Enumeration of Generalized Necklaces over $\mathbb{F}_q$

by

Jumah Ali Algallaf

B.Sc., King Fahd University of Petroleum and Minerals, Saudi Arabia, 2006

A Project Report Submitted in Partial

Fulfillment of the Requirements for the Degree of

MASTER OF ENGINEERING

In the Department of Electrical and Computer Engineering

University of Victoria

Supervisory Committee

Enumeration of Generalized Necklaces over $\mathbb{F}_q$

by

Jumah Ali Algallaf

B.Sc., King Fahd University of Petroleum and Minerals, Saudi Arabia, 2006

Supervisory Committee

Dr. T. Aaron Gulliver, Supervisor

(Department of Electrical and Computer Engineering)

Dr. Fayez Gebali, Departmental Member

(Department of Electrical and Computer Engineering)

Abstract

In combinatorial theory, a necklace is an equivalence class of a word under cyclic shift. Enumerating necklaces over a finite field $\mathbb{F}_q$ is an essential yet time-consuming step in constructing Quasi-Cyclic (QC) and Quasi-Twisted (QT) codes. QC and QT codes are important subclasses of linear block codes which can be characterized in terms of $m \times m$ circulant and twistulant matrices, respectively. Circulant and twistulant matrices have been used extensively in the construction of error correcting codes and many of the best-known linear codes have been obtained using constructions based on theses matrices. In this project, a generalization of necklaces which is related to circulant and twistulant matrices is presented along with a closed form expression to count their numbers. The goal is to enumerate these generalized necklaces over prime and prime power fields using MATLAB.

Table of Contents

Supervisory Committee **ii**

Abstract **iii**

Table of Contents **iv**

List of Tables **v**

List of Figures **vi**

Acknowledgment **vii**

Acronyms **viii**

1 Introduction **1**

1.1 Necklaces 4
1.1.1 Enumeration of Necklaces 6
1.2 Quasi-Cyclic (QC) and Quasi-Twisted (QT) Codes 6
1.3 Motivation 8
1.4 Previous Work 9
1.5 Report Organization 10

2 Enumeration of Generalized Necklaces with $\lambda = 1$ **11**
2.1 The Number of Generalized Necklace with $\lambda = 1$ 11
2.2 Calculations and Results 12

3 Enumeration of Generalized Necklaces with $\lambda \in \mathbb{F}_q \backslash \{0\}$ **15**
3.1 The Number of Generalized Necklaces with $\lambda \in \mathbb{F}_q \backslash \{0\}$ 15
3.2 Calculations and Results 16
3.2.1 Calculation over Prime Fields 17
3.2.2 Calculation over Prime Power Fields 26

4 Conclusion **33**
4.1 Conclusion 33
4.2 Future Works 33

Bibliography **34**

Appendices **35**

List of Tables

Table 1: Binary Linear Block Code with $k = 4$, $n = 7$, and $d = 3$ [7] 4

Table 2: The Number of Generalized Necklaces over $\mathbb{F}_2, \mathbb{F}_3, \mathbb{F}_5, \mathbb{F}_7$, and $\mathbb{F}_{11}$ with $\lambda = 1$ 13

Table 3: The Number of Generalized Necklaces over $\mathbb{F}_{13}, \mathbb{F}_{17}$, and $\mathbb{F}_{19}$ with $\lambda = 1$ 14

Table 4: The Number of Generalized Necklaces over $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_9$, and $\mathbb{F}_{16}$ with $\lambda = 1$ .. 14

Table 5: The Number of Generalized Necklaces over $\mathbb{F}_3$ with $\lambda \in \mathbb{F}_3 \backslash \{0\}$ 19

Table 6: The Number of Generalized Necklaces over $\mathbb{F}_5$ with $\lambda \in \mathbb{F}_5 \backslash \{0\}$ 20

Table 7: The Number of Generalized Necklaces over $\mathbb{F}_7$ with $\lambda \in \mathbb{F}_7 \backslash \{0\}$ 21

Table 8: The Number of Generalized Necklaces over $\mathbb{F}_{11}$ with $\lambda \in \mathbb{F}_{11} \backslash \{0\}$ 22

Table 9: The Number of Generalized Necklaces over $\mathbb{F}_{13}$ with $\lambda \in \mathbb{F}_{13} \backslash \{0\}$ 23

Table 10: The Number of Generalized Necklaces over $\mathbb{F}_{17}$ with $\lambda \in \mathbb{F}_{17} \backslash \{0\}$ 24

Table 11: The Number of Generalized Necklaces over $\mathbb{F}_{19}$ with $\lambda \in \mathbb{F}_{19} \backslash \{0\}$ 25

Table 12: The Number of Generalized Necklaces over $\mathbb{F}_4$ with $\lambda \in \mathbb{F}_4 \backslash \{0\}$ 29

Table 13: The Number of Generalized Necklaces over $\mathbb{F}_8$ with $\lambda \in \mathbb{F}_8 \backslash \{0\}$ 30

Table 14: The Number of Generalized Necklaces over $\mathbb{F}_9$ with $\lambda \in \mathbb{F}_9 \backslash \{0\}$ 31

Table 15: The Number of Generalized Necklaces over $\mathbb{F}_{16}$ with $\lambda \in \mathbb{F}_{16} \backslash \{0\}$ 32

List of Figures

Figure 1: Block Encoder Model 2

Figure 2: The Equivalence Classes of Binary Necklaces 5

Figure 3: Periodic and Aperiodic (Primitive) Necklaces 6

Figure 4: The Number of Necklaces with Constacyclic Shift $\lambda = 2$ for Example 4 18

Acknowledgements

First, I would like to express my sincere gratitude and deepest appreciation to my supervisor Dr. T. Aaron Gulliver for his continuous support, guidance, feedback, and motivation during my study. Beside my supervisor, I would like to thank my supervisory committee for their insightful comments.

I am so grateful and thankful to God for having my lovely parents, my wife Hebah Alqallaf, my son Ali and my daughter Zahraa without whose support, motivation, and patience, it would not have been possible to complete my MEng project. I would also like to thank my brothers, sisters, friends, and loved ones for their spiritual support.

Last but not the least; I would like to thank the Ministry of Education in Saudi Arabia and the Saudi Cultural Bureau in Canada for sponsoring my entire study in Canada.

THANK YOU …

Acronyms and Symbols

QC ..... Quasi-cyclic

QT ..... Quasi-twisted

gcd ..... Greatest common divisor

$\mathbb{F}_q$ ..... Finite fields of q elements

C ..... Linear block code

d ..... Hamming distance

G ..... Generator matrix

k ..... Number of data symbols in a linear block code

m ..... Length of a generalized necklace

n ..... Block length of a linear block code

p ..... Prime number

q ..... The number of elements in a finite field

R ..... Code rate

V ..... Vector space

λ ..... Non-zero element of a finite field

γ ..... Non-zero element of a finite field

α ..... Primitive element of a finite field

φ ..... Euler's totient function

Chapter 1

Introduction

Error control coding is an important part of modern data communication and storage systems since the accuracy in a sequence of received data symbols is not guaranteed. Information media are prone to noise and interference that can cause a loss of data integrity. Error control codes add redundancy to the original message at the transmitter in such a way that the receiver can detect and correct errors. However, adding redundancy so the receiver can efficiently detect and correct as many errors as possible is a major challenge in coding theory.

The theory of error control codes uses an algebraic structure called a finite field since the transmitted message consists of a finite sequence of symbols that are elements of some finite alphabet [8]. A finite field ($\mathbb{F}_q$) is a finite set of elements equipped with two binary operations called addition and multiplication [7]. These binary operations satisfy the commutative, associative, and distributive axioms. The number of elements in a finite field is $q = p^a$, where p is a prime number and $a \geq 1$ is an integer. The set of elements form the additive group of $\mathbb{F}_q$ and the non-zero elements of the set form the multiplicative group of $\mathbb{F}_q$. In a finite field, the multiplicative order of an element λ, denoted ord (λ), is the smallest positive integer z such that $\lambda^z = 1$. Every finite field has one or more primitive elements which are nonzero elements of order $q - 1$. Note that the sets of real numbers, complex numbers, and rational numbers are fields, but they are infinite.

Linear block codes are widely used in error control coding. A block code C of length n and dimension k is called a linear (n, k) code if and only if its q^k codewords form a k-dimensional subspace of the vector space $V(n, q)$ of all n-tuples (or words of length n) over the field $\mathbb{F}_q$ [4,7]. Various applications, including space and satellite communications, data transmission, data storage, and mobile communications rely on linear block codes to provide reliable communication and storage [6]. Many linear block codes have algebraic properties that allow for efficient error detection and correction.

The digital information source is a sequence of symbols where each message block $u = (u_1, u_2, \dots, u_k)$ consists of k information digits that result in a total of q^k distinct messages. The encoder transforms each input message u into an n-tuple $v = (v_1, v_2, \dots, v_n)$ called a codeword with $n > k$, as shown in Figure 1. The code rate is defined as the ratio of the number of data symbols in a codeword to the block length, denoted as R = k/n [7].

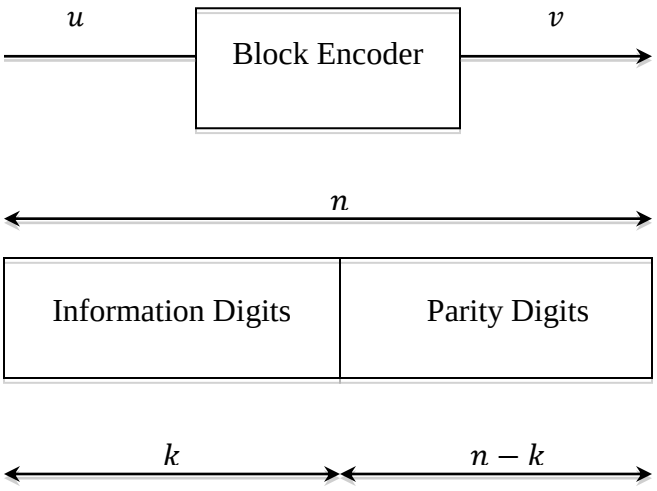


Figure 1: Block Encoder Model.

Linear block codes can be defined and described in terms of generator matrices [7]. With linear block codes, the sum of any two codewords produces another codeword, so a basis for the vector space can be formed so that all codewords can be obtained as linear combinations of basis vectors. If $\{g_0, g_1, \dots, g_{k-1}\}$ are the basis vectors, a generator matrix is obtained by arranging these vectors as the rows of a $k \times n$ matrix as follows:

$$G = \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ \vdots \\ g_{k-1} \end{bmatrix} = \begin{bmatrix} g_{0\,0} & g_{0\,1} & g_{0\,2} & \cdots & g_{0,n-1} \\ g_{1\,0} & g_{1\,1} & g_{1\,2} & \cdots & g_{1,n-1} \\ g_{2\,0} & g_{2\,1} & g_{2\,2} & \cdots & g_{2,n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ g_{k-1,0} & g_{k-1,1} & g_{k-1,2} & \cdots & g_{k-1,n-1} \end{bmatrix} \quad (1)$$

If $u = (u_0, u_1, \dots, u_{k-1})$ is a message block, the corresponding codeword is

$$\begin{aligned} v &= u \cdot G \\ &= (u_0, u_1, \dots, u_{k-1}) \cdot \begin{bmatrix} g_0 \\ g_1 \\ g_2 \\ \vdots \\ g_{k-1} \end{bmatrix} \\ &= u_0 g_0 + u_1 g_1 + \cdots + u_{k-1} g_{k-1}. \end{aligned} \tag{2}$$

The name generator matrix comes from the observation that the rows of G generate (or span) the (n, k) linear code C [7].

The random error detection and correction capability of a linear block code is determined by an important parameter called the Hamming distance or minimum distance d. The Hamming distance between any two codewords of C is defined as the number of places in which they differ. The Hamming weight of a codeword is defined as the number of its nonzero components. The minimum weight of C is the smallest weight among all nonzero codewords of C. The minimum distance d between codewords equals the minimum weight of a linear code. Therefore, an (n, k, d) code is an (n, k) code with minimum weight d [4, 7]. An example of a (7,4,3) binary linear block code is given in Table 1 [7].

Since error control codes occupy a critical position in most communication and storage systems, it is very important to devise methods for constructing them. Constructing good codes requires studying the structure of the codes. For example, the construction of quasi-cyclic (QC) and quasi-twisted (QT) codes, which are important subclasses of linear block codes, requires defining the relations among the elements of the code. QC and QT codes can be characterized in terms of $m \times m$ circulant and twistulant matrices, respectively. Circulant matrices have been used extensively in the construction of error correcting codes and many of the best-known linear codes have been obtained using constructions based on circulant matrices [4]. The first step in constructing QC and QT codes is to find the number of nonzero defining polynomials,

which are representatives of the equivalence classes of an equivalence relation among the circulant and twistulant matrices.

Table 1: Binary Linear Block Code with $k = 4$, $n = 7$, and $d = 3$ [7].

Messages	Codewords
(0 0 0 0)	(0 0 0 0 0 0 0)
(1 0 0 0)	(1 1 0 1 0 0 0)
(0 1 0 0)	(0 1 1 0 1 0 0)
(1 1 0 0)	(1 0 1 1 1 0 0)
(0 0 1 0)	(1 1 1 0 0 1 0)
(1 0 1 0)	(0 0 1 1 0 1 0)
(0 1 1 0)	(1 0 0 0 1 1 0)
(1 1 1 0)	(0 1 0 1 1 1 0)
(0 0 0 1)	(1 0 1 0 0 0 1)
(1 0 0 1)	(0 1 1 1 0 0 1)
(0 1 0 1)	(1 1 0 0 1 0 1)
(1 1 0 1)	(0 0 0 1 1 0 1)
(0 0 1 1)	(0 1 0 0 0 1 1)
(1 0 1 1)	(1 0 0 1 0 1 1)
(0 1 1 1)	(0 0 1 0 1 1 1)
(1 1 1 1)	(1 1 1 1 1 1 1)

1.1. Necklaces

A circular word or a necklace is an equivalence class of a word under cyclic shift [1,2]. We can think of a q-ary necklace as a circle with m-coloured beads and up to q different colours. Consider the set of binary words of length $m = 4$ and $q = 2$ denoted by the numbers 0 and 1

$$S = \{0000, 0001, 0010, 0011, 0100, 0101, 0110, 0111, \\ 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111\} \quad (3)$$

Two words of S are said to be related if they are the same or one is a cyclic shift of the other [1]. To get the resulting equivalence classes, one can represent a binary necklace from the above set using a circle. The numbers 0 and 1 are represented by black and white coloured beads, respectively. Figure 2 gives the resulting equivalence classes of binary necklaces $C1$ ={0000}, $C2$ ={0001,1000,0100,0010}, $C3$ = {0011,1001,1100,0110}, $C4$ ={0101,1010}, $C5$ ={0111,1011,1101,1110}, and $C6$ = {1111}.

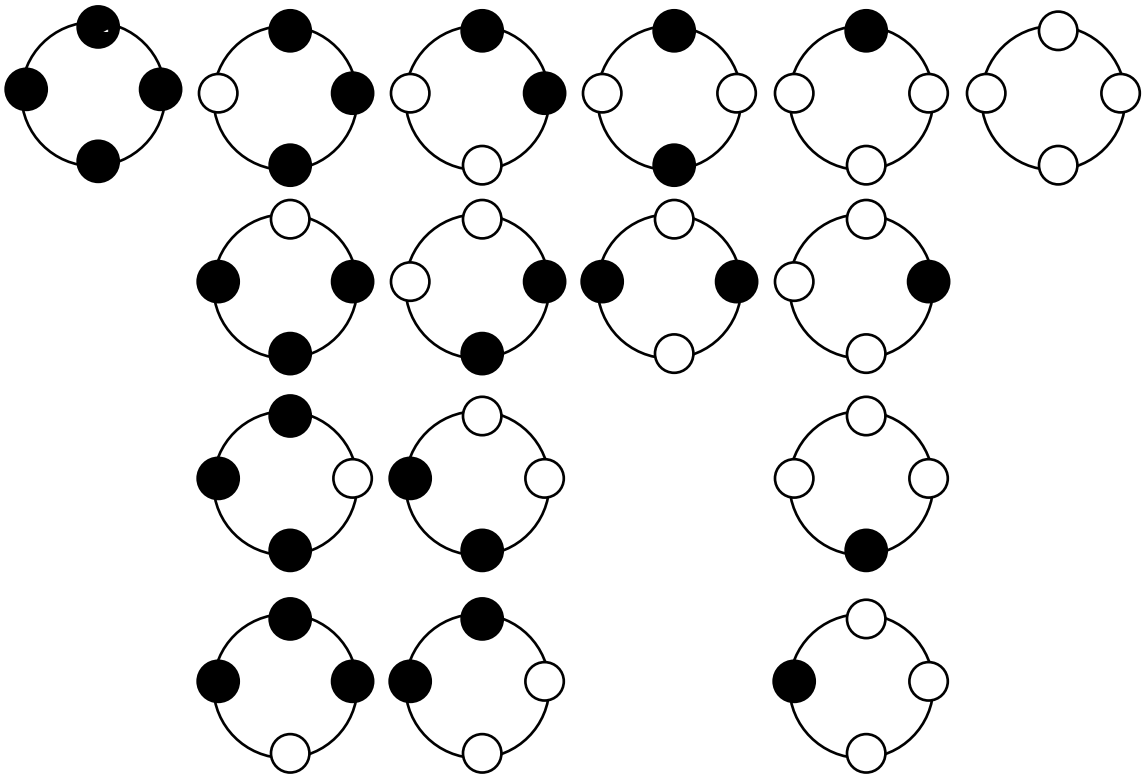


Figure 2: The Equivalence Classes of Binary Necklaces.

Note that rotating the circle in the equivalence class $C1$ in Figure 2 to the right will always result in the same word of 0000. However, each rotation of a circle in equivalence class $C2$ will result in a cyclic shift of the previous word which is different.

Each of these equivalence classes is called a binary (or 2-ary) necklace. In general, a q-ary necklace of length m is an equivalence class of q-ary words under rotation.

1.1.1. Enumeration of Necklaces

The enumeration of necklaces of length m on q symbols was first considered by MacMahon in 1892 [2]. A necklace of length m is called aperiodic or primitive if its period is not a proper divisor of m, i.e. no two distinct rotations from a primitive necklace are equal, as shown in Figure 3. Note that the equivalence classes $C1$ and $C6$ in Figure 2 are necklaces with period 1, whereas the equivalence classes $C2$, $C3$, and $C5$ are primitive necklaces. The total number of necklaces of length m on q symbols is

$$N(m,q) = \frac{1}{m}\sum_{d|m} q^d \varphi(m/d) \tag{4}$$

where φ is Euler's totient function. This is called MacMahon's formula [2]. From (4), the total number of necklaces of length 4 on 2 symbols is $N(4,2) = 6$ as shown in Figure 2.

A necklace with period 2 A primitive necklace

Figure 3: Periodic and Aperiodic (Primitive) Necklaces.

1.2. Quasi-Cyclic (QC) and Quasi-Twisted (QT) Codes

The Class of QT codes is a generalization of the class of QC codes, which is a further generalization of cyclic codes. Therefore, it is natural to begin with a description of cyclic and quasi-cyclic codes. For an m-tuple $(x_0, x_1, \dots, x_{m-1}) \in \mathbb{F}_q$, a cyclic shift of $(x_0, x_1, \dots, x_{m-1})$ is the m-tuple $(x_{m-1}, x_0, \dots, x_{m-2})$ [3]. A block code C is called a

linear (n, k) cyclic code if and only if every cyclic shift of a codeword is also a codeword in C [1,3,4,7,8].

The class of QC codes generalizes the cyclic codes so that a cyclic shift of a codeword by p positions is again a codeword in C. When $p = 1$, a QC code is a cyclic code [3]. The block length n of a QC code is a multiple of p, so that $n = mp$. Thus, QC codes can be characterized in terms of $m \times m$ circulant matrices with a suitable permutation of coordinates [3,9]. The generator matrix G can then be represented as

$$G = \left[R_0\, R_1\, R_2\, \cdots R_{p-1}\right] \tag{5}$$

where R_i, $i = 0,1, \ldots \ldots, p-1$, is an $m \times m$ circulant matrix of the form

$$R_i = \begin{bmatrix} r_{0,i} & r_{1,i} & r_{2,i} & \cdots & r_{m-1,i} \\ r_{m-1,i} & r_{0,i} & r_{1,i} & \cdots & r_{m-2,i} \\ r_{m-2,i} & r_{m-1,i} & r_{0,i} & \cdots & r_{m-3,i} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ r_{1,i} & r_{2,i} & r_{3,i} & \cdots & r_{0,i} \end{bmatrix} \tag{6}$$

Now, for an m-tuple $(x_0, x_1, \ldots, x_{m-1}) \in \mathbb{F}_q$ and $\lambda \in \mathbb{F}_q \backslash \{0\}$, a constacyclic shift of $(x_0, x_1, \ldots, x_{m-1})$ is the m-tuple $(\lambda x_{m-1}, x_0, \ldots, x_{m-2})$ [4]. A code C is called QT if every constacyclic shift of a codeword by p positions is again a codeword in C. Similar to the QC codes, the block length of a QT code is $n = mp$. QT codes can be characterized in terms of $m \times m$ twistulant matrices (or constacyclic matrices), with a suitable permutation of coordinates. Therefore, the generator matrix G can be represented as

$$G = \left[B_0\, B_1\, B_2\, \cdots B_{p-1}\right] \tag{7}$$

where B_i, $i = 0,1, \ldots \ldots, p-1$, is an $m \times m$ twistulant matrix of the form

$$B_i = \begin{bmatrix} b_{0,i} & b_{1,i} & b_{2,i} & \cdots & b_{m-1,i} \\ \lambda b_{m-1,i} & b_{0,i} & b_{1,i} & \cdots & b_{m-2,i} \\ \lambda b_{m-2,i} & \lambda b_{m-1,i} & b_{0,i} & \cdots & b_{m-3,i} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ \lambda b_{1,i} & \lambda b_{2,i} & \lambda b_{3,i} & \cdots & b_{0,i} \end{bmatrix} \tag{8}$$

The algebra of $m \times m$ twistulant matrices over $\mathbb{F}_q$ is isomorphic to the algebra of polynomials in the ring $S_m = \mathbb{F}_q[x]/(x^m - \lambda)$, if B_i is mapped onto the polynomial $b_i(x) = b_{0,i} + b_{1,i}x + b_{2,i}x^2 + \cdots + b_{m-1,i}x^{m-1}$, formed from the entries in the first row of B_i. The $b_i(x)$ are called the defining polynomials and the set $\{b_0(x), b_1(x), \ldots, b_{p-1}(x)\}$ defines an (mp, m) QT code with $k = m$ [4,5]. Note that the class of QT codes generalizes the classes of QC codes when $\lambda = 1$ and cyclic codes when $\lambda = 1$ and $p = 1$.

From the above description of circulant and twistulant matrices, generalized necklaces are identical to the defining polynomials which can be defined as equivalence classes of q-ary words of length m under constacyclic rotation and multiplication by $\gamma \in \mathbb{F}_q \backslash \{0\}$.

1.3. Motivation

A fundamental problem in coding theory is that of optimizing the parameters (n, k, d) of a linear code over the finite field $\mathbb{F}_q$. The challenge is to construct codes with the best possible parameters. QC and QT codes are important subclasses of linear block codes which can be characterized in terms of $m \times m$ circulant and twistulant matrices, respectively. Many of the best-known linear codes have been obtained using constructions based on circulant and twistulant matrices. As mentioned in the previous section, there is an isomorphism between the algebra of $m \times m$ twistulant matrices over $\mathbb{F}_q$ and the algebra of polynomials in the ring S_m, if B_i is mapped onto the defining polynomials $b_i(x)$, formed from the entries in the first row of B_i. Since generalized necklaces over $\mathbb{F}_q$ are identical to the defining polynomials, it is very important to enumerate them for different values of $q, m,$ and λ.

The aim of this project is to enumerate the generalized necklaces defined in [3,4] over a finite field $\mathbb{F}_q$. The calculations were done using MATLAB. Tables of the numbers of generalized necklaces for $\lambda \in \mathbb{F}_q \backslash \{0\}$ are given for $m = 1$ to 20 over $\mathbb{F}_q$,

where $q = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, \text{and } 19$. The enumeration can easily be extended to higher values of m and q.

1.4. Previous Work

Enumerating the defining polynomials is an essential yet time-consuming step in constructing QC and QT codes. Therefore, it is very important to derive an expression that can expedite the process of constructing these codes. An empirical expression for the number of defining polynomials was first considered in [10,12]. The defining polynomials computed in [12] were used to construct optimal ternary QC codes. The defining polynomials enumerated from the expression obtained in [10] were used to construct good QC codes of rates $1/p$ and $(p-1)/p$ over $\mathbb{F}_3$ and $\mathbb{F}_4$. Another expression for the number of defining polynomials was given in [11]. The corresponding defining polynomials were used to construct good rate $(m-1)/pm$ codes over $\mathbb{F}_3$ and $\mathbb{F}_4$. In [9], for $c(m, q, \lambda)$, the following expressions with $q = 3$ were given

$$c(m, 3, 1) = \frac{1}{2m} \sum_{\substack{d, \\ d|m}} \varphi(d)(3^{m/d} + 3^{(m/d)ev(d)}) \tag{9}$$

$$c(m, 3, 2) = \frac{1}{2m} \sum_{i=1}^{m} \varphi(d) \left(3^{\gcd(m,i)ev\left(\frac{i}{\gcd(m,i)}\right)} + 3^{\gcd(m,i)ev\left(\frac{m-i}{\gcd(m,i)}\right)} \right) \tag{10}$$

where $ev(m) = \begin{cases} 1, & \text{if } m \text{ is even} \\ 0, & \text{if } m \text{ is odd} \end{cases}$, gcd is the greatest common divisor, and $\varphi(d)$ is Euler's totient function, to count the number of ternary defining polynomials. These expressions are a special ternary case of the expression for the number of defining polynomials given in [4]. Recently, an analytical closed form expression for the number of defining polynomials corresponding to circulant matrices was derived in [3]. An analytical expression for the number of defining polynomials corresponding to twistulant matrices was derived in [4]. This latter expression is a generalization of the expression derived in [3] and corresponds to the defining polynomials used to construct QT codes.

1.5. Report Organization

Chapter 1 provided the background to understand the motivation and goals of this project. In particular, this chapter introduced linear block codes over finite fields, necklaces, and their enumeration, QC and QT codes, as well as a summary of the previous work.

Chapter 2 presents the enumeration of generalized necklaces over $\mathbb{F}_q$ with $\lambda = 1$. Examples of the calculations are presented along with tables of the results.

Chapter 3 presents the enumeration of generalized necklaces over $\mathbb{F}_q$ with $\lambda \in \mathbb{F}_{\boldsymbol{q}} \backslash \{0\}$. Examples of the calculations are presented along with tables of the results.

Chapter 4 concludes the report and outlines suggestions for future work.

Chapter 2

Enumeration of Generalized Necklaces with $\lambda = 1$

2.1. The Number of Generalized Necklaces with $\lambda = 1$

The study of circulant matrices is of particular interest, because of its relevance in the construction of QC codes. QC code construction requires a representative set of defining polynomials, which are equivalence classes among the circulant matrices [3]. This requirement defines a relation among the circulant matrices so that two polynomials $r_j(x)$ and $r_i(x)$ are related if and only if

$$r_j(x) = \gamma x^{\ell} r_i(x) \quad \text{mod}(x^m - 1) \tag{11}$$

where ℓ is an integer ≥ 0 and $\gamma \in \mathbb{F}_q \backslash \{0\}$ [3].

The number of necklaces differs from the number of defining polynomials, because multiplication by a nonzero constant of $\mathbb{F}_q$ does not change the Hamming weight of a codeword and hence does not change the equivalence class. Therefore, if the first row of one of the matrices over $\mathbb{F}_q$ is equal to a nonzero constant multiple of one of the rows of the other matrix, then the two matrices are said to be equivalent over $\mathbb{F}_q$. In [3], an analytical closed form expression for the number of nonzero defining polynomials for $m \times m$ circulant matrices over $\mathbb{F}_q$ was given as

$$b(m, q, 1) = \frac{1}{(q-1)m} \sum_{d|m} \varphi(d) \gcd(d, q-1)(q^{m/d} - 1) \tag{12}$$

The number of generalized necklaces which is the number of equivalence class of $m \times m$ circulant matrices over $\mathbb{F}_q$ was given as

$$c(m, q, 1) = \frac{1}{(q-1)m} \sum_{d|m} \varphi(d) \gcd(d, q-1)(q^{m/d} - 1) + 1 \tag{13}$$

Example 1: Let $q = 3$ and $m = 2$. The number of nonzero defining polynomials can be computed as follows:

Let $f\ (d, q, m) = \varphi\ (d)\ \gcd(d, q-1)(q^{m/d} - 1)$ for every divisor d of m. We know 1 and 2 are divisors of $m = 2$. Therefore, (12) can be expressed as

$$b(2,3,1) = \frac{1}{(3-1)2}\sum_{d|2} f(d,q,m)$$

where $\sum_{d|2} f(d,q,m) = f(1,3,2) + f(2,3,2)$

$$f(1,3,2) = \varphi(1)\ \gcd\ (1,3\text{-}1)(3^{2/1} - 1)$$
$$= 1\times1\times8$$
$$= 8$$

$$f(2,3,2) = \varphi(2)\ \gcd\ (2,3\text{-}1)(3^{2/2} - 1)$$
$$= 1\times2\times2$$
$$= 4$$

Thus, the number of nonzero defining polynomials is

$$b(2,3,1) = \frac{1}{(3-1)2}(8+4) = 3$$

and the number of generalized necklaces is $c(2,3,1) = b(2,3,1) + 1 = 4$.

2.2. Calculations and Results

A MATLAB program was developed to calculate the number of generalized necklaces over prime and prime power fields $\mathbb{F}_{\boldsymbol{q}}$, where $q = 2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, \text{and } 19$ (see Appendix A1). Tables 2 to 4 show the results obtained from calculating these generalized necklaces.

Example 2: Let $q = 3$ and $m = 2$ as in the Example 1. Since $\mathbb{F}_{\boldsymbol{3}} = \{0, 1, 2\}$, there are a total of $3^2 = 9$ words. Therefore, the set S, consisting of all possible words of length 2, is

$S_2 = \{[0\ 0], [0\ 1], [0\ 2], [1\ 0], [1\ 1], [1\ 2], [2\ 0], [2\ 1], \text{and } [2\ 2]\}$. Based on the relation defined in (11) the equivalence classes are

$$C1 = \{[0\ 1], [0\ 2], [1\ 0], [2\ 0]\},$$

$$C2 = \{[1\ 1], [2\ 2]\},$$

$$C3 = \{[1\ 2], [2\ 1]\},$$

and $$C4 = \{[0\ 0]\},$$

Note the word $[0\ 2]$ in $C1$ is a constant multiple of the word $[0\ 1]$ and the words $[1\ 0]$ and $[2\ 0]$ are cyclic shifts of the words $[0\ 1]$ and $[0\ 2]$, respectively. Likewise, $C2, C3,$ and $C4$ are obtained.

Table 2: The Number of Generalized Necklaces over $\mathbb{F}_{\mathbf{2}}, \mathbb{F}_{\mathbf{3}}, \mathbb{F}_{\mathbf{5}}, \mathbb{F}_{\mathbf{7}}$, and $\mathbb{F}_{\mathbf{11}}$ with $\lambda = 1$.

				q	
m	**2**	**3**	**5**	**7**	**11**
1	2	2	2	2	2
2	3	4	5	6	8
3	4	6	12	22	46
4	6	14	45	106	374
5	8	26	158	562	3226
6	14	68	665	3298	29576
7	20	158	2792	19610	278390
8	36	424	12255	120206	2679860
9	60	1098	54262	747330	26199450
10	108	2980	244301	4708486	259377496
11	188	8054	1109732	29959498	2593742462
12	352	22218	5086965	192243598	26153599626
13	632	61322	23475062	1242166802	265559324186
14	1182	170980	108994145	8074103814	2712499089704
15	2192	478318	508626416	52750684582	27848321131766
16	4116	1345634	2384198085	346176480306	287185814327186
17	7712	3798242	11219697842	2280691313602	2973217814701730
18	14602	10762820	52981961165	15077904438230	30888429545620424
19	27596	30585830	250966925372	99990308643626	321889949728497614
20	52488	87172598	1192093139997	664935557188666	3363749974922179006

Table 3: The Number of Generalized Necklaces over $\mathbb{F}_4, \mathbb{F}_8, \mathbb{F}_9$, and $\mathbb{F}_{16}$ with $\lambda = 1$.

	q			
m	**4**	**8**	**9**	**16**
1	2	2	2	2
2	4	6	7	10
3	10	26	32	94
4	24	150	213	1098
5	70	938	1478	13986
6	238	6258	11107	186478
7	782	42806	85412	2556530
8	2744	299670	672825	35791946
9	9726	2130458	5380862	509033346
10	34990	15339642	43586287	7330084546
11	127102	111557594	356602952	106619309362
12	466198	818092242	2941985613	1563749966062
13	1720742	6041272682	24441017582	23095382704466
14	6391714	44878047054	204257160907	343131401458882
15	23861074	335089258634	1715759435132	5124095576058766
16	89479864	2513169584790	14476720898445	76861433658352714
17	336860182	18922687509962	122626336026962	1157442765409226770
18	1272588226	142971417811314	1042323861617407	17490246233105427346
19	4822419422	1083572842675610	8887182353111792	265115311318997626034
20	18325211326	8235153612004794	75985409162693733	4029752732052428965826

Table 4: The Number of Generalized Necklaces over $\mathbb{F}_{13}, \mathbb{F}_{17}$, and $\mathbb{F}_{19}$ with $\lambda = 1$.

	q		
m	**13**	**17**	**19**
1	2	2	2
2	9	11	12
3	64	104	130
4	605	1317	1822
5	6190	17750	27514
6	67117	251543	435760
7	747008	3663740	7094222
8	8497807	54499433	117943232
9	98189934	823526990	1991899630
10	1148826961	12599979635	34061506732
11	13576972684	194726683568	588334640902
12	161792326165	3034491071421	10246828768390
13	1941507093542	47618163619742	179713604539562
14	23436764947605	751686729375359	3170661458613612
15	284366072312932	11926762714636148	56226396406998826
16	3465711514660797	190082780818824465	1001532686116627842
17	42403999604810482	3041324492229179282	17909760973152948322
18	520626884135163809	48830154348281073059	321380710798015121320
19	6411931098137921540	786422485806418831736	5784852794328402307382
20	79187349063152164621	1270072314578626413093	1044165929376617231563 90

Chapter 3

Enumeration of Generalized Necklaces with $\lambda \in \mathbb{F}_q \backslash \{0\}$

3.1. The Number of Generalized Necklaces with $\lambda \in \mathbb{F}_q \backslash \{0\}$

The construction of QT codes requires a representative set of defining polynomials, which are an equivalence relation among the twistulant matrices [4]. Let $S_m = \mathbb{F}_q[x]/(x^m - \lambda), \lambda \in \mathbb{F}_q \backslash \{0\}$. Since the algebra of twistulant matrices of order m over $\mathbb{F}_q$ is isomorphic to the algebra of polynomials in the ring S_m, a relation among the twistulant matrices was defined in [4] in that two polynomials $s_j(x)$ and $s_i(x)$ are related if and only if

$$s_j(x) = \gamma x^{\ell} s_i(x) \quad \bmod(x^m - \lambda) \tag{14}$$

where ℓ is an integer $\geq 0, \lambda \in \mathbb{F}_q \backslash \{0\}$, and $\gamma \in \mathbb{F}_q \backslash \{0\}$. Based on this definition, two polynomials are related if one is the same, a constant multiple, a constacyclic shift with constant λ, or a constant multiple of a constacyclic shift with constant λ [1]. The analytical closed form expression for the number of generalized necklaces of length m over $\mathbb{F}_q$ [4] is

$$c(m, q, \lambda) = \frac{1}{(q-1)ord(\lambda)m} \sum_{\substack{i=1 \\ t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = 1}}^{ord(\lambda)m} \left(q^{\gcd(m,i)} - 1\right) + 1 \tag{15}$$

where $\lambda \in \mathbb{F}_q \backslash \{0\}$, $t \in \mathbb{F}_q \backslash \{0\}$, $1 \leq i \leq ord(\lambda)m$, and $ord(\lambda)$ is the multiplicative order of λ. Note that this expression generalizes the expression in (13) for the generalized necklaces with $\lambda = 1$.

Example 3: Let $q = 3, m = 2,$ and $\lambda = 2$. Thus, $ord(2) = 2$, $1 \le i \le 4$, and (15) can be expressed as

$$c(2,3,2) = \frac{1}{(3-1)ord(2)2} \sum_{\substack{i=1 \\ t\in\mathbb{F}_3\setminus\{0\}, t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}}=1}}^{4} \left(3^{\gcd(2,i)} - 1\right) + 1$$

when $t = 1$ and $i = 1$, $t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = 2 \bmod 3$,

when $t = 1$ and $i = 2$, $t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = 2 \bmod 3$,

when $t = 1$ and $i = 3$, $t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = 2 \bmod 3$,

when $t = 1$ and $i = 4$, $t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = 1 \bmod 3$,

when $t = 2$ and $i = 1$, $t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = 2 \bmod 3$,

when $t = 2$ and $i = 2$, $t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = 1 \bmod 3$,

when $t = 2$ and $i = 3$, $t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = 2 \bmod 3$,

and when $t = 2$ and $i = 4$, $t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = 2 \bmod 3$.

Therefore, the number of generalized necklaces is

$$c(2,3,2) = \frac{1}{8}\left[\left(3^{\gcd(2,2)} - 1\right) + \left(3^{\gcd(2,4)} - 1\right)\right] + 1 = 3$$

Similarly, the evaluation can be obtained when $\lambda = 1$ to get $c(2,3,1) = 4,$ which is the result obtained in Example 1. This proves that the generalized necklaces in (15) are a generalization of (13) when $\lambda = 1$.

3.2. Calculations and Results

Two MATLAB programs were developed to calculate the number of generalized necklaces over $\mathbb{F}_q$. The arithmetic over prime fields is defined modulo q. Therefore, the first MATLAB program was developed to calculate the number of generalized necklaces over the prime fields $\mathbb{F}_q$, where $q = 2, 3, 5, 7, 11, 13, 17,$ and 19 (see Appendix A2).

Since the arithmetic over prime power fields differs from that over prime fields, the number of generalized necklaces over prime power fields $\mathbb{F}_{\boldsymbol{q}}$, where $q = 4, 8, 9, \text{and } 16$ was obtained using a modified MATLAB program (see Appendix A3).

3.2.1 Calculation over Prime Fields

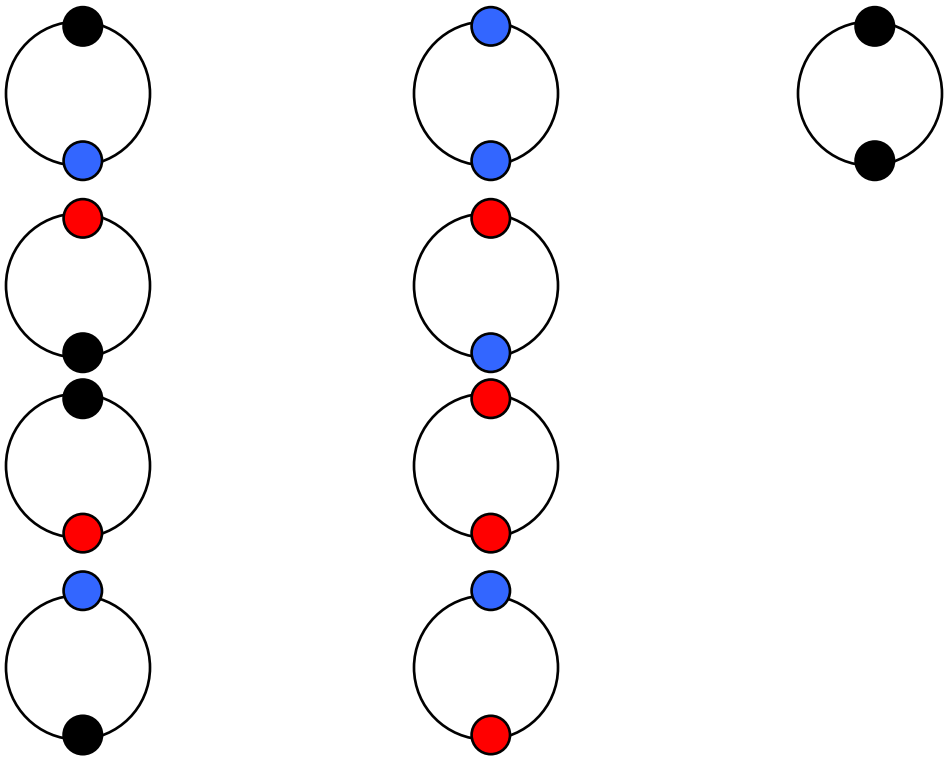
Example 4: Let $q = 3, m = 2, \text{and } \lambda = 2$, as in Example 3 above. Since $\mathbb{F}_{\boldsymbol{3}} = \{0, 1, 2\}$, there are a total of $3^2 = 9$ words. Therefore, the set S, consisting of all possible words of length 2, is $S_2 = \{[0\ 0], [0\ 1], [0\ 2], [1\ 0], [1\ 1], [1\ 2], [2\ 0], [2\ 1], \text{and } [2\ 2]\}$. Based on the relation defined in (14), the equivalence classes are as follows:

$$C1 = \{[0\ 1], [2\ 0], [0\ 2], [1\ 0]\},$$

$$C2 = \{[1\ 1], [2\ 1], [2\ 2], [1\ 2]\},$$

and $\quad C3 = \{[0\ 0]\}$,

In addition, to obtain the resulting equivalence classes based on the relation defined in (14), one can represent a ternary necklace of length 2, as in Example 4 above for the set S_2 using a circle with two beads. The numbers 0, 1, and 2 represent the black, blue, and red coloured beads of the circle, respectively. Figure 4 shows that the first word of the equivalence class $C1$ in the first circle is [0 1] with the top bead representing the number 0 and the bottom bead representing the number 1. Rotating the circle to the right, while multiplying the bottom bead by a constant λ (2 in this case), results in the second word [2 0] in the same equivalence class. Similarly, the other equivalence classes are obtained. Tables 5 through 11 show the results of enumerating the number of generalized necklaces over the prime fields $\mathbb{F}_{\boldsymbol{q}}$, where $q = 2, 3, 5, 7, 11, 13, 17, 19$ using MATLAB.



$C1$ $C2$ $C3$

Figure 4: The Number of Necklaces with a Constacyclic Shift $\lambda = 2$ for Example 4.

Table 5: The Number of Generalized Necklaces over $\mathbb{F}_3$ with $\lambda \in \mathbb{F}_3 \backslash \{0\}$.

$q = 3$		
m	λ	$number$
1	1,2	2
2	1	4
2	2	3
3	1,2	6
4	1	14
4	2	11
5	1,2	26
6	1	68
6	2	63
7	1,2	158
8	1	424
8	2	411
9	1,2	1098
10	1	2980
10	2	2955
11	1,2	8054
12	1	22218
12	2	22151
13	1,2	61322
14	1	170980
14	2	170823
15	1,2	478318
16	1	1345634
16	2	1345211
17	1,2	3798242
18	1	10762820
18	2	10761723
19	1,2	30585830
20	1	87172598
20	2	87169619

Table 6: The Number of Generalized Necklaces over $\mathbb{F}_5$ with $\lambda \in \mathbb{F}_5 \backslash \{0\}$.

$q = 5$		
m	λ	$number$
1	1,2,3,4	2
2	1,4	5
2	2,3	4
3	1,2,3,4	12
4	1	45
4	2,3	40
4	4	43
5	1,2,3,4	158
6	1,4	665
6	2,3	654
7	1,2,3,4	2792
8	1	12255
8	2,3	12208
8	4	12247
9	1,2,3,4	54262
10	1,4	244301
10	2,3	244144
11	1,2,3,4	1109732
12	1	5086965
12	2,3	5086290
12	4	5086943
13	1,2,3,4	23475062
14	1,4	108994145
14	2,3	108991354
15	1,2,3,4	508626416
16	1	2384198085
16	2,3	2384185792
16	4	2384197999
17	1,2,3,4	11219697842
18	1,4	52981961165
18	2,3	52981906904
19	1,2,3,4	250966925372
20	1	1192093139997
20	2,3	1192092895540
20	4	1192093139683

Table 7: The Number of Generalized Necklaces over $\mathbb{F}_7$ with $\lambda \in \mathbb{F}_7 \backslash \{0\}$.

$q = 7$		
m	λ	$number$
1	1,2,3,4,5,6	2
2	1,2,4	6
2	3,5,6	5
3	1,6	22
3	2,3,4,5	20
4	1,2,4	106
4	3,5,6	101
5	1,2,3,4,5,6	562
6	1	3298
6	2,4	3288
6	3,5	3269
6	6	3277
7	1,2,3,4,5,6	19610
8	1,2,4	120206
8	3,5,6	120101
9	1,6	747330
9	2,3,4,5	747290
10	1,2,4	4708486
10	3,5,6	4707925
11	1,2,3,4,5,6	29959498
12	1	192243598
12	2,4	192243388
12	3,5	192240101
12	6	192240301
13	1,2,3,4,5,6	1242166802
14	1,2,4	8074103814
14	3,5,6	8074084205
15	1,6	52750684582
15	2,3,4,5	52750683460
16	1,2,4	346176480306
16	3,5,6	346176360101
17	1,2,3,4,5,6	2280691313602
18	1	15077904438230
18	2,4	15077904431646
18	3,5	15077903684357
18	6	15077903690901
19	1,2,3,4,5,6	99990308643626
20	1,2,4	664935557188666
20	3,5,6	664935552480181

Table 8: The Number of Generalized Necklaces over $\mathbb{F}_{11}$ with $\lambda \in \mathbb{F}_{11}\backslash\{0\}$.

$q = 11$		
m	λ	$number$
1	1,2,3,4,5,6,7,8,9,10	2
2	1, 3,4,5,9	8
2	2,6,7,8,10	7
3	1,2,3,4,5,6,7,8,9,10	46
4	1,3,4,5,9	374
4	2,6,7,8,10	367
5	1,10	3226
5	2,3,4,5,6,7,8,9	3222
6	1,3,4,5,9	29576
6	2,6,7,8,10	29531
7	1,2,3,4,5,6,7,8,9,10	278390
8	1,3,4,5,9	2679860
8	2,6,7,8,10	2679487
9	1,2,3,4,5,6,7,8,9,10	26199450
10	1	259377496
10	2,6,7,8	259374247
10	3,4,5,9	259377468
10	10	259374271
11	1,2,3,4,5,6,7,8,9,10	2593742462
12	1,3,4,5,9	26153599626
12	2,6,7,8,10	26153570051
13	1,2,3,4,5,6,7,8,9,10	265559324186
14	1,3,4,5,9	2712499089704
14	2,6,7,8,10	2712498811315
15	1,10	27848321131766
15	2,3,4,5,6,7,8,9	27848321131586
16	1,3,4,5,9	287185814327186
16	2,6,7,8,10	287185811647327
17	1,2,3,4,5,6,7,8,9,10	2973217814701730
18	1,3,4,5,9	30888429545620424
18	2,6,7,8,10	30888429519420975
19	1,2,3,4,5,6,7,8,9,10	321889949728497614
20	1	3363749974922179006
20	2,6,7,8	3363749974662800047
20	3,4,5,9	3363749974922177514
20	10	3363749974662801511

Table 9: The Number of Generalized Necklaces over $\mathbb{F}_{13}$ with $\lambda \in \mathbb{F}_{13}\backslash\{0\}$.

$q = 13$		
m	λ	$number$
1	1,2,3,4,5,6,7,8,9,10,11,12	2
2	1,3,4,9,10,12	9
2	2,5,6,7,8,11	8
3	1,5,8,12	64
3	2,3,4,6,7,9,10,11	62
4	1,3,9	605
4	2,5,6,7,8,11	596
4	4,10,12	603
5	1,2,3,4,5,6,7,8,9,10,11,12	6190
6	1,12	67117
6	2,6,7,11	67040
6	3,4,9,10	67101
6	5,8	67054
7	1,2,3,4,5,6,7,8,9,10,11,12	747008
8	1,3,9	8497807
8	2,5,6,7,8,11	8497196
8	4,10,12	8497791
9	1,5,8,12	98189934
9	2,3,4,6,7,9,10,11	98189810
10	1,3,4,9,10,12	1148826961
10	2,5,6,7,8,11	1148820772
11	1,2,3,4,5,6,7,8,9,10,11,12	13576972684
12	1	161792326165
12	2,6,7,11	161792257796
12	3,9	161792324957
12	4,10	161792324835
12	5,8	161792258986
12	12	161792326039
13	1,2,3,4,5,6,7,8,9,10,11,12	1941507093542
14	1,3,4,9,10,12	23436764947605
14	2,5,6,7,8,11	23436764200598
15	1,5,8,12	284366072312932
15	2,3,4,6,7,9,10,11	284366072300554
16	1,3,9	3465711514660797
16	2,5,6,7,8,11	3465711506162396
16	4,10,12	3465711514659591
17	1,2,3,4,5,6,7,8,9,10,11,12	42403999604810482
18	1,12	520626884135163809
18	2,6,7,11	520626884036839784
18	3,4,9,10	520626884135029593
18	5,8	520626884036973876
19	1,2,3,4,5,6,7,8,9,10,11,12	6411931098137921540
20	1,3,9	79187349063152164621
20	2,5,6,7,8,11	79187349062003331472
20	4,10,12	79187349063152152243

Table 10: The Number of Generalized Necklaces over $\mathbb{F}_{17}$ with $\lambda \in \mathbb{F}_{17}\backslash\{0\}$.

$q = 17$		
m	λ	$number$
1	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	2
2	1,2,4,8,9,13,15,16	11
2	3,5,6,7,10,11,12,14	10
3	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	104
4	1,4,13,16	1317
4	2,8,9,15	1315
4	3,5,6,7,10,11,12,14	1306
5	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	17750
6	1,2,4,8,9,13,15,16	251543
6	3,5,6,7,10,11,12,14	251440
7	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	3663740
8	1,16	54499433
8	2,8,9,15	54499411
8	3,5,6,7,10,11,12,14	54498106
8	4,13	54499429
9	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	823526990
10	1,2,4,8,9,13,15,16	12599979635
10	3,5,6,7,10,11,12,14	12599961886
11	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	194726683568
12	1,4,13,16	3034491071421
12	2,8,9,15	3034491071215
12	3,5,6,7,10,11,12,14	3034490819776
13	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	47618163619742
14	1,2,4,8,9,13,15,16	751686729375359
14	3,5,6,7,10,11,12,14	751686725711620
15	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	11926762714636148
16	1	190082780818824465
16	2,8,9,15	190082780818821811
16	3,5,6,7,10,11,12,14	190082780764323706
16	4,13	190082780818824421
16	16	190082780818824457
17	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	3041324492229179282
18	1,2,4,8,9,13,15,16	48830154348281073059
18	3,5,6,7,10,11,12,14	48830154347457546070
19	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16	786422485806418831736
20	1,4,13,16	12700723145786264130933
20	2,8,9,15	12700723145786264095435
20	3,5,6,7,10,11,12,14	12700723145773664133550

Table 11: The Number of Generalized Necklaces over $\mathbb{F}_{19}$ with $\lambda \in \mathbb{F}_{19}\backslash\{0\}$.

$q = 19$		
m	λ	$number$
1	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18,	2
2	1,4,5,6,7,9,11,16,17	12
2	2,3,8,10,12,13,14,15,18	11
3	1,7,8,11,12,18	130
3	2,3,4,5,6,9,10,13,14,15,16,17	128
4	1,4,5,6,7,9,11,16,17	1822
4	2,3,8,10,12,13,14,15,18	1811
5	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18	27514
6	1,7,11	435760
6	2,3,10,13,14,15	435611
6	4,5,6,9,16,17	435738
6	8,12,18	435631
7	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18	7094222
8	1,4,5,6,7,9,11,16,17	117943232
8	2,3,8,10,12,13,14,15,18	117941411
9	1,18	1991899630
9	2,3,4,5,6,9,10,13,14,15,16,17	1991899370
9	7,8,11,12	1991899624
10	1,4,5,6,7,9,11,16,17	34061506732
10	2,3,8,10,12,13,14,15,18	34061479219
11	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18	588334640902
12	1,7,11	10246828768390
12	2,3,10,13,14,15	10246828329011
12	4,5,6,9,16,17	10246828764748
12	8,12,18	10246828332631
13	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18	179713604539562
14	1,4,5,6,7,9,11,16,17	3170661458613612
14	2,3,8,10,12,13,14,15,18	3170661451519391
15	1,7,8,11,12,18	56226396406998826
15	2,3,4,5,6,9,10,13,14,15,16,17	56226396406943800
16	1,4,5,6,7,9,11,16,17	1001532686116627842
16	2,3,8,10,12,13,14,15,18	1001532685998684611
17	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18	17909760973152948322
18	1	321380710798015121320
18	2,3,10,13,14,15	321380710796022350411
18	4,5,6,9,16,17	321380710798014249780
18	7,11	321380710798015121254
18	8,12	321380710796023221631
18	18	321380710796023221691
19	1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17,18	5784852794328402307382
20	1,4,5,6,7,9,11,16,17	104416592937661723156390
20	2,3,8,10,12,13,14,15,18	104416592937627661649659

3.2.2 Calculation over Prime Power Fields

The calculation over prime power fields $\mathbb{F}_{\boldsymbol{q}}$, where $q = p^a$, p is prime, and $a \geq 1$ is an integer, differs from that for prime fields. The order of an element $\alpha^i$of $\mathbb{F}_{\boldsymbol{q}}$ is $ord(\alpha^i) = \frac{j}{\gcd(j,i)}$, where $j = q - 1$ and α is a primitive element of $\mathbb{F}_{\boldsymbol{q}}$.

Example 5: Let $q = 4, m = 1,$ and $\lambda = \alpha$. Therefore, $ord(\alpha) = 3$, $1 \leq i \leq 3$, and (15) can be expressed as

$$c(1,4,\alpha) = \frac{1}{(4-1)ord(\alpha)1} \sum_{t \in \mathbb{F}_4 \setminus \{0\}, t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = 1}^{3} \left(4^{\gcd(1,i)} - 1\right) + 1$$

when $t = 1$ and $i = 1$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = \alpha$,

when $t = 1$ and $i = 2$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = \alpha^2$,

when $t = 1$ and $i = 3$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = 1$,

when $t = \alpha$ and $i = 1$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = \alpha^2$,

when $t = \alpha$ and $i = 2$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = 1$,

when $t = \alpha$ and $i = 3$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = \alpha$,

when $t = \alpha^2$ and $i = 1$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = 1$,

when $t = \alpha^2$ and $i = 2$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = \alpha$,

and when $t = \alpha^2$ and $i = 3$, $t^{\frac{m}{\gcd(m,i)}} \lambda^{\frac{i}{\gcd(m,i)}} = \alpha^2$.

Therefore, the number of generalized necklaces is

$$c(1,4,\alpha) = \frac{1}{9}\left[\left(4^{\gcd(1,3)} - 1\right) + \left(4^{\gcd(1,2)} - 1\right) + \left(4^{\gcd(1,1)} - 1\right)\right] + 1 = 2$$

To perform the multiplication over prime power fields in MATLAB, assume the elements are $\alpha = 2, \alpha^2 = 3, \ldots, \alpha^{(p^a-2)} = p^a - 1$. Therefore, $\mathbb{F}_{\boldsymbol{q}} = \{0,1,\alpha,\alpha^2,\ldots,\alpha^{q-2}\}$ and

$\mathbb{F}_q{}' = \{0,1,2,3,\dots,q-1\}$. The order of an element α^i in $\mathbb{F}_q$ is $ord(\alpha^i) = \frac{j}{\gcd(j,i)}$, where $j = q-1$, whereas the order of an element λ in $\mathbb{F}_q{}'$ is $ord(\lambda) = \frac{j}{\gcd(j,(\lambda-1))}$, where $j = q-1$ and $\lambda \in \mathbb{F}_q{}'\backslash\{0\}$. Based on above assumption, the condition for the generalized necklaces in (15) becomes

$$t^{\frac{m}{\gcd(m,i)}}\lambda^{\frac{i}{\gcd(m,i)}} = \alpha^{\left(\frac{m}{\gcd(m,i)}(t-1)+\frac{i}{\gcd(m,i)}(\lambda-1)\right) \bmod (q-1)} \tag{16}$$

where on the left side of the equation, $t \in \mathbb{F}_q\backslash\{0\}$, and $\lambda \in \mathbb{F}_q\backslash\{0\}$ while $t \in \mathbb{F}_q{}'\backslash\{0\}$, and $\lambda \in \mathbb{F}_q{}'\backslash\{0\}$ on the right side of the equation.

Example 6: Let $q = 4, m = 1,$ and $\lambda = \alpha = 2,$ as in the previous example. The order of λ, $ord(2) = \frac{3}{\gcd(3,(2-1))} = 3$. Let $T = \frac{m}{\gcd(m,i)}(t-1)$, $T2 = \frac{i}{\gcd(m,i)}(\lambda-1)$, and $T3 = (T+T2) \bmod (q-1)$, therefore

$$\alpha^{\left(\frac{m}{\gcd(m,i)}(t-1)+\frac{i}{\gcd(m,i)}(\lambda-1)\right) \bmod (q-1)} = \alpha^{T3} \tag{17}$$

When $t = 1$ and $i = 1$

$$T = \frac{1}{\gcd(1,1)}(1-1) = 0,\ T2 = \frac{1}{\gcd(1,1)}(2-1) = 1,$$
$$T3 = (T+T2) \bmod 3 = 1$$
$$\alpha^{T3} = \alpha^1$$

when $t = 1$ and $i = 2$

$$T = \frac{1}{\gcd(1,2)}(1-1) = 0,\ T2 = \frac{2}{\gcd(1,2)}(2-1) = 2,$$
$$T3 = (T+T2) \bmod 3 = 2$$
$$\alpha^{T3} = \alpha^2$$

when $t = 1$ and $i = 3$

$$T = \frac{1}{\gcd(1,3)}(1-1) = 0,\ T2 = \frac{3}{\gcd(1,3)}(2-1) = 3,$$
$$T3 = (T+T2) \bmod 3 = 0$$

$$\alpha^{T3} = \alpha^0 = 1$$

when $t = \alpha = 2$ and $i = 1$

$$T = \frac{1}{\gcd(1,1)}(2-1) = 1,\ \ T2 = \frac{1}{\gcd(1,1)}(2-1) = 1,$$

$$T3 = (T + T2) \bmod 3 = 2$$

$$\alpha^{T3} = \alpha^2$$

when $t = \alpha = 2$ and $i = 2$

$$T = \frac{1}{\gcd(1,2)}(2-1) = 1,\ \ T2 = \frac{2}{\gcd(1,2)}(2-1) = 2,$$

$$T3 = (T + T2) \bmod 3 = 0$$

$$\alpha^{T3} = \alpha^0 = 1$$

when $t = \alpha = 2$ and $i = 3$

$$T = \frac{1}{\gcd(1,3)}(2-1) = 1,\ \ T2 = \frac{3}{\gcd(1,3)}(2-1) = 3,$$

$$T3 = (T + T2) \bmod 3 = 1$$

$$\alpha^{T3} = \alpha^1$$

when $t = \alpha^2$ and $i = 1$

$$T = \frac{1}{\gcd(1,1)}(3-1) = 2,\ \ T2 = \frac{1}{\gcd(1,1)}(2-1) = 1,$$

$$T3 = (T + T2) \bmod 3 = 0$$

$$\alpha^{T3} = \alpha^0 = 1$$

when $t = \alpha^2$ and $i = 2$

$$T = \frac{1}{\gcd(1,2)}(3-1) = 2,\ \ T2 = \frac{2}{\gcd(1,2)}(2-1) = 2,$$

$$T3 = (T + T2) \bmod 3 = 1$$

$$\alpha^{T3} = \alpha^1$$

and when $t = \alpha^2$ and $i = 3$

$$T = \frac{1}{\gcd(1,3)}(3-1) = 2, \quad T2 = \frac{3}{\gcd(1,3)}(2-1) = 3,$$

$$T3 = (T + T2) \bmod 3 = 2$$

$$\alpha^{T3} = \alpha^2$$

Tables 12 through 15 show the results over the prime power fields $\mathbb{F}_4$, $\mathbb{F}_8$, $\mathbb{F}_9$, and $\mathbb{F}_{16}$.

Table 12: The Number of Generalized Necklaces over $\mathbb{F}_4$ with $\lambda \in \mathbb{F}_4 \backslash \{0\}$.

$q = 4$		
m	λ	$number$
1	$1,\alpha,\alpha^2$	2
2	$1,\alpha,\alpha^2$	4
3	1	10
3	α,α^2	8
4	$1,\alpha,\alpha^2$	24
5	$1,\alpha,\alpha^2$	70
6	1	238
6	α,α^2	232
7	$1,\alpha,\alpha^2$	782
8	$1,\alpha,\alpha^2$	2744
9	1	9726
9	α,α^2	9710
10	$1,\alpha,\alpha^2$	34990
11	$1,\alpha,\alpha^2$	127102
12	1	466198
12	α,α^2	466152
13	$1,\alpha,\alpha^2$	1720742
14	$1,\alpha,\alpha^2$	6391714
15	1	23861074
15	α,α^2	23860936
16	$1,\alpha,\alpha^2$	89479864
17	$1,\alpha,\alpha^2$	336860182
18	1	1272588226
18	α,α^2	1272587758
19	$1,\alpha,\alpha^2$	4822419422
20	$1,\alpha,\alpha^2$	18325211326

Table 13: The Number of Generalized Necklaces over $\mathbb{F}_{\mathbf{8}}$ with $\lambda \in \mathbb{F}_{\mathbf{8}}\backslash\{0\}$.

$\boldsymbol{q = 8}$		
m	λ	$number$
1	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	2
2	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	6
3	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	26
4	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	150
5	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	938
6	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	6258
7	1	42806
7	$\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	42800
8	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	299670
9	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	2130458
10	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	15339642
11	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	111557594
12	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	818092242
13	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	6041272682
14	1	44878047054
14	$\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	44878047024
15	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	335089258634
16	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	2513169584790
17	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	18922687509962
18	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	142971417811314
19	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	1083572842675610
20	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6$	8235153612004794

Table 14: The Number of Generalized Necklaces over $\mathbb{F}_9$ with $\lambda \in \mathbb{F}_9 \backslash \{0\}$.

$q = 9$		
m	λ	$number$
1	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	2
2	$1,\alpha^2,\alpha^4,\alpha^6$	7
2	$\alpha,\alpha^3,\alpha^5,\alpha^7$	6
3	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	32
4	$1,\alpha^4$	213
4	$\alpha,\alpha^3,\alpha^5,\alpha^7$	206
4	α^2,α^6	211
5	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	1478
6	$1,\alpha^2,\alpha^4,\alpha^6$	11107
6	$\alpha,\alpha^3,\alpha^5,\alpha^7$	11076
7	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	85412
8	1	672825
8	$\alpha,\alpha^3,\alpha^5,\alpha^7$	672606
8	α^2,α^6	672811
8	α^4	672821
9	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	5380862
10	$1,\alpha^2,\alpha^4,\alpha^6$	43586287
10	$\alpha,\alpha^3,\alpha^5,\alpha^7$	43584810
11	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	356602952
12	$1,\alpha^4$	2941985613
12	$\alpha,\alpha^3,\alpha^5,\alpha^7$	2941974476
12	α^2,α^6	2941985551
13	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	24441017582
14	$1,\alpha^2,\alpha^4,\alpha^6$	204257160907
14	$\alpha,\alpha^3,\alpha^5,\alpha^7$	204257075496
15	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	1715759435132
16	1	14476720898445
16	$\alpha,\alpha^3,\alpha^5,\alpha^7$	14476720225406
16	α^2,α^6	14476720898011
16	α^4	14476720898421
17	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	122626336026962
18	$1,\alpha^2,\alpha^4,\alpha^6$	1042323861617407
18	$\alpha,\alpha^3,\alpha^5,\alpha^7$	1042323856236546
19	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7$	8887182353111792
20	$1,\alpha^4$	75985409162693733
20	$\alpha,\alpha^3,\alpha^5,\alpha^7$	75985409119105970
20	α^2,α^6	75985409162690779

Table 15: The Number of Generalized Necklaces over $\mathbb{F}_{16}$ with $\lambda \in \mathbb{F}_{16}\backslash\{0\}$.

$q = 16$		
m	λ	$number$
1	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	2
2	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	10
3	$1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12}$	94
3	$\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^7,\alpha^8,\alpha^{10},\alpha^{11},\alpha^{13},\alpha^{14}$	92
4	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	1098
5	$1,\alpha^5,\alpha^{10}$	13986
5	$\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	13982
6	$1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12}$	186478
6	$\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^7,\alpha^8,\alpha^{10},\alpha^{11},\alpha^{13},\alpha^{14}$	186460
7	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	2556530
8	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	35791946
9	$1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12}$	509033346
9	$\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^7,\alpha^8,\alpha^{10},\alpha^{11},\alpha^{13},\alpha^{14}$	509033162
10	$1,\alpha^5,\alpha^{10}$	7330084546
10	$\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	7330084510
11	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	106619309362
12	$1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12}$	1563749966062
12	$\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^7,\alpha^8,\alpha^{10},\alpha^{11},\alpha^{13},\alpha^{14}$	1563749963868
13	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	23095382704466
14	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	343131401458882
15	1	5124095576058766
15	$\alpha,\alpha^2,\alpha^4,\alpha^7,\alpha^8,\alpha^{11},\alpha^{13},\alpha^{14}$	5124095576030432
15	$\alpha^3,\alpha^6,\alpha^9,\alpha^{12}$	5124095576058394
15	α^5,α^{10}	5124095576030796
16	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	76861433658352714
17	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	1157442765409226770
18	$1,\alpha^3,\alpha^6,\alpha^9,\alpha^{12}$	17490246233105427346
18	$\alpha,\alpha^2,\alpha^4,\alpha^5,\alpha^7,\alpha^8,\alpha^{10},\alpha^{11},\alpha^{13},\alpha^{14}$	17490246233105054410
19	$1,\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^5,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{10},$ $\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	265115311318997626034
20	$1,\alpha^5,\alpha^{10}$	4029752732052428965826
20	$\alpha,\alpha^2,\alpha^3,\alpha^4,\alpha^6,\alpha^7,\alpha^8,\alpha^9,\alpha^{11},\alpha^{12},\alpha^{13},\alpha^{14}$	4029752732052428961438

Chapter 4

Conclusion

4.1. Conclusion

This work defined and studied necklaces, circulant matrices, twistulant matrices, and their relations to the construction of linear block codes. In particular, the application of these objects to the construction of quasi-cyclic (QC) and quasi-twisted (QT) codes over finite fields was presented. In addition, generalization of necklaces and the corresponding analytical closed form expressions to count their numbers were discussed. The generalized necklaces were enumerated to facilitate the construction of quasi-cyclic and quasi-twisted codes. Both of these closed form expressions were enumerated over various prime and prime power fields using MATLAB.

4.2. Future Work

In addition to utilizing the results obtained in this work in the construction of QC and QT codes, future work can include the derivation of similar expressions for other variations of generalized necklaces over finite fields.

Bibliography

[1] V. Ch. Venkaiah, "Necklaces: Generalizations", *Resonance*, vol. 20, no. 6, pp. 542-555, 2015.

[2] J. Berstel and D. Perrin, "The origins of combinatorics on words", European Journal of Combinatorics, vol. 28, no. 3, pp. 996 - 1022, 2007.

[3] V. Ch. Venkaiah and T. A. Gulliver, "Quasi-cyclic codes over $\mathbb{F}_{13}$ and enumeration of defining polynomials", Journal of Discrete Algorithms, vol. 16, pp. 249-257, 2012.

[4] V. Ch. Venkaiah, T. A. Gulliver, and J. A. Algallaf, "Generalized necklaces and twistulant matrices", unpublished.

[5] E. Z. Chen and N. Aydin, "A database of linear codes over $\mathbb{F}_{13}$ with minimum distance bounds and new quasi-twisted codes from a heuristic search algorithm", Journal of Algebra Combinatorics Discrete Structures and Applications, vol. 2, no. 1, pp. 1-16, 2015.

[6] D. J. Costello, Jr., J. Hagenauer, H. Imai, and S. B. Wicker, "Applications of error-control coding", IEEE Trans. Inform. Theory, vol. 44, no. 6, pp. 2531-2560, 1998.

[7] S. Lin and D. J. Costello, Jr., Error control coding. Englewood Cliffs, N.J.: Prentice-Hall, 1983.

[8] R. Lidl and H. Niederreiter, Introduction to finite fields and their applications. Cambridge: Cambridge University Press, 1986.

[9] T. A. Gulliver, "New optimal ternary linear codes", IEEE Trans. Inform. Theory, vol. 41, no. 4, pp. 1182-1185, 1995.

[10] T. A. Gulliver and V. K. Bhargava, "Some best rate 1/p and rate (p-1)/p systematic quasi-cyclic codes over GF(3) and GF(4)", IEEE Trans. Inform. Theory, vol. 38, no. 4, pp. 1369-1374, 1992.

[11] T. A. Gulliver and V. K. Bhargava, "New good rate (m-1)/pm ternary and quaternary quasi-cyclic codes", Des Codes Crypt, vol. 7, no. 3, pp. 223-233, 1996.

[12] P. Greenough and R. Hill, "Optimal ternary quasi-cyclic codes", Des Codes Crypt, vol. 2, no. 1, pp. 81-91, 1992.

Appendices

A1. The Number of Generalized Necklaces in (13).

File Name: NecklacesF1.m

```
clear all
clc;
m=20;
q=2;
d = feval(symengine,'numlib::divisors',m);%find the
divisiors of m
a = 1/((q-1)*m);
for ii=1:length(d);

f=(feval(symengine,'numlib::phi',d(ii)))*(q.^(m./d(ii))-
1)*gcd(d(ii),(q-1));% Evaluating the function for every
value of d
    f_set(ii+1)=f;
end
f_total=sum(f_set);
Number_of_Necklaces=a*f_total+1
```

A2. The Number of Generalized Necklaces in (15) for Prime Fields.

File Name: NecklacesPF.m

```
clear all
clc;
n=6;
l=5;
q=13;
ord_l= feval(symengine,'numlib::order',l,q);%Evaluate the
order of lampda l
t=1:1:sym(q)-1;
i=1:1:sym(ord_l)*sym(n);
for ii=1:length(t)
    for jj=1:length(i)
        t1_1=(sym(ii).^(sym(n)./gcd(sym(n),sym(jj))));
        t1_2=(sym(l).^(sym(jj)./gcd(sym(n),sym(jj))));
        t1_3=sym(t1_1)*sym(t1_2);
        t1_4=mod(sym(t1_3),sym(q));%multiplication over
prime fields is defined mod q
        f_set(jj)=sym(t1_4);
        [col{ii}]=find(sym(f_set)==1);
    end
end
b=cell2mat(col);
g=(1./((sym(q)-1)*sym(ord_l)*sym(n)))*(sym(q).^gcd(n,b)-1);
format long
Number_of_Necklaces=sum(sym(g))+1
```

A3. The Number of Generalized Necklaces in (15) for Prime Power Fields.

File Name: NecklacesPPF.m

```
clear all
clc;
n=10;
l=2;
q=9;
ord_l=(sym(q)-1)/gcd(sym(q)-1,l-1);%Evaluate the order of
lampda l
t=1:1:sym(q)-1;
i=1:1:sym(ord_l)*sym(n);
for ii=1:length(t)
    for jj=1:length(i)
        T=(sym(n)./gcd(sym(n),sym(jj)))*(t(ii)-1);
        t1_1=(sym(ii));
        T2=(sym(jj)./gcd(sym(n),sym(jj)))*(l-1);
        t1_2=(sym(l));
        T3=mod((T+T2),sym(q)-1);
        t1_3=(sym(t1_1)*sym(t1_2)).^T3;%multiplication over
prime power fields
        f_set(jj)=sym(t1_3);
        [col{ii}]=find(sym(f_set)==1);
    end
end
b=cell2mat(col);
g=(1./((sym(q)-1)*sym(ord_l)*sym(n)))*(sym(q).^gcd(n,b)-1);
format long
Number_of_Necklaces=sum(sym(g))+1
```