RING OF NEGA-CIRCULANT MATRICES OVER FINITE FIELDS

By
MR. Prarinya NAKSING



A Thesis Submitted in Partial Fulfillment of the Requirements
for Master of Science MATHEMATICS
Department of MATHEMATICS
Academic Year 2024

Title	The Unit Group of the Ring of Nega-Circulant Matrices over Finite Fields
By	MR. Prarinya NAKSING
Field of Study	MATHEMATICS
Advisor	Associate Professor Somphong Jitman, Ph.D.

Faculty of Science, Silpakorn University in Partial Fulfillment of the Requirements for the Master of Science

.....Dean of Faculty of Science
(Assistant Professor Narong Chimpalee, Ph.D.)

Approved by

.....Chair person
(Associate Professor Jittisak Rakbud, Ph.D.)

.....Advisor
(Associate Professor Somphong Jitman, Ph.D.)

.....External Examiner
(Associate Professor Sajee Pianskool, Ph.D.)

640720036 : Major MATHEMATICS
Keyword : circulant matrices/ nega-circulant matrices/ unit groups/ polynomial rings/ enumeration

MR. Prarinya NAKSING : The Unit Group of the Ring of Nega-Circulant Matrices over Finite Fields Thesis advisor : Associate Professor Somphong Jitman, Ph.D.

Circulant and nega-circulant matrices have been of interest due to their nice algebraic structures and wide applications. This thesis focuses on the algebraic characterization and enumeration of the unit group of the ring of n x n nega-circulant matrices over a finite field F_q. Based on the well-known fact that the ring of n x n nega-circulant matrices over F_q is isomorphic to the quotient ring $F_q[x]/\langle x^n+1\rangle$, the study is given through the factorization of x^n+1 in $F_q[x]$. The results are presented into two cases where gcd(n, q) = 1 and where n is any arbitrary positive integer. This study provides not only the algebraic structures and enumeration of such unit groups but also efficient methods for computation. In some cases, simplified and efficient formulas for the number of units in these matrix rings are presented.

ACKNOWLEDGEMENTS

The successful completion of this thesis would not have been possible without the generous support and assistance of numerous individuals and institutions.

First and foremost, I wish to express my deepest gratitude to my thesis advisor, Associate Professor Somphong Jitman, Ph.D., for his invaluable guidance, unwavering support, and profound expertise throughout the course of this research. His encouragement and insightful advice have been instrumental in the successful completion of this work.

I am also sincerely appreciative of the constructive feedback and valuable suggestions provided by the members of my thesis committee: Associate Professor Jittisak Rakbud, Ph.D., and Associate Professor Sajee Pianskool, Ph.D. Their thoughtful recommendations have greatly contributed to the improvement of this thesis.

I gratefully acknowledge the Faculty of Science at Silpakorn University for the research assistant scholarship, as well as the Department of Mathematics for providing the necessary facilities and a supportive academic environment.

Lastly, I extend my heartfelt thanks to my family for their unwavering support, patience, and encouragement throughout my academic journey.

Prarinya NAKSING

CONTENTS

Chapter 1

Introduction

Let R be a commutative ring. An $n \times n$ **circulant matrix** over R is a matrix of the form

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{bmatrix},$$

where $a_i \in R$ for all $i = 1, 2, 3, \dots, n$. A **twistulant matrix** is a generalization of a circulant matrix defined as follows. For an element $\lambda \in R$, an $n \times n$ matrix A is a λ-twistulant matrix if

$$A = \begin{bmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ \lambda a_n & a_1 & a_2 & \dots & a_{n-1} \\ \lambda a_{n-1} & \lambda a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda a_2 & \lambda a_3 & \lambda a_4 & \dots & a_1 \end{bmatrix},$$

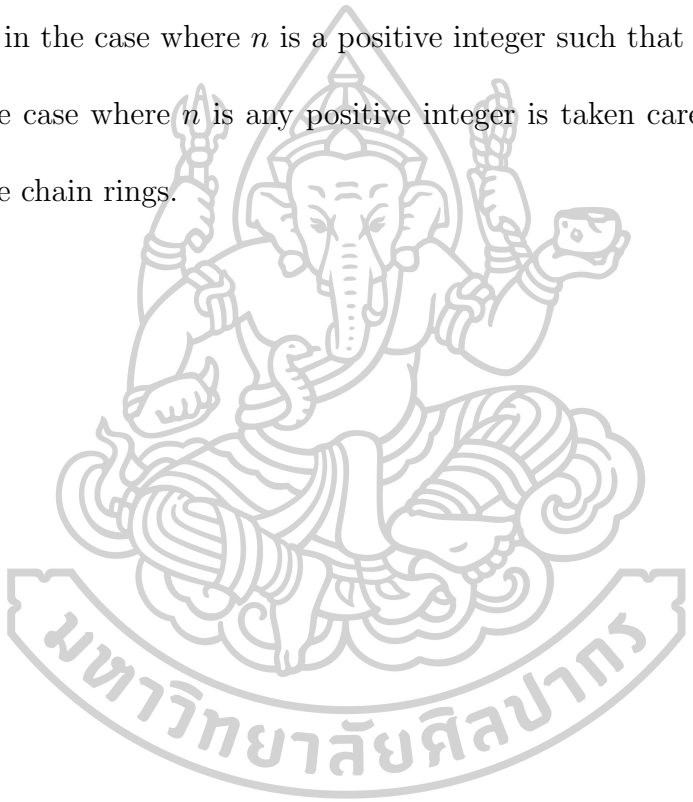
where $a_i \in R$ for all $i = 1, 2, 3, \dots, n$. From the definition, it can be observed that a 1-twistulant matrix is a circulant matrix. Extensively, a (-1)-twistulant matrix is referred to as a **nega-circulant matrix**. Twistulant matrices and nega-circulant

matrices play an important role in the study of negacyclic codes, constacyclic codes [4], and quasi-twisted codes [9].

Denote by $\mathrm{Cir}_n(R)$ and $\mathcal{U}(\mathrm{Cir}_n(R))$ the ring of $n \times n$ nega-circulant matrices over a ring R and the unit group of $\mathrm{Cir}_n(R)$, respectively. Units in $\mathrm{Cir}_n(R)$ are useful in various applications such as linear systems of equations, numerical analysis [14], number theory [19], and coding theory [15]. Since the ring $\mathrm{Cir}_n(R)$ is isomorphic to the quotient ring $R[x]/\langle x^n - 1\rangle$, the algebraic structures and enumeration of the group $\mathcal{U}(\mathrm{Cir}_n(\mathbb{F}_q))$, where $\mathbb{F}_q$ is a finite field of size q, have been studied through the ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ in [13] and [17]. In [17], the results on $\mathcal{U}\left(\mathrm{Cir}_n(\mathbb{F}_q)\right)$ were presented for $n = 2, 3, 4, 5$ under the condition that $\gcd(n, q) = 1$. Later, in [13], $\mathcal{U}\left(\mathrm{Cir}_n(\mathbb{F}_q)\right)$ was studied for arbitrary n with $\gcd(n, q) = 1$ and applied to the general case where n is any positive integer.

In this thesis, we examine the algebraic structures, properties, and enumeration of the ring of $n \times n$ nega-circulant matrices over $\mathbb{F}_q$ and its unit group. Let $\mathrm{NCir}_n(\mathbb{F}_q)$ denote the ring of $n \times n$ nega-circulant matrices over $\mathbb{F}_q$. From [6], it follows that the ring $\mathrm{NCir}_n(\mathbb{F}_q)$ is isomorphic to the quotient ring $\mathbb{F}_q[x]/\langle x^n + 1\rangle$. Therefore, the study of $\mathrm{NCir}_n(\mathbb{F}_q)$ and $\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$ will be conducted through $\mathbb{F}_q[x]/\langle x^n + 1\rangle$ which can be determined using the irreducible monic factors of the polynomial $x^n + 1$ over $\mathbb{F}_q$. Some results on the factorization of $x^n + 1$ over $\mathbb{F}_q$ have been discussed in [1], [11], and [16]. The study of $\mathrm{NCir}_n(\mathbb{F}_q)$ and $\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$ begins with the case where n is a positive integer such that $\gcd(n, q) = 1$. Later, the above results are extended to an arbitrary positive integer n by using the notion of finite chain rings.

This thesis is organized as follows. Chapter 2 provides necessary basic knowledge including definitions and properties of rings and fields, notion of circulant matrices and nega-circulant matrices, units of matrix rings, and number theoretical results. Chapter 3 presents a relationship between the ring of circulant matrices and the ring of nega-circulant matrices as well as the factorization of the polynomial $x^n + 1$. In Chapter 4, gives an investigation of $\mathrm{NCir}_n(\mathbb{F}_q)$ and $\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$ in the case where n is a positive integer such that $\gcd(n, q) = 1$. In Chapter 5, the case where n is any positive integer is taken care of by using the notion of finite chain rings.



Chapter 2

Preliminaries

In this chapter, definitions and fundamental results in algebra and number theory are recalled along with some properties of circulant and nega-circulant matrices which are used in the next chapters.

2.1 Rings

Let R be a commutative ring with identity and let $\mathcal{U}(R)$ denote the set of units in R. From [8, p. 116], $\mathcal{U}(R)$ is a group under the multiplication and it is called the **group of units** of R

From [18, Proposition 2.11], we have the following property for the unit group of a cartesian product of rings.

Lemma 2.1. *Let $R = \prod_{i=1}^{k} R_i$ be a direct product of rings with identity. Then*

$$\mathcal{U}(R) = \prod_{i=1}^{k} \mathcal{U}(R_i).$$

Definition 2.2. A commutative finite ring R with identity $1 \neq 0$ is called a **finite commutative chain ring** (FCCR) if its ideals are linearly ordered by inclusion.

Further properties of commutative finite chain rings are discussed and applied in Chapter 5.

Definition 2.3. Let R be a commutative ring with identity $1 \neq 0$. The ring R is called a **field** if every non-zero element in R has a multiplicative inverse.

Definition 2.4. A **finite field** is a field with a finite number of elements.

It is well known (see [8, Corollary 5.2]) that the cardinality of a finite field is a prime power. For a prime power q, a finite field of q elements is unique up to isomorphism and it is denoted by $\mathbb{F}_q$.

Definition 2.5. Let n be a positive integer. An element $a \in \mathbb{F}_q$ is called a **primitive nth root of unity** if $a^n = 1$ and $a^m \neq 1$ for all positive integers $m < n$. An element $a \in \mathbb{F}_q$ is called a **primitive element** if a is a primitive $(q-1)$th root of unity in $\mathbb{F}_q$.

Example 2.6. In $\mathbb{F}_7$, we have $\mathbb{F}_7 = \{0, 3, 3^2 = 2, 3^3 = 6, 3^4 = 4, 3^5 = 5, 3^6 = 1\}$. Hence, 3 is a primitive element in $\mathbb{F}_7$.

For a commutative ring R, denote by

$$R[x] = \left\{a_0 + a_1x + a_2x^2 + \ldots + a_kx^k | k \in \mathbb{N} \cup \{0\} \text{ and } a_0, a_1, a_2, \ldots, a_k \in R\right\}$$

the polynomial ring over R. For $f(x) \in R[x]$, let $\langle f(x) \rangle$ be the ideal in $R[x]$ generated by $f(x)$ and let $R[x]/\langle f(x) \rangle$ denote the quotient of ring $R[x]$ by $\langle f(x) \rangle$. Alternatively, if $\deg(f(x)) = n$, $R[x]/\langle f(x) \rangle$ can be viewed as

$$R[x]/\langle f(x) \rangle = \left\{a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1} | a_0, a_1, a_2, \ldots, a_{n-1} \in R\right\}$$

where the addition and the multiplication are computed as polynomials modulo $f(x)$.

2.2 Circulant and Nega-circulant Matrices

The notion of circulant and nega-circulant matrices is given in this section.

Definition 2.7. For a positive integer n and a commutuative ring R, an $n \times n$ **circulant matrix** over R is a matrix of the form:

$$\operatorname{circ}(a_1, a_2, \ldots, a_n) = \begin{bmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ a_n & a_1 & a_2 & \ldots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \ldots & a_1 \end{bmatrix},$$

where $a_i \in R$ for all $i = 1, 2, 3, \ldots, n$. For a positive integer n, let $\operatorname{Cir}_n(R)$ denote the set of all $n \times n$ circulant matrices over R.

An $n \times n$ **nega-circulant matrix** over R is a matrix of the form:

$$\operatorname{ncirc}(a_1, a_2, \ldots, a_n) = \begin{bmatrix} a_1 & a_2 & a_3 & \ldots & a_n \\ -a_n & a_1 & a_2 & \ldots & a_{n-1} \\ -a_{n-1} & -a_n & a_1 & \ldots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_2 & -a_3 & -a_4 & \ldots & a_1 \end{bmatrix},$$

where $a_i \in R$ for all $i = 1, 2, 3, \ldots, n$. For a positive integer n, let $\operatorname{NCir}_n(R)$ denote the set of all $n \times n$ nega-circulant matrices over R.

From [6] and [12], $\operatorname{Cir}_n(R)$ and $\operatorname{NCir}_n(R)$ are commutative rings under the usual addition and multiplication of matrices. A matrix A in these matrix rings over R is a unit if and only if $\det(A)$ is a unit in R.

Example 2.8. We have the following results.

1. $A = \begin{bmatrix} 1 & 3 & 6 \\ 6 & 1 & 3 \\ 3 & 6 & 1 \end{bmatrix}$ is a 3×3 circulant matrix over $\mathbb{F}_7$. Since $\det(A) = 1$, A is a unit in $\mathrm{Cir}_3(\mathbb{F}_7)$.

2. $A = \begin{bmatrix} 3 & 1 & 5 & 2 \\ 2 & 3 & 1 & 5 \\ 5 & 2 & 3 & 1 \\ 1 & 5 & 2 & 3 \end{bmatrix}$ is a 4×4 circulant matrix over $\mathbb{F}_{11}$. Since $\det(A) = 0$, A is not a unit in $\mathrm{Cir}_4(\mathbb{F}_{11})$.

3. $A = \begin{bmatrix} 1 & 5 & 4 \\ -4 & 1 & 5 \\ -5 & -4 & 1 \end{bmatrix}$ is a 3×3 nega-circulant matrix over $\mathbb{F}_7$. Since $\det(A) = 0$, A is not a unit in $\mathrm{NCir}_3(\mathbb{F}_7)$.

4. $A = \begin{bmatrix} 1 & 4 & 6 & 1 \\ -1 & 1 & 4 & 6 \\ -6 & -1 & 1 & 4 \\ -4 & -6 & -1 & 1 \end{bmatrix}$ is a 4×4 nega-circulant matrix over $\mathbb{F}_7$. Since $\det(A) = 3$, A is a unit in $\mathrm{NCir}_4(\mathbb{F}_7)$.

2.3 Number Theoretical Results

Number theoretical results required in the study of the nega-circulant matrices and their units are recalled in this section.

Definition 2.9. An integer b is said to be **divisible** by a nonzero integer a if there exists an integer k such that $b = ka$. In this case, it is written as $a|b$. For a positive integer a and an integer s, the notation $2^s||a$ is used whenever s is the largest integer such that $2^s|a$.

Definition 2.10. Let n be a positive integer and let a be an integer coprime to n, the **multiplicative order** $\mathrm{ord}_n(a)$ of a modulo n is the smallest positive integer k such that $a^k \equiv 1 \bmod n$. The **additive order** $\mathrm{O}_n^+(a)$ of a modulo n is defined to be the smallest positive integer k such that $ka \equiv 0 \bmod n$.

Definition 2.11. For a positive integer n, the **Euler's phi function** $\phi(n)$ is defined to be the number of integers k in the range $1 \leq k \leq n$ for which $\gcd(n, k) = 1$.

The following properties of the Euler's phi function are useful in the enumeration of nega-circulant matrices.

Theorem 2.12 ([7]). *Let n and d be a positive integers. If d is a divisor of n, the number of elements of order d in $\mathbb{Z}_n$ is $\phi(d)$. Equivalently, the number of elements in $\{0, 1, \ldots, n-1\}$ whose additive order is d equals $\phi(d)$.*

Theorem 2.13 ([3]). *Let p be a prime and let k be a positive integer. Then*

$$\phi\left(p^k\right) = p^k - p^{k-1} = (p-1)\, p^{k-1}.$$

Theorem 2.14 ([3]). *Let m and n be positive integers. If $\gcd(m,n) = 1$, then $\phi(mn) = \phi(m)\,\phi(n)$.*

Theorem 2.15 ([3]). *For each positive integer*

$$n = \sum_{d|n} \phi(d),$$

where the sum is computed over all positive divisors of n.

Chapter 3

The Ring $\mathrm{NCir}_n(\mathbb{F}_q)$

In this chapter, properties of the ring $\mathrm{Cir}_n(\mathbb{F}_q)$ of circulant matrices and the ring $\mathrm{NCir}_n(\mathbb{F}_q)$ of nega-circulant matrices are recalled. For an even prime power q, we have $-1 = 1 \in \mathbb{F}_q$ which means that every nega-circulant matrix is a circulant matrix. In order to study nega-circulant matrices over $\mathbb{F}_q$, we may assume that q is an odd prime power. For an odd positive integer n, a link between $\mathrm{Cir}_n(\mathbb{F}_q)$ and $\mathrm{NCir}_n(\mathbb{F}_q)$ is given. For the other case, the algebraic structures and enumeration of $\mathrm{NCir}_n(\mathbb{F}_q)$ are dicussed. Subsequently, the factorization of the polynomial $x^n + 1$ is discussed and it plays a crucial role in this study.

3.1 Algebraic Structures of $\mathrm{NCir}_n(\mathbb{F}_q)$

Properties of circulant matrices and nega-circulant matrices are recalled in terms of the quotient rings $\mathbb{F}_q[x]/\langle x^n - 1\rangle$ and $\mathbb{F}_q[x]/\langle x^n + 1\rangle$, respectively.

Proposition 3.1 ([12, Theorem 2.3]). *Let q be a prime power and let n be a positive integer. Then*

$$\mathrm{Cir}_n(\mathbb{F}_q) \cong \mathbb{F}_q[x]/\langle x^n - 1\rangle$$

as rings via the map

$$\mathrm{circ}\,(a_0, a_1, a_2, \ldots, a_{n-1}) \mapsto a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}.$$

Proposition 3.2 ([12, Theorem 2.3])**.** *Let q be an odd prime power and let n be a positive integer. Then*

$$\mathrm{NCir}_n(\mathbb{F}_q) \cong \mathbb{F}_q[x]/\langle x^n + 1\rangle$$

as rings via the map

$$\mathrm{ncirc}\,(a_0, a_1, a_2, \ldots, a_{n-1}) \mapsto a_0 + a_1x + a_2x^2 + \ldots + a_{n-1}x^{n-1}.$$

For an odd positive integer n, a link between $\mathrm{Cir}_n(\mathbb{F}_q)$ and $\mathrm{NCir}_n(\mathbb{F}_q)$ is given in the following lemma.

Lemma 3.3. *Let q be an odd prime power and let n be a positive integer. If n is odd, then*

$$\mathbb{F}_q[x]/\langle x^n - 1\rangle \cong \mathbb{F}_q[x]/\langle x^n + 1\rangle.$$

In this case,

$$\mathrm{Cir}_n(\mathbb{F}_q) \cong \mathrm{NCir}_n(\mathbb{F}_q).$$

Proof. Assume that n is odd. Let $\psi : \mathbb{F}_q[x]/\langle x^n - 1\rangle \to \mathbb{F}_q[x]/\langle x^n + 1\rangle$ define by,

$$\psi\left(f(x) + \langle x^n - 1\rangle\right) = f(-x) + \langle x^n + 1\rangle\,.$$

Let $f(x) + \langle x^n - 1\rangle \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then $f(x) = t(x)(x^n - 1) + r(x)$ for some $t(x)$ and $r(x)$ in $\mathbb{F}_q[x]$ such that $\deg(r(x)) < n$. Since n is odd, it follows that $(-x)^n - 1 = -x^n - 1 = -(x^n + 1)$ and

$$f(-x) = t(-x)((-x)^n - 1) + r(-x) = -t(-x)(x^n + 1) + r(-x).$$

Hence, $\psi(f(x) + \langle x^n - 1\rangle) = f(-x) + \langle x^n + 1\rangle \in \mathbb{F}_q[x]/\langle x^n + 1\rangle$.

Let $f_1(x) + \langle x^n - 1\rangle, f_2(x) + \langle x^n - 1\rangle \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$ be such that $f_1(x)+\langle x^n - 1\rangle = f_2(x)+\langle x^n - 1\rangle$. Then $(x^n-1)|(f_1(x)-f_2(x))$. Since $(-x)^n-1 = -(x^n+1)$, we have $(x^n+1)|(f_1(-x) - f_2(-x))$ which implies that

$$\begin{aligned}\psi(f_1(x) + \langle x^n - 1\rangle) &= (f_1(-x) + \langle x^n + 1\rangle \\ &= f_2(-x)) + \langle x^n + 1\rangle \\ &= \psi(f_2(x) + \langle x^n - 1\rangle).\end{aligned}$$

Hence, ψ is a well-defined function.

Let $f(x) + \langle x^n - 1\rangle, g(x) + \langle x^n - 1\rangle \in \mathbb{F}_q[x]/\langle x^n - 1\rangle$. Then

$$\begin{aligned}\psi\left((f(x) + g(x)) + \langle x^n - 1\rangle\right) &= (f(-x) + g(-x)) + \langle x^n + 1\rangle \\ &= f(-x) + \langle x^n - 1\rangle + g(-x) + \langle x^n + 1\rangle \\ &= \psi\left(f(x) + \langle x^n - 1\rangle\right) + \psi\left(g(x) + \langle x^n - 1\rangle\right)\end{aligned}$$

and

$$\begin{aligned}\psi\left((f(x) \cdot g(x)) + \langle x^n - 1\rangle\right) &= (f(-x) \cdot g(-x)) + \langle x^n + 1\rangle \\ &= (f(-x) + \langle x^n - 1\rangle) \cdot (g(-x) + \langle x^n + 1\rangle) \\ &= \psi\left(f(x) + \langle x^n - 1\rangle\right) \cdot \psi\left(g(x) + \langle x^n - 1\rangle\right).\end{aligned}$$

Therefore, ψ is a ring homomorphism.

Next, we show that ψ is a bijection. Since $|\mathbb{F}_q[x]/\langle x^n-1\rangle| = |\mathbb{F}_q[x]/\langle x^n+1\rangle|$, it suffices to show that $\ker(\psi) = \{\langle x^n - 1\rangle\}$. Since $\langle x^n - 1\rangle \in \ker(\psi)$. It remains to show that $\ker(\psi) \subseteq \{\langle x^n - 1\rangle\}$. Let $f(x) + \langle x^n - 1\rangle \in \ker(\psi)$. Then

$$f(-x) + \langle (-x)^n - 1\rangle = \psi\left(f(x) + \langle x^n - 1\rangle\right) = 0 + \langle x^n + 1\rangle \in \{\langle x^n - 1\rangle\}$$

which implies that $f(-x) \in \langle x^n + 1 \rangle$. Equivalently, $f(x) \in \langle (-x)^n + 1 \rangle = \langle x^n - 1 \rangle$ which implies that $f(x) + \langle x^n - 1 \rangle \in \{\langle x^n - 1 \rangle\}$.

Hence, ψ is a ring isomorphism and

$$\mathbb{F}_q[x]/\langle x^n - 1 \rangle \cong \mathbb{F}_q[x]/\langle x^n + 1 \rangle$$

as desired. □

Since properties of $\mathrm{Cir}_n(\mathbb{F}_q) \cong \mathrm{NCir}_n(\mathbb{F}_q)$ are well-known, in order to study the ring $\mathrm{NCir}_n(\mathbb{F}_q)$, it is sufficient to focus on the case where n is an even integer. However, if the result hold true for an odd integer n, it will be included as well.

3.2 Factorization of $x^n + 1$ over $\mathbb{F}_q$

Let n be a positive integer and let q be a prime power such that $\gcd(n, q) = 1$. For each $a \in \{0, 1, \ldots, n-1\}$, let

$$C_{q,n}(a) = \{q^i a \bmod n \mid i = 0, 1, 2, \ldots\}$$

be the q-cyclotomic coset of a modulo n. It is not difficult to see that

$$C_{q,n}(a) = \{q^i a \bmod n \mid 0 \le i < \mathrm{ord}_{O_n^+(a)}(q)\}$$

and $|C_{q,n}(q)| = \mathrm{ord}_{O_n^+(a)}(q)$. Moreover, $O_n^+(a) = O_n^+(j)$ for all $j \in C_{q,n}(a)$. Let $S_q(n)$ denote a complete set of representatives of the q-cyclotomic cosets modulo n and let α be a primitive nth root of unity in some extension field of $\mathbb{F}_q$. It is well known (see [1]) that

$$x^n - 1 = \prod_{a \in S_q(n)} f_a(x) \tag{3.1}$$

where

$$f_a(x) = \prod_{j \in C_{q,n}(a)} \left(x - \alpha^j\right),$$

is the minimal polynomial of α^a over $\mathbb{F}_q$ referred to as the irreducible polynomial induced by $C_{q,n}(a)$.

The factorization of $x^n - 1$ over finite fields is an algebraic tool used in the study of cyclic codes and circulant matrices. In addition, the factorization of $x^n - 1$ key to determine the factorization of $x^n + 1$ over finite fields. In [2], the factorization of $x^n + 1$ is given using equation (3.1) and [2, Lemma 2 and Lemma 3]. From [2, Lemma 2], the parity of a representative of $C_{q,n}(a)$ is independent of its choices. By [2, Lemma 3], the monic irreducible divisors of $x^n + 1$ are induced by the q-cyclotomic cosets modulo n containing odd integers. Let $SO_q(n)$ denote a complete set of representatives of the q-cyclotomic cosets containing odd integers modulo n. It follows that

$$x^n + 1 = \frac{x^{2n} - 1}{x^n - 1} = \prod_{a \in SO_q(2n)} f_a(x). \tag{3.2}$$

From [2], we have the following characterization.

Lemma 3.4 ([2, Lemma 3])**.** *Let $i \geq 0$ be an integer and let n' be an odd positive integer. Let $0 \leq \mu < 2^{i+1}n'$ and let α be a primitive $2^{i+1}n$ th root of unity. Let $f_\mu(x) = \prod_{j \in C_{q,2^{i+1}n'}(\mu)} (x - \alpha^j)$. Then the following statements are equivalent.*

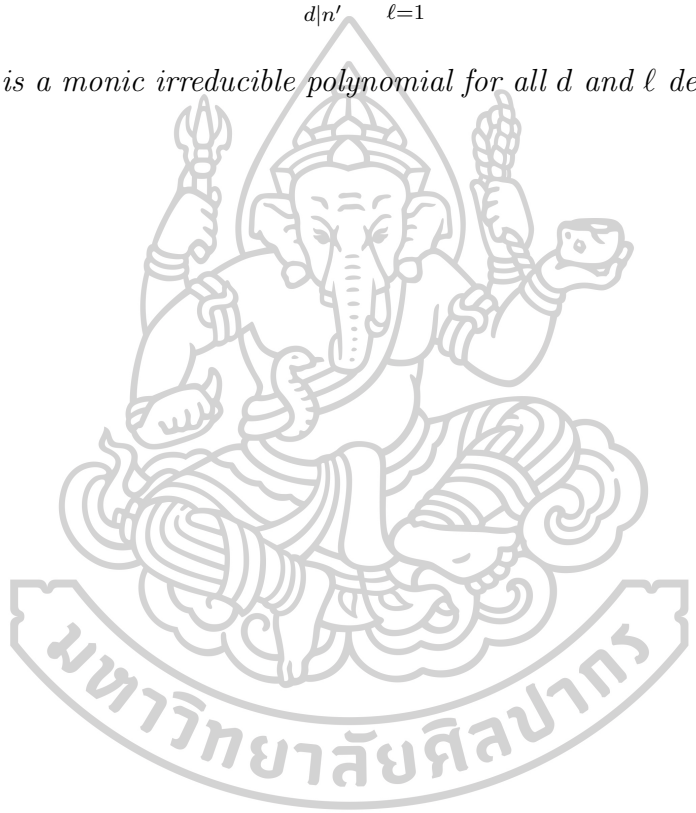
1. $f_\mu(x) | (x^{2^i n'} + 1)$.
2. *μ is odd.*
3. $2^{i+1} | \mathrm{O}^+_{2^{i+1}n'}(\mu)$.

Alteratively, the factorization of $x^n - 1$ can be sumarized in terms of (3.1) and Lemma 3.4, as follows.

Theorem 3.5. *Let $i \geq 0$ be an integer and let n' be an odd positive integer such that $\gcd(n', q) = 1$. Let $n = 2^i n'$. Then*

$$x^n + 1 = \prod_{d|n'} \prod_{\ell=1}^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} f_{d,\ell}(x), \tag{3.3}$$

where $f_{d,\ell}(x)$ is a monic irreducible polynomial for all d and ℓ defined as in (3.1).



Chapter 4

The Unit Group of $\mathrm{NCir}_n(\mathbb{F}_q)$ with $\gcd(n,q)=1$

In this chapter, the characterization and enumeration of $\mathrm{NCir}_n(\mathbb{F}_q)$ and its unit group are preseted in the case where $\gcd(n,q)=1$. The theoretical results are given together with illustrative examples.

4.1 Decomposition and Enumeration

This section focuses on the characterization and enumeration of $\mathrm{NCir}_n(\mathbb{F}_q)$ and $\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$ in the case where $\gcd(n,q)=1$.

Lemma 4.1 ([2]). *Let q be a prime power and let n be a positive integer such that $gcd(n,q)=1$. Let $a,b\in\{0,1,2,\ldots,n-1\}$. If $O_n^+(a)=O_n^+(b)$, then $|C_{q,n}(a)|=\mathrm{ord}_{O_n^+(a)}(q)=\mathrm{ord}_{O_n^+(b)}(q)=|C_{q,n}(b)|$.*

The decomposition of $\mathrm{NCir}_n(\mathbb{F}_q)$ is presented in the next theorem.

Theorem 4.2. *Let q be an odd prime power and let n be a positive integer such that $\gcd(n,q)=1$. Write $n=2^in'$ for some odd positive integer n' and integer $i\geq 0$. Then*

$$\mathrm{NCir}_n(\mathbb{F}_q)\cong\prod_{d|n'}\left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}}.$$

Proof. From (3.2) and [1, Equation 5], we have

$$x^{2^i n'}+1=\frac{x^{2^{i+1}n'}-1}{x^{2^i n'}-1}=\prod_{a\in SO_q(2^{i+1}n')} f_a\left(x\right),$$

where $f_a(x)=\prod_{j\in C_{q,2^{i+1}n'}(a)}(x-\alpha^j)$ and α is a $2^{i+1}n'$th root of unity. It is not difficult to see that $\deg(f_a(x))=\left|C_{q,2^{i+1}n'}(a)\right|=\mathrm{ord}_{\mathrm{O}^+_{2^{i+1}n'}(a)}(q)$ (see [2, page 4]). Let d be a divisor of n' and let

$$A_d=\left\{\, a\in\mathbb{Z}\,|\,0\le a<2^{i+1}n' \text{ and } \mathrm{O}^+_{2^{i+1}n'}(a)=2^{i+1}d\right\}.$$

By Theorem 2.12, we have $|A_d|=\phi\left(2^{i+1}d\right)$. By Lemma 4.1, the elements in A_d are partitioned into q-cyclotomic cosets of the same size $\left|C_{q,2^{i+1}n'}(a)\right|$. Then the number of q-cyclotomic cosets of size $\left|C_{q,2^{i+1}n'}(a)\right|=\mathrm{ord}_{2^{i+1}d}(q)$ is $\dfrac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}$.

From Proposition 3.2 and Theorem 3.5, it can be concluded that

$$\begin{aligned}\mathrm{NCir}_n(\mathbb{F}_q)&\cong\mathbb{F}_q[x]/\langle x^n+1\rangle\\&\cong\prod_{d|n'}\prod_{\ell=1}^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}}\mathbb{F}_q[x]/\langle f_{d,\ell}\rangle\\&\cong\prod_{d|n'}\left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}},\end{aligned}$$

where $f_{d,\ell}\left(x\right)$ is a monic irreducible polynomial of degree $\mathrm{ord}_{2^{i+1}d}(q)$. □

Example 4.3. Let $q=7$ and $n=12$. Then $n=2^2\cdot 3$ which implies that $i=2$ and $n'=3$. The factorization of $x^{12}+1$ over $\mathbb{F}_7$ is of the form

$$\begin{aligned}x^{12}+1=&\left(x^2+x+4\right)\left(x^2+2x+2\right)\left(x^2+3x+1\right)\left(x^2+4x+1\right)\\&\left(x^2+5x+2\right)\left(x^2+6x+4\right).\end{aligned}$$

It follows that

$$\begin{aligned}\mathrm{NCir}_{12}(\mathbb{F}_7) &\cong \mathbb{F}_{7^2} \times \mathbb{F}_{7^2} \times \mathbb{F}_{7^2} \times \mathbb{F}_{7^2} \times \mathbb{F}_{7^2} \times \mathbb{F}_{7^2} \\ &\cong \left(\mathbb{F}_{7^2}\right)^6 .\end{aligned}$$

Alternatively, by Theorem 4.2, we have

$$\begin{aligned}\mathrm{NCir}_{12}(\mathbb{F}_7) &\cong \prod_{d|n'} \left(\mathbb{F}_{7^{\mathrm{ord}_{2^{2+1}d}(7)}}\right)^{\frac{\phi\left(2^{2+1}d\right)}{\mathrm{ord}_{2^{2+1}d}(7)}} \\ &\cong \left(\mathbb{F}_{7^{\mathrm{ord}_{2^{2+1}}(7)}}\right)^{\frac{\phi\left(2^{2+1}\right)}{\mathrm{ord}_{2^{2+1}3}(7)}} \times \left(\mathbb{F}_{7^{\mathrm{ord}_{2^{2+1}3}(7)}}\right)^{\frac{\phi\left(2^{2+1}3\right)}{\mathrm{ord}_{2^{2+1}3}(7)}} \\ &\cong \left(\mathbb{F}_{7^2}\right)^{\frac{4}{2}} \times \left(\mathbb{F}_{7^2}\right)^{\frac{8}{2}} \\ &\cong \left(\mathbb{F}_{7^2}\right)^6 .\end{aligned}$$

From Example 4.3, it can be observed that the complexity of factoring the polynomial $x^n + 1$ increases whenever n becomes larger. The complexity can be reduced using Theorem 4.2.

The characterization and enumeration of $\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$ are given in the next theorem.

Theorem 4.4. *Let q be an odd prime power and let n be a positive integer such that $\gcd(n, q) = 1$. Write $n = 2^i n'$ for some odd positive integer n' and integer $i \geq 0$. Then*

$$|\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{\mathrm{ord}_{2^{i+1}d}(q)} - 1\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} .$$

Proof. By Theorem 4.2, we have

$$\mathrm{NCir}_n(\mathbb{F}_q) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}} .$$

By Lemma 2.1, we have

$$\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}} \setminus \{0\}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}}.$$

Hence,

$$|\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{\mathrm{ord}_{2^{i+1}d}(q)} - 1\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}}$$

as desired. □

Example 4.5. From Example 4.3, we have

$$\mathrm{NCir}_{12}(\mathbb{F}_7) \cong \prod_{d|n'} \left(\mathbb{F}_{7^{\mathrm{ord}_{2^{2+1}d}(7)}}\right)^{\frac{\phi\left(2^{2+1}d\right)}{\mathrm{ord}_{2^{2+1}d}(7)}}.$$

By Theorem 4.4, it follows that

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{12}(\mathbb{F}_7))| &= \prod_{d|3} \left(7^{\mathrm{ord}_{2^{2+1}d}(7)} - 1\right)^{\frac{\phi(2^{2+1}d)}{\mathrm{ord}_{2^{2+1}d}(7)}} \\
&= \left(7^{\mathrm{ord}_{2^{2+1}}(7)} - 1\right)^{\frac{\phi(2^{2+1})}{\mathrm{ord}_{2^{2+1}}(7)}} \times \left(7^{\mathrm{ord}_{2^{2+1}3}(7)} - 1\right)^{\frac{\phi(2^{2+1}3)}{\mathrm{ord}_{2^{2+1}3}(7)}} \\
&= \left(7^2 - 1\right)^2 \times \left(7^2 - 1\right)^4 \\
&= 48^6.
\end{aligned}$$

Examples of nega-circulant matrices which are units in $\mathrm{NCir}_{12}(\mathbb{F}_7)$ are given below. Let

$$A_1 = \mathrm{ncirc}(3, 6, 5, 6, 4, 6, 2, 3, 4, 3, 1, 4)$$

and

$$A_2 = \mathrm{ncirc}(6, 5, 3, 4, 2, 5, 4, 2, 6, 3, 6, 6).$$

Since $\det(A_1) = 6 \neq 0$ and $\det(A_2) = 5 \neq 0$, we have $A_1, A_2 \in \mathcal{U}(\mathrm{NCir}_{12}(\mathbb{F}_7))$.

In the remaining parts of this section, we mainly focus on the simplicity of the formulas in Theorem 4.4. Precisely, $\phi(2^{i+1}d)$ and $\mathrm{ord}_{2^{i+1}d}(q)$ are simplified using number theoretical results. The results are presented into two cases where $q \equiv 1 \bmod 4$ and where $q \equiv 3 \bmod 4$.

First, the simplification formula for $|\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))|$ is given for the case where $q \equiv 1 \bmod 4$.

Theorem 4.6. *Let q be a prime power such that $q \equiv 1 \bmod 4$ and let n' be an odd positive integer such that $\gcd(q, n') = 1$ and $\mathrm{ord}_{n'}(q)$ is odd. Let β be the positive integer such that $2^\beta \| (q^2 - 1)$. Then*

$$|\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q))| = \begin{cases} \prod\limits_{d|n'} \left(q^{\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}} & \text{if } i = 0, \\ \prod\limits_{d|n'} \left(q^{\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_d(q)}} & \text{if } 1 \le i \le \beta - 2, \\ \prod\limits_{d|n'} \left(q^{2^{i-\beta+2}\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi\left(2^{\beta-1}d\right)}{\mathrm{ord}_d(q)}} & \text{if } i \ge \beta - 1. \end{cases} \tag{4.1}$$

Proof. From Theorem 4.2, we have

$$\mathrm{NCir}_{2^i n'}(\mathbb{F}_q) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}}. \tag{4.2}$$

Next, we divide the proof in to the following 3 cases.

Case $i = 0$: Then $\phi(2d) = \phi(d)$ and $\mathrm{ord}_{2^1 d}(q) = \mathrm{lcm}(\mathrm{ord}_2(q), \mathrm{ord}_d(q)) = \mathrm{lcm}(1, \mathrm{ord}_d(q)) = \mathrm{ord}_d(q)$ for all divisors d of n'. From (4.2), it can be deduced that

$$\mathrm{NCir}_{n'}(\mathbb{F}_q) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^1 d}(q)}}\right)^{\frac{\phi\left(2^1 d\right)}{\mathrm{ord}_{2^1 d}(q)}} = \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_d(q)}}\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}}.$$

By Lemma 2.1, it follows that

$$\mathcal{U}(\mathrm{NCir}_{n'}(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_d(q)}} \setminus \{0\}\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}},$$

and hence,

$$|\mathcal{U}(\mathrm{NCir}_{n'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}}.$$

Case $1 \leq i \leq \beta - 2$: Since $\mathrm{ord}_{n'}(q)$ is odd, we have $\mathrm{ord}_d(q)$ is odd for all divisors d of n'. From [1, Lemma 5], we have $\mathrm{ord}_{2^{i+1}}(q) = 1$ for all $1 \leq i \leq \beta - 2$. It follows that $\mathrm{ord}_{2^{i+1}d}(q) = \mathrm{lcm}(\mathrm{ord}_{2^{i+1}}(q), \mathrm{ord}_d(q)) = \mathrm{lcm}(1, \mathrm{ord}_d(q)) = \mathrm{ord}_d(q)$ for all divisors d of n'. From (4.2), we have

$$\mathrm{NCir}_{2^i n'}(\mathbb{F}_q) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}} = \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_d(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_d(q)}}.$$

By Lemma 2.1, we have

$$\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_d(q)}} \setminus \{0\}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_d(q)}}$$

and

$$|\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_d(q)}}.$$

Case $i \geq \beta - 1$: Since $\mathrm{ord}_{n'}(q)$ is odd, it follows that d is odd,

$$\phi\left(2^{i+1}d\right) = 2^i\phi(d) = 2^{i-\beta+2}2^{\beta-2}\phi(d) = 2^{i-\beta+2}\phi(2^{\beta-1}d),$$

and $\mathrm{ord}_d(q)$ is odd for all divisors d of n'. From [1, Lemma 5], we have $\mathrm{ord}_{2^{i+1}}(q) = 2^{i-\beta+2}$ for all $i \geq \beta - 1$. It follows that

$$\mathrm{ord}_{2^{i+1}d}(q) = \mathrm{lcm}(\mathrm{ord}_{2^{i+1}}(q), \mathrm{ord}_d(q)) = \mathrm{lcm}(2^{i-\beta+2}, \mathrm{ord}_d(q)) = 2^{i-\beta+2}\mathrm{ord}_d(q)$$

for all divisors d of n'. From (4.2), it can be deduced that

$$\begin{aligned}\mathrm{NCir}_{2^in'}(\mathbb{F}_q) &\cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}} \\ &= \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\beta+2}\mathrm{ord}_d(q)}}\right)^{\frac{2^{i-\beta+2}\phi\left(2^{\beta-1}d\right)}{2^{i-\beta+2}\mathrm{ord}_d(q)}} \\ &= \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\beta+2}\mathrm{ord}_d(q)}}\right)^{\frac{\phi\left(2^{\beta-1}d\right)}{\mathrm{ord}_d(q)}}.\end{aligned}$$

By Lemma 2.1, we have

$$\mathcal{U}(\mathrm{NCir}_{2^in'}(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\beta+2}\mathrm{ord}_d(q)}} \setminus \{0\}\right)^{\frac{\phi\left(2^{\beta-1}d\right)}{\mathrm{ord}_d(q)}}$$

which imples that

$$|\mathcal{U}(\mathrm{NCir}_{2^in'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{2^{i-\beta+2}\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi\left(2^{\beta-1}d\right)}{\mathrm{ord}_d(q)}}$$

as desired. □

Remark 4.7. In Theorem 4.6, a simplified formula for $|\mathcal{U}(\mathrm{NCir}_{2^in'}(\mathbb{F}_q))|$ is presented for $q \equiv 1 \bmod 4$. For the algebraic structures of $\mathrm{NCir}_{2^in'}(\mathbb{F}_q)$ and $\mathcal{U}(\mathrm{NCir}_{2^in'}(\mathbb{F}_q))$, recursive factorizations of $x^{2^in'}+1$ in [1, Theorem 2(ii)] are useful.

1. For $1 \le i \le \beta - 2$, we have

$$x^{2^in'} + 1 = \prod_{a \in SO_q(2^in')} g_a(x)\, g_{a+2^in'}(x),$$

where $g_a(x) = \prod_{j \in C_{q,2^{i+1}n'}(a)} (x - \gamma^j)$ and γ is a primitive $2^{i+1}n'$th root of unity. In this case, $\deg(g_a(x)) = \left|C_{q,2^{i+1}n'}(a)\right| = \left|C_{q,2^{i+1}n'}(a+2^in')\right| = \deg(g_{a+2^in'}(x))$.

2. For $k \geq 0$, we have

$$x^{2^{\beta-2+k}n'} + 1 = \prod_{a \in SO_q\left(2^{\beta-1}n'\right)} f_a\left(x^{2^k}\right)$$

where $f_a(x) = \prod_{j \in C_{q,2^{\beta-1}n'}(a)} (x - \alpha^j)$ and α is a primitive $2^{\beta-1}n'$th root of unity.

Example 4.8. Let $q = 5$ and $n' = 11$. Then $q \equiv 1 \bmod 4$ and $\mathrm{ord}_{11}(5) = 5$. It is easy to see that $2^3 || (5^2 - 1)$ which impies that $\beta = 3$. By Theorem 4.6, we have the follwing results:

Case $i = 0$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{11}(\mathbb{F}_5))| &= \prod_{d|11} \left(5^{\mathrm{ord}_d(5)} - 1\right)^{\frac{\phi(d)}{\mathrm{ord}_d(5)}} \\
&= \left(5^{\mathrm{ord}_1(5)} - 1\right)^{\frac{\phi(1)}{\mathrm{ord}_1(5)}} \times \left(5^{\mathrm{ord}_{11}(5)} - 1\right)^{\frac{\phi(11)}{\mathrm{ord}_{11}(5)}} \\
&= \left(5^1 - 1\right)^1 \times \left(5^5 - 1\right)^{\frac{10}{5}}.
\end{aligned}$$

Case $i = 1$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{22}(\mathbb{F}_5))| &= \prod_{d|11} \left(5^{\mathrm{ord}_d(5)} - 1\right)^{\frac{\phi(2^2 d)}{\mathrm{ord}_d(5)}} \\
&= \left(5^{\mathrm{ord}_1(5)} - 1\right)^{\frac{\phi(4)}{\mathrm{ord}_1(5)}} \times \left(5^{\mathrm{ord}_{11}(5)} - 1\right)^{\frac{\phi(44)}{\mathrm{ord}_{11}(5)}} \\
&= \left(5^1 - 1\right)^{\frac{2}{1}} \times \left(5^5 - 1\right)^{\frac{20}{5}}.
\end{aligned}$$

Case $i = 2$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{44}(\mathbb{F}_5))| &= \prod_{d|11} \left(5^{2\mathrm{ord}_d(5)} - 1\right)^{\frac{\phi\left(2^2 d\right)}{\mathrm{ord}_d(5)}} \\
&= \left(5^{2\mathrm{ord}_1(5)} - 1\right)^{\frac{\phi(4)}{\mathrm{ord}_1(5)}} \times \left(5^{2\mathrm{ord}_{11}(5)} - 1\right)^{\frac{\phi(44)}{\mathrm{ord}_{11}(5)}} \\
&= \left(5^2 - 1\right)^{\frac{2}{1}} \times \left(5^{2\cdot 5} - 1\right)^{\frac{20}{5}} \\
&= (5^2 - 1)^2 \times (5^{10} - 1)^4.
\end{aligned}$$

Case $i = 3$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{88}(\mathbb{F}_5))| &= \prod_{d|11} \left(5^{2^2\mathrm{ord}_d(5)} - 1\right)^{\frac{\phi\left(2^2 d\right)}{\mathrm{ord}_d(5)}} \\
&= \left(5^{4\mathrm{ord}_1(5)} - 1\right)^{\frac{\phi(4)}{\mathrm{ord}_1(5)}} \times \left(5^{4\mathrm{ord}_{11}(5)} - 1\right)^{\frac{\phi(44)}{\mathrm{ord}_{11}(5)}} \\
&= \left(5^4 - 1\right)^{\frac{2}{1}} \times \left(5^{4\times 5} - 1\right)^{\frac{20}{5}} \\
&= (5^4 - 1)^2 \times (5^{20} - 1)^4.
\end{aligned}$$

In the following theorem, a simplified formula for $|\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q)|$ is presented in the case where $q \equiv 3 \bmod 4$.

Theorem 4.9. *Let q be a prime power such that $q \equiv 3 \bmod 4$ and let n' be an odd positive integer such that $\gcd(q, n') = 1$ and $\mathrm{ord}_{n'}(q)$ is odd. Let β be the positive integer such that $2^\beta \| (q^2 - 1)$. Then*

$$|\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q))| = \begin{cases}
\prod_{d|n'} (q^{\mathrm{ord}_d(q)} - 1)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}} & \text{if } i = 0, \\
\prod_{d|n'} \left(q^{2\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}} & \text{if } i = 1, \\
\prod_{d|n'} (q^{2\mathrm{ord}_d(q)} - 1)^{\frac{\phi(2^i d)}{\mathrm{ord}_d(q)}} & \text{if } 2 \le i \le \beta - 1, \\
\prod_{d|n'} \left(q^{2^{i-\beta+2}\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi\left(2^{\beta-1} d\right)}{\mathrm{ord}_d(q)}} & \text{if } i \ge \beta.
\end{cases} \tag{4.3}$$

Proof. From Theorem 4.2, we have

$$\mathrm{NCir}_{2^i n'}(\mathbb{F}_q) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}}. \tag{4.4}$$

The proof is given in the following 4 cases.

Case $i = 0$: Then $\phi(2d) = \phi(d)$ and $\mathrm{ord}_{2^1 d}(q) = \mathrm{lcm}(\mathrm{ord}_2(q), \mathrm{ord}_d(q)) = \mathrm{lcm}(1, \mathrm{ord}_d(q)) = \mathrm{ord}_d(q)$ for all divisors d of n'. From (4.4), it can be deduced that

$$\mathrm{NCir}_{n'}(\mathbb{F}_q) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^1 d}(q)}}\right)^{\frac{\phi\left(2^1 d\right)}{\mathrm{ord}_{2^1 d}(q)}} = \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_d(q)}}\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}}.$$

By Lemma 2.1, we have

$$\mathcal{U}(\mathrm{NCir}_{n'}(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_d(q)}} \setminus \{0\}\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}}$$

and

$$|\mathcal{U}(\mathrm{NCir}_{n'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}}.$$

Case $i = 1$: Since $q \equiv 3 \bmod 4$ and $\mathrm{ord}_{n'}(q)$ is odd, we have $\mathrm{ord}_{2^2}(q) = 2$ and $\mathrm{ord}_d(q)$ is odd for all divisors d of n'. It follows that $\phi(4d) = 2\phi(d)$ and

$$\mathrm{ord}_{2^2 d}(q) = \mathrm{lcm}(\mathrm{ord}_{2^2}(q), \mathrm{ord}_d(q)) = \mathrm{lcm}(2, \mathrm{ord}_d(q)) = 2\mathrm{ord}_d(q)$$

for all divisors d of n'. From (4.4), it can be deduced that

$$\mathrm{NCir}_{2n'}(\mathbb{F}_q) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^2 d}(q)}}\right)^{\frac{\phi\left(2^2 d\right)}{\mathrm{ord}_{2^2 d}(q)}} = \prod_{d|n'} \left(\mathbb{F}_{q^{2\mathrm{ord}_d(q)}}\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}}.$$

By Lemma 2.1, it follows that

$$\mathcal{U}(\mathrm{NCir}_{2n'}(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{2\mathrm{ord}_d(q)}} \setminus \{0\}\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}}$$

and

$$|\mathcal{U}(\mathrm{NCir}_{2n'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{2\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi(d)}{\mathrm{ord}_d(q)}}.$$

Case $2 \leq i \leq \beta - 1$. Since $\mathrm{ord}_{n'}(q)$ is odd, $\mathrm{ord}_d(q)$ is odd for all divisors d of n'. From [1, Lemma 4], we have $\mathrm{ord}_{2^{i+1}}(q) = 2$ for all $1 \leq i \leq \beta - 2$. It follows that $\mathrm{ord}_{2^{i+1}d}(q) = \mathrm{lcm}(\mathrm{ord}_{2^{i+1}}(q), \mathrm{ord}_d(q)) = \mathrm{lcm}(2, \mathrm{ord}_d(q)) = 2\mathrm{ord}_d(q)$ for all divisors d of n'. From (4.4), we have

$$\begin{aligned}
\mathrm{NCir}_{2^i n'}(\mathbb{F}_q) &\cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}} \\
&= \prod_{d|n'} \left(\mathbb{F}_{q^{2\mathrm{ord}_d(q)}}\right)^{\frac{2\phi\left(2^i d\right)}{2\mathrm{ord}_d(q)}} \\
&= \prod_{d|n'} \left(\mathbb{F}_{q^{2\mathrm{ord}_d(q)}}\right)^{\frac{\phi\left(2^i d\right)}{\mathrm{ord}_d(q)}}.
\end{aligned}$$

By Lemma 2.1, it follows that

$$\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{2\mathrm{ord}_d(q)}} \setminus \{0\}\right)^{\frac{\phi\left(2^i d\right)}{\mathrm{ord}_d(q)}}$$

and

$$|\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{2\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi(2^i d)}{\mathrm{ord}_d(q)}}.$$

Case $i \geq \beta$: Since $\mathrm{ord}_{n'}(q)$ is odd, we have that d is odd,

$$\phi\left(2^{i+1}d\right) = 2^i\phi(d) = 2^{i-\beta+2}2^{\beta-2}\phi(d) = 2^{i-\beta+2}\phi(2^{\beta-1}d),$$

and $\mathrm{ord}_d(q)$ is odd for all divisors d of n'. From [1, Lemma 4], we have $\mathrm{ord}_{2^{i+1}}(q) = 2^{i-\beta+2}$ for all $i \geq \beta$. Then

$$\mathrm{ord}_{2^{i+1}d}(q) = \mathrm{lcm}(\mathrm{ord}_{2^{i+1}}(q), \mathrm{ord}_d(q)) = \mathrm{lcm}(2^{i-\beta+2}, \mathrm{ord}_d(q)) = 2^{i-\beta+2}\mathrm{ord}_d(q)$$

for all divisors d of n'. From (4.4), it follows that

$$\begin{aligned}\mathrm{NCir}_{2^in'}(\mathbb{F}_q) &\cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}} \\ &= \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\beta+2}\mathrm{ord}_d(q)}}\right)^{\frac{2^{i-\beta+2}\phi\left(2^{\beta-1}d\right)}{2^{i-\beta+2}\mathrm{ord}_d(q)}} \\ &= \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\beta+2}\mathrm{ord}_d(q)}}\right)^{\frac{\phi\left(2^{\beta-1}d\right)}{\mathrm{ord}_d(q)}}.\end{aligned}$$

By Lemma 2.1, it can be deduced that

$$\mathcal{U}(\mathrm{NCir}_{2^in'}(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\beta+2}\mathrm{ord}_d(q)}} \setminus \{0\}\right)^{\frac{\phi\left(2^{\beta-1}d\right)}{\mathrm{ord}_d(q)}}$$

and

$$|\mathcal{U}(\mathrm{NCir}_{2^in'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{2^{i-\beta+2}\mathrm{ord}_d(q)} - 1\right)^{\frac{\phi\left(2^{\beta-1}d\right)}{\mathrm{ord}_d(q)}}$$

as desired. □

Remark 4.10. In Theorem 4.9, a simplified formula for $|\mathcal{U}(\mathrm{NCir}_{2^in'}(\mathbb{F}_q))|$ is presented in the case where $q \equiv 3 \bmod 4$. For the algebraic structures of $\mathrm{NCir}_{2^in'}(\mathbb{F}_q)$ and $\mathcal{U}(\mathrm{NCir}_{2^in'}(\mathbb{F}_q))$, recursive factorizations of $x^{2^in'}+1$ in [1, Theorem 1(ii)] are useful.

1. For $2 \le i \le \beta - 1$, we have

$$x^{2^in'} + 1 = \prod_{a \in SO_q(2^in')} g_a(x)\, g_{a+2^in'}(x)$$

where $g_a(x) = \prod_{j \in C_{q,2^{i+1}n'}(a)} (x - \gamma^j)$ and γ is a primitive $2^{i+1}n'$th root of unity. In this case, $\deg(g_a(x)) = \left|C_{q,2^{i+1}n'}(a)\right| = \left|C_{q,2^{i+1}n'}(a+2^in')\right| = \deg(g_{a+2^in'}(x))$.

2. For $k \geq 0$,

$$x^{2^{\beta-1+k}n'} + 1 = \prod_{a \in SO_q\left(2^\beta n'\right)} f_a\left(x^{2^k}\right),$$

where $f_a(x) = \prod_{j \in C_{q,2^\beta n'}(a)} (x - \alpha^j)$ and α is a primitive $2^\beta n'$th root of unity .

Example 4.11. Let $q = 3$ and $n' = 11$. Then $q \equiv 3 \bmod 4$ and $\mathrm{ord}_{11}(3) = 5$. It is easy to see that $2^3 || (3^2 - 1)$ which implies that $\beta = 3$. By Theorem 4.9, we have the following results:

Case $i = 0$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{11}(\mathbb{F}_3))| &= \prod_{d|11} \left(3^{\mathrm{ord}_d(3)} - 1\right)^{\frac{\phi(d)}{\mathrm{ord}_d(3)}} \\
&= \left(3^{\mathrm{ord}_1(3)} - 1\right)^{\frac{\phi(1)}{\mathrm{ord}_1(3)}} \times \left(3^{\mathrm{ord}_{11}(3)} - 1\right)^{\frac{\phi(11)}{\mathrm{ord}_{11}(3)}} \\
&= \left(3^1 - 1\right)^{\frac{1}{1}} \times \left(3^5 - 1\right)^{\frac{10}{5}} \\
&= \left(3^1 - 1\right)^1 \times \left(3^5 - 1\right)^2.
\end{aligned}$$

Case $i = 1$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{22}(\mathbb{F}_3))| &= \prod_{d|11} \left(3^{2\mathrm{ord}_d(3)} - 1\right)^{\frac{\phi(d)}{\mathrm{ord}_d(3)}} \\
&= \left(3^{2\mathrm{ord}_1(3)} - 1\right)^{\frac{\phi(1)}{\mathrm{ord}_1(3)}} \times \left(3^{2\mathrm{ord}_{11}(3)} - 1\right)^{\frac{\phi(11)}{\mathrm{ord}_{11}(3)}} \\
&= \left(3^{2\cdot 1} - 1\right)^{\frac{1}{1}} \times \left(3^{2\cdot 5} - 1\right)^{\frac{10}{5}} \\
&= \left(3^2 - 1\right)^1 \times \left(3^{10} - 1\right)^2.
\end{aligned}$$

Case $i = 2$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{44}(\mathbb{F}_3))| &= \prod_{d|11} \left(3^{2\mathrm{ord}_d(3)} - 1\right)^{\frac{\phi(2^2 d)}{\mathrm{ord}_d(3)}} \\
&= \left(3^{2\mathrm{ord}_1(3)} - 1\right)^{\frac{\phi(4)}{\mathrm{ord}_1(3)}} \times \left(3^{2\mathrm{ord}_{11}(3)} - 1\right)^{\frac{\phi(44)}{\mathrm{ord}_{11}(3)}} \\
&= \left(3^{2\cdot 1} - 1\right)^{\frac{2}{1}} \times \left(3^{2\cdot 5} - 1\right)^{\frac{20}{5}} \\
&= \left(3^2 - 1\right)^2 \times \left(3^{10} - 1\right)^4.
\end{aligned}$$

Case $i = 3$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{88}(\mathbb{F}_3))| &= \prod_{d|11} \left(3^{2^2\mathrm{ord}_d(3)} - 1\right)^{\frac{\phi(2^2 d)}{\mathrm{ord}_d(3)}} \\
&= \left(3^{2^2\mathrm{ord}_1(3)} - 1\right)^{\frac{\phi(4)}{\mathrm{ord}_1(3)}} \times \left(3^{2^2\mathrm{ord}_{11}(3)} - 1\right)^{\frac{\phi(44)}{\mathrm{ord}_{11}(3)}} \\
&= \left(3^{4\cdot 1} - 1\right)^{\frac{2}{1}} \times \left(3^{4\cdot 5} - 1\right)^{\frac{20}{5}} \\
&= \left(3^4 - 1\right)^2 \times \left(3^{20} - 1\right)^4.
\end{aligned}$$

While Theorems 4.6 and 4.9 have taken care of the the case where $\mathrm{ord}_{n'}(q)$ is odd, the following theorem extends the study to cover the case where $\mathrm{ord}_{n'}(q)$ is even for some certain n'.

Theorem 4.12. *Let q be an odd prime power and let n' be a positive integer such that $\gcd(q, n') = 1$ and $\mathrm{ord}_{n'}(q)$ is even. Let λ be the positive integer such that $2^\lambda || \mathrm{ord}_{n'}(q)$, and let β be the positive integer such that $2^\beta || (q^2 - 1)$. Then*

$$|\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{2^{i-\lambda-\beta+1}\mathrm{ord}_{2^{\lambda+\beta}d}(q)} - 1\right)^{\frac{\phi\left(2^{\lambda+\beta}d\right)}{\mathrm{ord}_{2^{\lambda+\beta}d}(q)}}$$

for all $i \geq \lambda + \beta - 1$.

Proof. Let i be a positive integer such that $i \geq \lambda + \beta - 1$. From [1, Lemma 4], we have $\mathrm{ord}_{2^{i+1}}(q) = 2\mathrm{ord}_{2^i}(q)$ and $\mathrm{ord}_{2^i}(q) = 2^{i-\beta+1} \geq 2^\lambda$ since $i \geq \lambda + \beta - 1 \geq \beta$. Since $2^\lambda || \mathrm{ord}_{n'}(q)$, we have $\frac{\mathrm{ord}_d(q)}{2^\gamma}$ is odd for some integer $\gamma \leq \lambda$. It follows that

$$\begin{aligned}
\mathrm{ord}_{2^{i+1}d}(q) &= \mathrm{lcm}(\mathrm{ord}_{2^{i+1}}(q), \mathrm{ord}_d(q)) \\
&= \mathrm{lcm}(2\mathrm{ord}_{2^i}(q), \mathrm{ord}_d(q)) \\
&= 2\mathrm{lcm}(\mathrm{ord}_{2^i}(q), \mathrm{ord}_d(q)) \\
&= 2\mathrm{ord}_{2^i d}(q)
\end{aligned}$$

for all divisors d of n'. Continue this process, we have

$$\mathrm{ord}_{2^{i+1}d}(q) = 2^{i-\lambda-\beta+1}\mathrm{ord}_{2^{\lambda+\beta}d}(q).$$

We note that

$$\phi\left(2^{i+1}d\right) = 2^i\phi(d) = 2^{i-\lambda-\beta+1}2^{\lambda+\beta-1}\phi(d) = 2^{i-\lambda-\beta+1}\phi(2^{\lambda+\beta}d)$$

for all divisors d of n'. From Theorem 4.2, we have

$$\begin{aligned}
\mathrm{NCir}_{2^i n'}(\mathbb{F}_q) &\cong \prod_{d|n'} \left(\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}\right)^{\frac{\phi\left(2^{i+1}d\right)}{\mathrm{ord}_{2^{i+1}d}(q)}} \\
&= \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\lambda-\beta+1}\mathrm{ord}_{2^{\lambda+\beta}d}(q)}}\right)^{\frac{2^{i-\lambda-\beta+1}\phi(2^{\lambda+\beta}d)}{2^{i-\lambda-\beta+1}\mathrm{ord}_{2^{\lambda+\beta}d}(q)}} \\
&= \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\lambda-\beta+1}\mathrm{ord}_{2^{\lambda+\beta}d}(q)}}\right)^{\frac{\phi(2^{\lambda+\beta}d)}{\mathrm{ord}_{2^{\lambda+\beta}d}(q)}}.
\end{aligned}$$

Then

$$\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q)) \cong \prod_{d|n'} \left(\mathbb{F}_{q^{2^{i-\lambda-\beta+1}\mathrm{ord}_{2^{\lambda+\beta}d}(q)}} \setminus \{0\}\right)^{\frac{\phi(2^{\lambda+\beta}d)}{\mathrm{ord}_{2^{\lambda+\beta}d}(q)}}$$

by Lemma 2.1. Therefore, we have

$$|\mathcal{U}(\mathrm{NCir}_{2^i n'}(\mathbb{F}_q))| = \prod_{d|n'} \left(q^{2^{i-\lambda-\beta+1}\mathrm{ord}_{2^{\lambda+\beta}d}(q)} - 1\right)^{\frac{\phi(2^{\lambda+\beta}d)}{\mathrm{ord}_{2^{\lambda+\beta}d}(q)}}$$

as desired. □

Example 4.13. Let $q = 3$ and $n' = 5$. Then $\mathrm{ord}_5(3) = 4$ and $3^2 - 1 = 8$ which implies that $\lambda = 2$ and $\beta = 3$. By Theorem 4.12, we have the following results.

Case $i = 4$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{2^4.5}(\mathbb{F}_3))| &= \prod_{d|5} \left(3^{\mathrm{ord}_{2^5 d}(3)} - 1\right)^{\frac{\phi\left(2^5 d\right)}{\mathrm{ord}_{2^5 d}(3)}} \\
&= \left(3^8 - 1\right)^{\frac{16}{8}} \times \left(3^8 - 1\right)^{\frac{64}{8}} \\
&= \left(3^8 - 1\right)^2 \times \left(3^8 - 1\right)^8 \\
&= \left(3^8 - 1\right)^{10}.
\end{aligned}$$

Case $i = 5$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{2^5.5}(\mathbb{F}_3))| &= \prod_{d|5} \left(3^{2^1 \mathrm{ord}_{2^5 d}(3)} - 1\right)^{\frac{\phi\left(2^5 d\right)}{\mathrm{ord}_{2^5 d}(3)}} \\
&= \left(3^{16} - 1\right)^{\frac{16}{8}} \times \left(3^{16} - 1\right)^{\frac{64}{8}} \\
&= \left(3^{16} - 1\right)^2 \times \left(3^{16} - 1\right)^8 \\
&= \left(3^{16} - 1\right)^{10}.
\end{aligned}$$

Case $i = 6$:

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{2^5.5}(\mathbb{F}_3))| &= \prod_{d|5} \left(3^{2^2 \mathrm{ord}_{2^5 d}(3)} - 1\right)^{\frac{\phi\left(2^5 d\right)}{\mathrm{ord}_{2^5 d}(3)}} \\
&= \left(3^{32} - 1\right)^{\frac{16}{8}} \times \left(3^{32} - 1\right)^{\frac{64}{8}} \\
&= \left(3^{32} - 1\right)^2 \times \left(3^{32} - 1\right)^8 \\
&= \left(3^{32} - 1\right)^{10}.
\end{aligned}$$

From Examples 4.8, 4.11 and 4.13, it turns out that the degrees of each monic irreducible polynomials in the factorization of $x^{2^i n'}+1$ are recursively related to the case of $2^{i-1}n'$ for all $i \leq \lambda + \beta - 1$.

The following tables present the number of units in $\mathrm{NCir}_n(\mathbb{F}_q)$, where $q = 3, 5, 7, 9$ and $\gcd(n, q) = 1$.

q	n	$\lvert\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$
3	1	2
	2	8
	4	64
	5	160
	7	1456
	8	6400
	10	51200
	11	117128
	13	913952
	14	4239872
	16	43033600
	17	86093440
	19	774840976
	20	2621440000
	22	27893330432
	23	62761410632
	25	557885504000

q	n	$\lvert\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$
5	1	4
	2	16
	3	96
	4	576
	6	9216
	7	62496
	8	389376
	9	1499904
	11	39037504
	12	191102976
	13	971882496
	14	3905750016
	16	152587109376
	17	610351562496
	18	2249712009216
	19	15258773437504
	21	366140629499904

q	n	$\lvert\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$
7	1	6
	2	48
	3	216
	4	2304
	5	14400
	6	110592
	8	5308416
	9	25264224
	10	276480000
	11	1694851488

q	n	$\lvert\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$
9	1	8
	2	64
	4	4096
	5	51200
	7	4239872
	8	40960000
	10	2621440000
	11	27893330432
	13	2247064322048
	14	17976514576384

Table 4.1: The enumeration of unit group of $\mathrm{NCir}_n(\mathbb{F}_q)$ determined by Theorem 4.4.

4.2 Some special cases

This section presents formulas for $|\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))|$ for some special n. These can be viewed as corollaries of the results in Section 4.1. However, it is worth to restate them in explicit form.

Theorem 4.14. *Let q be an odd prime power. Then*

$$|\mathcal{U}(\mathrm{NCir}_2(\mathbb{F}_q))| = \begin{cases} q^2-1 & \text{if } q \equiv 3 \pmod 4, \\ (q-1)^2 & \text{if } q \equiv 1 \pmod 4. \end{cases} \tag{4.5}$$

Proof. We consider the following two cases.

Case $q \equiv 3 \pmod 4$: We have $i = 1$ and $n' = 1$. By Theorem 4.9, it follows that

$$|\mathcal{U}(\mathrm{NCir}_2(\mathbb{F}_q))| = \left(q^{2\mathrm{ord}_1(q)} - 1\right)^{\frac{\phi(1)}{\mathrm{ord}_1(q)}} = q^2 - 1.$$

Case $q \equiv 1 \pmod 4$: We have $i = 1$ and $n' = 1$. By Theorem 4.6,

$$|\mathcal{U}(\mathrm{NCir}_2(\mathbb{F}_q))| = \left(q^{\mathrm{ord}_{2^2}(q)} - 1\right)^{\frac{\phi\left(2^2\right)}{\mathrm{ord}_{2^2}(q)}} = (q-1)^2.$$

The proof is completed. □

Theorem 4.15. *Let q be an odd prime power. Then*

$$|\mathcal{U}(\mathrm{NCir}_4(\mathbb{F}_q))| = \begin{cases} (q^2-1)^2 & \text{if } \mathrm{ord}_8(q) = 2, \\ (q-1)^4 & \text{if } \mathrm{ord}_8(q) = 1. \end{cases} \tag{4.6}$$

Proof. We consider the two cases.

Case $\mathrm{ord}_8(q) = 2$: We have that $i = 2$ and $n' = 1$. Then $\phi(2^{i+1}) = \phi(8) = 4$. By Theorem 4.4, it can be deduced that

$$|\mathcal{U}(\mathrm{NCir}_4(\mathbb{F}_q))| = \left(q^{\mathrm{ord}_8(q)} - 1\right)^{\frac{\phi(8)}{\mathrm{ord}_8(q)}} = \left(q^2-1\right)^{\frac{4}{2}} = \left(q^2-1\right)^2.$$

Case $\mathrm{ord}_8(q) = 1$: we have that $i = 2$ and $n' = 1$. Then $\phi(2^{i+1}) = \phi(8) = 4$. By Theorem 4.4, it follows that

$$|\mathcal{U}(\mathrm{NCir}_4(\mathbb{F}_q))| = \left(q^{\mathrm{ord}_8(q)} - 1\right)^{\frac{\phi(8)}{\mathrm{ord}_8(q)}} = (q-1)^{\frac{4}{1}} = (q-1)^4.$$

This completes the proof. □

Theorem 4.16. *Let q be an odd prime power and let i be a positive integer. Then*

$$|\mathcal{U}(\mathrm{NCir}_{2^i}(\mathbb{F}_q))| = \left(q^{\mathrm{ord}_{2^{i+1}}(q)} - 1\right)^{\frac{2^i}{\mathrm{ord}_{2^{i+1}}(q)}}. \tag{4.7}$$

Proof. We have that $n' = 1$ and $\phi\left(2^{i+1}\right) = 2^i$. By Theorem 4.4, we have

$$|\mathcal{U}(\mathrm{NCir}_{2^i}(\mathbb{F}_q))| = \left(q^{\mathrm{ord}_{2^{i+1}}(q)} - 1\right)^{\frac{2^i}{\mathrm{ord}_{2^{i+1}}(q)}}$$

as desired. □

Theorem 4.17. *Let q be an odd prime power and let p be an odd prime such that $p \nmid q$. Then*

$$|\mathcal{U}(\mathrm{NCir}_p(\mathbb{F}_q))| = (q-1)\left(q^{\mathrm{ord}_{2p}(q)} - 1\right)^{\frac{p-1}{\mathrm{ord}_{2p}(q)}}. \tag{4.8}$$

Proof. We have that $i = 0$ and $n' = p$. By Theorem 4.4,

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_p(\mathbb{F}_q))| &= \prod_{d|p} \left(q^{\mathrm{ord}_{2d}(q)} - 1\right)^{\frac{\phi(2d)}{\mathrm{ord}_{2d}(q)}} \\
&= \left(q^{\mathrm{ord}_2(q)} - 1\right)^{\frac{\phi(2)}{\mathrm{ord}_2(q)}} \times \left(q^{\mathrm{ord}_{2p}(q)} - 1\right)^{\frac{\phi(2p)}{\mathrm{ord}_{2p}(q)}} \\
&= (q-1) \times \left(q^{\mathrm{ord}_{2p}(q)} - 1\right)^{\frac{p-1}{\mathrm{ord}_{2p}(q)}}
\end{aligned}$$

as desired. □

Chapter 5

General Results for the Unit Group of $\mathrm{NCir}_n(\mathbb{F}_q)$

In this chapter, we focus on a general case where $\gcd(n, q) \neq 1$. The characterization and enumeration of $\mathrm{NCir}_n(\mathbb{F}_q)$ and $\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$ are given in terms of finite chain rings and results in Chapter 4.

The following lemma is useful in the study of the algebraic structures of $\mathrm{NCir}_n(\mathbb{F}_q)$ and $\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$.

Lemma 5.1 (cf.[5, Theorem 4.3])**.** *Let $q = p^t$ be a prime power for some prime p and positive integer t. Let $\mu \geq 0$ be an integer and let $f(x)$ be a monic irreducible polynomial of degree η over $\mathbb{F}_q$. Then $\mathbb{F}_q[x]/\langle (f(x))^{p^\mu} \rangle$ is a FCCR of nilpotency index p^μ and residue field $\mathbb{F}_{q^\eta}$. Moreover,*

$$\mathbb{F}_q[x]/\langle (f(x))^{p^\mu} \rangle \cong \mathbb{F}_{q^\eta} + u\mathbb{F}_{q^\eta} + u^2\mathbb{F}_{q^\eta} + \ldots + u^{p^\mu - 1}\mathbb{F}_{q^\eta},$$

where $u^{p^\mu} = 0$.

From Lemma 5.1 and [10, Lemma 2.1], we have the following Corollary.

Corollary 5.2. *Let $q = p^t$ be a prime power for some prime p and positive integer t. Let $\mu \geq 0$ be an integer and let $f(x)$ be a monic irreducible polynomial of degree η over $\mathbb{F}_q$. Then*

$$\mathcal{U}(\mathbb{F}_q[x]/\langle (f(x))^{p^\mu} \rangle) \cong \mathbb{F}_{q^\eta} \setminus \{0\} + u\mathbb{F}_{q^\eta} + u^2\mathbb{F}_{q^\eta} + \ldots + u^{p^\mu - 1}\mathbb{F}_{q^\eta}$$

and

$$|\mathcal{U}(\mathbb{F}_q[u]/\langle u^{p^\mu}\rangle)| = (q^\eta - 1)\, q^{\eta(p^\mu - 1)}.$$

The characterization of $\mathrm{NCir}_n(\mathbb{F}_q)$ is given as follows.

Theorem 5.3. *Let $q = p^t$ be a prime power for some odd prime p and positive integer t. Let n be a positive integer and write $n = 2^i p^\mu n'$ for some odd positive integer n' such that $p \nmid n'$ and integers $i \geq 0$ and $\mu \geq 0$. Assume the factorization of $x^n + 1$ in (3.3). Then*

$$\mathrm{NCir}_n(\mathbb{F}_q) \cong \prod_{d|n'} \prod_{\ell=1}^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} R_d,$$

where $R_d = \mathbb{F}_q[x]/\langle (f_{d,1}(x))^{p^\mu}\rangle$ is a FCCR of nilpotency index p^μ and residue field $\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}$.

Proof. From (3.3), we have

$$x^n + 1 = \left(x^{2^i n'} + 1\right)^{p^\mu} = \prod_{d|n'} \prod_{\ell=1}^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} (f_{d,\ell}(x))^{p^\mu}. \tag{5.1}$$

It follows that

$$\mathrm{NCir}_{2^i n'}(\mathbb{F}_q) \cong \mathbb{F}_q[x]/\langle x^n + 1\rangle \cong \prod_{d|n'} \prod_{\ell=1}^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} \mathbb{F}_q[x]/\langle (f_{d,\ell}(x))^{p^\mu}\rangle.$$

By Lemma 5.1, we have $R_d := \mathbb{F}_q[x]/\langle (f_{d,1}(x))^{p^\mu}\rangle \cong \mathbb{F}_q[x]/\langle (f_{d,\ell}(x))^{p^\mu}\rangle$ is a FCCR of nilpotency index p^μ and residue field $\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}$ for all $d|n'$ and $\ell = 1, 2, \ldots, \frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}$. Hence,

$$\mathrm{NCir}_{2^i n'}(\mathbb{F}_q) \cong \prod_{d|n'} \prod_{\ell=1}^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} R_d$$

as desired. □

Lemma 5.4. *Let q be a prime power and let n' be an odd positive integer such that* $\gcd(n', q) = 1$. *Then*

$$\prod_{d|n'} q^{\phi(2^{i+1}d)} = q^{2^i n'}.$$

Proof. Since n' is odd, d is odd for all positive divisor of n'. Then $\gcd(2, d) = 1$. By Theorems 2.13, 2.14, and 2.15, it can be deduced that

$$\begin{aligned}\prod_{d|n'} q^{\phi(2^{i+1}d)} &= q^{\sum_{d|n'} \phi(2^{i+1}d)} \\ &= q^{\sum_{d|n'} \phi(2^{i+1})\phi(d)} \\ &= q^{\phi(2^{i+1}) \sum_{d|n'} \phi(d)} \\ &= q^{2^i n'}.\end{aligned}$$

This completes the proof. □

The algebraic structures and enumeration of $\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))$ are given in the next theorem.

Theorem 5.5. *Let $q = p^t$ be a prime power for some odd prime p and positive integer t. Let n be a positive integer and write $n = 2^i p^\mu n'$ for some odd positive integer n' such that $p \nmid n'$ and integers $i \geq 0$ and $\mu > 0$. Then the following statements hold.*

1.

$$\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q)) \cong \prod_{d|n'} \prod_{\ell=1}^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} \mathcal{U}(R_d),$$

where R_d is a FCCR of nilpotency index p^μ and residue field $\mathbb{F}_{q^{\mathrm{ord}_{2^{i+1}d}(q)}}$.

2.

$$|\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))| = q^n \prod_{d|n'} \left(1 - q^{-\mathrm{ord}_{2^{i+1}d}(q)}\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}}.$$

Proof. The first statement follows directly from Theorem 5.3.

By Corollary 5.2, we have

$$|\mathcal{U}(R_d)| = \left(q^{\mathrm{ord}_{2^{i+1}d}(q)} - 1\right) q^{(p^\mu - 1)\mathrm{ord}_{2^{i+1}d}(q)}.$$

By Lemma 5.4, it follows that

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))| &= \prod_{d|n'} \left(\left(q^{\mathrm{ord}_{2^{i+1}d}(q)} - 1\right) q^{(p^\mu - 1)\mathrm{ord}_{2^{i+1}d}(q)}\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} \\
&= \prod_{d|n'} \left(q^{\mathrm{ord}_{2^{i+1}d}(q)} - 1\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} q^{(p^\mu - 1)\phi(2^{i+1}d)} \\
&= \prod_{d|n'} q^{\phi(2^{i+1}d)} \prod_{d|n'} q^{(p^\mu - 1)\phi(2^{i+1}d)} \prod_{d|n'} \left(1 - q^{-\mathrm{ord}_{2^{i+1}d}(q)}\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} \\
&= q^{2^i n'} q^{(p^\mu - 1)2^i n'} \prod_{d|n'} \left(1 - q^{-\mathrm{ord}_{2^{i+1}d}(q)}\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} \\
&= q^{2^i p^\mu n'} \prod_{d|n'} \left(1 - q^{-\mathrm{ord}_{2^{i+1}d}(q)}\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}} \\
&= q^n \prod_{d|n'} \left(1 - q^{-\mathrm{ord}_{2^{i+1}d}(q)}\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}}.
\end{aligned}$$

This completes the second statement. □

Since $|\mathrm{NCir}_n(\mathbb{F}_q)| = q^n$, it follows that

$$\begin{aligned}
|\mathrm{NCir}_n(\mathbb{F}_q, 0)| &= |\mathrm{NCir}_n(\mathbb{F}_q)| - |\mathcal{U}(\mathrm{NCir}_n(\mathbb{F}_q))| \\
&= q^n - q^n \prod_{d|n'} \left(1 - q^{-\mathrm{ord}_{2^{i+1}d}(q)}\right)^{\frac{\phi(2^{i+1}d)}{\mathrm{ord}_{2^{i+1}d}(q)}}.
\end{aligned}$$

Example 5.6. Let $q = 3$ and $n = 30 = 2^1 \cdot 3^1 \cdot 5$, we have $i = 1, \mu = 1$ and $n' = 5$.

By Theorem 5.3, it follows that

$$\begin{aligned}
\mathrm{NCir}_{30}(\mathbb{F}_3) &\cong \prod_{d|5} \prod_{\ell=1}^{\frac{\phi(2^{1+1}d)}{\mathrm{ord}_{2^{1+1}d}(3)}} \mathbb{F}_3[x]/\langle (f_{d,1}(x))^{3^1} \rangle \\
&\cong \prod_{\ell=1}^{\frac{\phi(2^{1+1})}{\mathrm{ord}_{2^{1+1}}(3)}} \mathbb{F}_3[x]/\langle (f_{1,1}(x))^{3^1} \rangle \times \prod_{\ell=1}^{\frac{\phi(2^{1+1}5)}{\mathrm{ord}_{2^{1+1}5}(3)}} \mathbb{F}_3[x]/\langle (f_{5,1}(x))^{3^1} \rangle \\
&\cong \prod_{\ell=1}^{1} \left(\mathbb{F}_{3^{\mathrm{ord}_{2^{1+1}}(3)}} + u\mathbb{F}_{3^{\mathrm{ord}_{2^{1+1}}(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_{2^{1+1}}(3)}} \right) \\
&\quad \times \prod_{\ell=1}^{2} \left(\mathbb{F}_{3^{\mathrm{ord}_{2^{1+1.5}}(3)}} + u\mathbb{F}_{3^{\mathrm{ord}_{2^{1+1.5}}(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_{2^{1+1.5}}(3)}} \right) \\
&\cong \left(\mathbb{F}_{3^{\mathrm{ord}_4(3)}} + u\mathbb{F}_{3^{\mathrm{ord}_4(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_4(3)}} \right) \\
&\quad \times \left(\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} + u\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} \right)^2.
\end{aligned}$$

By Corollary 5.2 and Lemma 2.1, we have

$$\begin{aligned}
\mathcal{U}(\mathrm{NCir}_{30}(\mathbb{F}_3)) &\cong \mathcal{U}\left(\left(\mathbb{F}_{3^{\mathrm{ord}_4(3)}} + u\mathbb{F}_{3^{\mathrm{ord}_4(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_4(3)}} \right) \right. \\
&\qquad \left. \times \left(\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} + u\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} \right)^2 \right) \\
&\cong \mathcal{U}\left(\mathbb{F}_{3^{\mathrm{ord}_4(3)}} + u\mathbb{F}_{3^{\mathrm{ord}_4(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_4(3)}} \right) \\
&\qquad \times \mathcal{U}\left(\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} + u\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} \right)^2 \\
&\cong \left(\mathbb{F}_{3^{\mathrm{ord}_4(3)}} \setminus \{0\} + u\mathbb{F}_{3^{\mathrm{ord}_4(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_4(3)}} \right) \\
&\qquad \times \left(\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} \setminus \{0\} + u\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} \right)^2.
\end{aligned}$$

Hence,

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{30}(\mathbb{F}_3))| &= |\left(\mathbb{F}_{3^{\mathrm{ord}_4(3)}} \setminus \{0\} + u\mathbb{F}_{3^{\mathrm{ord}_4(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_4(3)}}\right) \\
&\quad \times \left(\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} \setminus \{0\} + u\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}} + u^2\mathbb{F}_{3^{\mathrm{ord}_{20}(3)}}\right)^2 | \\
&= (3^{\mathrm{ord}_4(3)} - 1)(3^{2\mathrm{ord}_4(3)}) \left((3^{\mathrm{ord}_{20}(3)} - 1)(3^{2\mathrm{ord}_{20}(3)})\right)^2 \\
&= (3^2 - 1) \cdot 3^4 \cdot (3^4 - 1)^2 \cdot (3^8)^2 \\
&= 2^9 \cdot 10^4 \cdot 3^{20}.
\end{aligned}$$

On the other hand, by a direct application of Theorem 5.5 (2), we obtain that

$$\begin{aligned}
|\mathcal{U}(\mathrm{NCir}_{30}(\mathbb{F}_3))| &= 3^{30} \prod_{d|5} \left(1 - 3^{-\mathrm{ord}_{2^{1+1}d}(3)}\right)^{\frac{\phi(2^{1+1}d)}{\mathrm{ord}_{2^{1+1}d}(3)}} \\
&= 3^{30} \cdot \left(1 - 3^{-2}\right)^{\frac{2}{2}} \cdot \left(1 - 3^{-4}\right)^{\frac{8}{4}} \\
&= 3^{30} \cdot \left(\frac{8}{9}\right) \cdot \left(\frac{80}{81}\right)^2 \\
&= 2^9 \cdot 10^4 \cdot 3^{20}.
\end{aligned}$$

Bibliography

[1] A. Boripan and S. Jitman. Revisiting the factorization of $x^n + 1$ over finite fields with applications. *Journal of Mathematics*, 2021:1–10, 2021.

[2] A. Boripan and S. Jitman. SRIM and SCRIM factors of x^n+1 over finite fields and their applications. *Discrete Mathematics, Algorithms and Applications*, 13(01):2050098, 2021.

[3] D. Burton. *Elementary Number Theory*. McGraw-Hill, 2011.

[4] B. Chen, Y. Fan, L. Lin, and H. Liu. Constacyclic codes over finite fields. *Finite Fields and Their Applications*, 18(6):1217–1231, 2012.

[5] P. Choosuwan and S. Jitman. Self-dual codes over $\mathbb{F}_q+u\mathbb{F}_q+u^2\mathbb{F}_q$ and applications. *Journal of Algebra Combinatorics Discrete Structures and Applications*, 7(3):209–227, 2020.

[6] P. Davis. *Circulant Matrices*. Chelsea Publishing Series. Chelsea, 1994.

[7] J. A. Gallian. *Contemporary Abstract Algebra*. Richard Stratton, 2013.

[8] T. Hungerford. *Algebra*. Graduate Texts in Mathematics. Springer New York, 2012.

[9] Y. Jia. On quasi-twisted codes over finite fields. *Finite Fields and Their Applications*, 18(2):237–257, 2012.

[10] S. Jitman. Determinants of some special matrices over commutative finite chain rings. *Special Matrices*, 8(1):242–256, 2020.

[11] S. Jitman, S. Prugsapitak, and R. Madhu. Some generalizations of good integers and their applications in the study of self-dual negacyclic codes. *Advances in Mathematics of Communications*, 14:35–51, 2018.

[12] S. Kittiwut and S. Jitman. On the algebraic structure of complex twistulant matrices. In *The 11th IMT-GT International Conference on Mathematics, Statistics and Its Applications 2015*, 2015.

[13] N. Makhijani, R. Sharma, and J. Srivastava. The unit group of algebra of circulant matrices. *International Journal of Group Theory*, 3:13–16, 2014.

[14] B. J. Olson, S. W. Shaw, C. Shi, C. Pierre, and R. G. Parker. Circulant matrices and their application to vibration analysis. *Applied Mechanics Reviews*, 66(4):040803, 2014.

[15] R. Roth and A. Lempel. Application of circulant matrices to the construction and decoding of linear codes. *IEEE Transactions on Information Theory*, 36(5):1157–1163, 1990.

[16] E. Sangwisut, S. Jitman, S. Ling, and P. Udomkavanich. Hulls of cyclic and negacyclic codes over finite fields. *Finite Fields and Their Applications*, 33:232–257, 2015.

[17] R. Sharma and P. Yadav. Unit group of algebra of circulant matrices. *International Journal of Group Theory*, 2:1–6, 2013.

[18] R. Underwood. *Fundamentals Of Modern Algebra: A Global Perspective*. World Scientific Publishing Company, 2015.

[19] H.-L. Wu and L.-Y. Wang. Applications of circulant matrices to determinants involving $\boldsymbol{k}$ th power residues. *Bulletin of the Australian Mathematical Society*, 106(2):243–253, 2022.

Biography

Name	Mr. Prarinya Naksing
Address	38 Village No.10, Pradu Yuen Sub-district, Lan Sak District, Uthai Thani, 61160
Date of Birth	24 September 1998
Education	
2017-2021	Bachelor of Science in Mathematics, (First Class Honors), Silpakorn University.
2021-2025	Master of Science in Mathematics, Silpakorn University.
Scholarships	- Phetsanamchan Scholarship, - Research Assistant Scholarship.
Publications	P. Naksing and S. Jitman, Unit group of the ring of negacirculant matrices over finite commutative chain rings. *Special Matrices*, vol. 13, no. 1, 2025, pp. 20250035.