Constructing Secret Sharing Schemes Based on Cyclic Codes

By

HOO MEI HUI

A project report submitted in partial fulfilment of the
requirements for the award of Bachelor of Science (Hons.)
Applied Mathematics With Computing

Faculty of Engineering and Science
Universiti Tunku Abdul Rahman

AUGUST 2014

DECLARATION OF ORIGINALITY

I hereby declare that this project report entitled "**Constructing Secret Sharing Schemes Based on Cyclic Codes** " is my own work except for citations and quotations which have been duly acknowledged. I also declare that it has not been previously and concurrently submitted for any other degree or award at UTAR or other institutions.

Signature : _____

Name : _____

ID No. : _____

Date : _____

APPROVAL FOR SUBMISSION

I certify that this project report entitled "**Constructing Secret Sharing Schemes Based on Cyclic Codes** " was prepared by **HOO MEI HUI** has met the required standard for submission in partial fulfilment of the requirements for the award of Bachelor of Science (Hons.) Applied Mathematics With Computing at Universiti Tunku Abdul Rahman.

Approved by,

Signature : _____

Supervisor : _____

Date : _____

ACKNOWLEDGEMENTS

I really appreciate the support given by my family and friends when I encountered problems in completing my project. Most of all, I wish to thank Dr Denis for his proper guidance and for sharing his knowledge in coding theory and cryptology with me. It was very enlightening.

HOO MEI HUI

Constructing Secret Sharing Schemes Based on Cyclic Codes

HOO MEI HUI

ABSTRACT

Secret sharing scheme is a method of breaking down a secret into smaller portions called shares and distribute them among a group of participants. The groups of participants who can reconstruct the secret by combining their shares forms the access set. Binary cyclic codes were used here as we believed that the polynomial base properties of cyclic codes ease the implementation of secret sharing schemes. To construct cyclic codes, we used the cyclotomic cosets approach and represented them in terms of group algebra notation. When we represent the cyclotomic cosets in term of group ring, we can easily verify them to be idempotent and since they can generate cyclic codes, we called them the generating idempotent. In order to construct cyclotomic cosets modulo n for any integer n, we developed a program to generate them. Using the program, we also observed several general patterns on the size of the cylotomic cosets modulo p where p is a prime number. We narrowed down our observation based on two types of primes p. The first type of prime p satisfy the condition that 2 is a primitive root modulo p while the second type of prime p satisfy 2 has order $\frac{p-1}{2}$ modulo p. After the construction of cyclic codes for $n = 9, 25$ and 49 based on all the possible generating idempotent, we selected a few cyclic codes where we can list out all of its codewords to construct the secret sharing schemes. We formed our access set by finding the set of all minimal codewords in the cyclic code. Although we did not discover any general pattern for the secret sharing schemes based on the generating idempotent, but we are interested to investigate further in a future work.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1: INTRODUCTION

Secret sharing scheme was invented by Shamir and Blakley independently in the year of 1979. Shamir's famous (t, w)-threshold secret sharing scheme constructs the key by means of polynomial interpolation. Similar to Shamir, Blakley defined a threshold scheme but based on hyperplane interpolation. The definition of the threshold secret sharing scheme is informally defined as follows (refer to Stinson (2006)): Let t, w be positive integers such that $t \leq w$. A (t, w)-threshold scheme is a method of sharing a key K among a set of w participants (denoted by P), in such a way that any t participants can compute the value of K, but no group of $t - 1$ participants can do so. The value of K is chosen by a special participant called the dealer. The dealer is denoted by D and we assume $D \notin P$. When D wants to share the key K among the participants in P, he distributes some partial information to each participants called share. The shares will be distributed secretly, so no participant knows the share given to another participant.

From the definition of the threshold secret sharing scheme, only t participants can determine the key. However, a more general circumstance is to specify which subsets of participants should be able to determine the key and which should not. Let Γ be a set of subset of P where the subsets in Γ are those subsets of participants that can reconstruct the key. Γ is called an access structure of a secret sharing scheme and each subset in Γ is called an authorized subset.

Another type of secret sharing scheme is the perfect secret sharing scheme. A perfect secret sharing scheme realizing the access structure Γ is a method of sharing a key K among the set of w participants (denoted by P), in such a way that the following properties are satisfied. Firstly, if an authorized subset of participants $B \subseteq P$ pool their shares, then they can determine the value of K. Secondly, if an unauthorized subset of participants $B \subseteq P$ pool their shares, then they can determine nothing about the value of K.

Besides the method used by Shamir and Blakley, the construction of secret sharing schemes can use linear codes also known as error-correcting codes which is used for encoding and decoding messages. To ease the encoding and decoding of words, one

naturally requires a cyclic shift of a codeword in a code C to be still a codeword in C. This combinatorial structure is fulfilled by cyclic codes which is a class of linear code. Fortunately, this structure can be converted into an algebraic one (refer to MacWilliams & Sloane (1977)).

1-1 Objectives

The objective of this project is to construct secret sharing scheme by using cyclic codes define over a binary finite field. We strongly believe that the polynomial base properties of cyclic codes will ease the implementation of secret sharing scheme. By observing the cyclotomic cosets modulo different modulus n, we generalize the number of cyclotomic cosets modulo n and the number of elements in each cosets. Furthermore, we introduce the use of group algebra notation and cyclotomic cosets to represent a cyclic code, in which we think that many properties of cyclic codes can be described more nicely in terms of group algebra.

1-2 Problem Statements

Secret sharing scheme is a method of sharing secrets in the form of shares to a subset of participants and the subset of these participants who can reconstruct the secret is called the access structure. In order to construct secret sharing schemes, we can use a special type of linear code called the cyclic code. The goal of using cyclic codes to construct the scheme is to list down all the minimal codeword in a cyclic code to form the access structure of the scheme. However, it might not be easy to determine all the minimal codeword of the cyclic code if the size is too big. Then, in order to construct cyclic codes, there are several methods to do so. We proposed to use cyclotomic cosets and represent them in terms of group algebra to construct cyclic codes. Is there some kind of pattern we are expecting from the cyclotomic cosets modulo different modulus in order to classify them to ease the construction of cyclic codes.

1-3 Research Methodology

Our main purpose of this project is to construct secret sharing schemes using a type of linear code called cyclic codes which have nice algebraic and combinatorial structures. Hence, in Project 1, a research study was done on the related topics like cyclic codes, cyclotomic cosets, primitive element, order, minimal codewords and secret sharing schemes to understand the basics before actually constructing the schemes.

In our project, we adopted the cyclotomic coset approach to construct the cyclic codes. To see a general pattern in the cyclotomic cosets for different modulo n, we developed a window-based application using $C\#$ to compute and display the cyclotomic cosets modulo n. During project 2, we further modified it and add on some features to help us in observing the pattern.

The modified application prompts the user to enter the specific value n and choose the value q. By default, the value q is set to 2. Then, if the values are valid, it will display the cyclotomic cosets modulo n and the number of elements for each cosets. However, if the values are invalid, an error message will appear.

Our scope for the modulus is narrowed down to two types of odd prime numbers with $q = 2$. The first type of prime number p is where 2 is a primitive root modulo p and the second type is where the order of 2 modulo p is $(p-1)/2$. We observed the pattern on the number of elements for all cyclotomic cosets modulo p^2, p^3 and for a general case p^n.

Using the observations, we formed a general formula for each cases and since the result held strong for most p, we defined them as theorems. Then, we constructed some cyclic codes based on cyclotomic cosets in term of group algebra for some of the theorems. We showed the detailed steps to find the dimension and minimum distance. In the process of finding the generator polynomial of the cyclic code, we used a matlab function called "gfdeconv" to perform polynomial division over $\mathbb{F}_2$. Finally, we constructed secret sharing schemes based on cyclic codes with small dimension generated by the generating idempotent in the second section.

1-4 Methodology and Planning

Our project used cyclotomic cosets to generate cyclic codes and cyclic codes to construct secret sharing schemes. In chapter 2, we explained the situation where we can use secret sharing schemes to solve a problem. Besides, we also provided a brief history on the inventors of secret sharing schemes and other authors who used linear codes to construct these schemes. Moreover, we briefly described the history of cyclic codes.

In chapter 3, we define cyclotomic cosets, primitive elements, idempotents, group algebra and cyclic codes. We also provided some examples to illustrate them. Topics that are in relation to cyclic codes such as irreducible polynomial, minimal polynomial, generator polynomial, minimum distance were briefly explained as well. At the end of the section of cyclotomic cosets, we explained the modifications made on the program and benefit of the new features that assisted us in observing the general pattern of the number of elements in each cyclotomic cosets modulo n.

In chapter 4, our results and discussions are broken down into three sections. In the first section, from the general pattern found on the number of cyclotomic cosets modulo n and the number of elements in each cosets, we proposed the results as theorems and proved them. In the second section, using the theorems from the first section, we constructed the cyclic codes for $n = 9, 25$ and 49. Then, in the last section, we constructed the secret sharing schemes using some of the cyclic codes from the second section, where we can list down all the codewords in order to find all the minimal codewords.

In chapter 5, we summarized our findings and discussions. Moreover, we provided a table where we listed down all the cyclic codes we constructed and indicated which cyclic codes were used to construct secret sharing schemes. Then, we concluded that we fulfilled our objectives and mentioned about our future goals.

The following is the gantt chart for project 1 and 2. At the end of the first week, a suitable supervisor was found and a project title was temporarily defined. The study on secret sharing schemes and cyclic codes were ongoing throughout project 1 and project 2. Proposal writing took roughly three weeks (week 5 to week 7) which also took place coherently with the research on secret sharing schemes and cyclic codes. Around week 8, the study on cyclotomic cosets began as it is related to the construction of cyclic codes. The program created to generate the set of cyclotomic cosets for odd

numbers took about two weeks. The study on cyclotomic cosets was ongoing, as well as the improvisation on the cyclotomic coset calculator to handle larger values. Interim report writing using Microsoft Word started around week 8 and later converted to LaTeX. During week 11, the interim report was completely written using LaTeX. The completed interim report was submitted in week 12. The figures below show the planning of project 1 and the milestones achieved along the period.

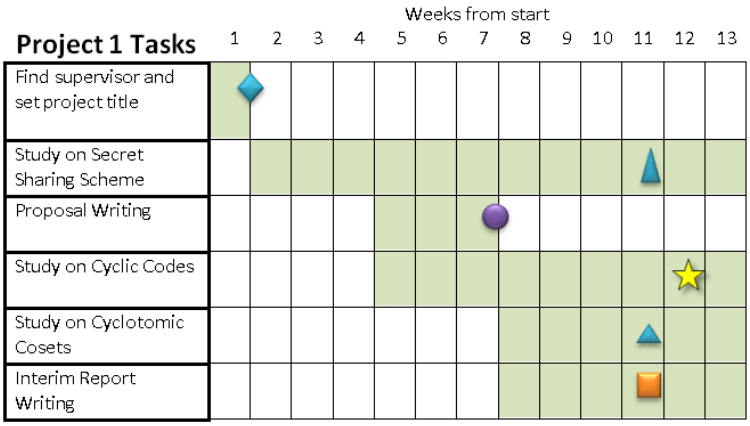


Figure 1.1: Gantt chart for Project 1

Found Dr Denis as supervisor and confirmed the temporary title as "Secret Sharing Scheme and Application"

The study on secret sharing scheme is still in progress. Read about basic definition of secret sharing schemes and construction of Shamir's Threshold scheme.

Proposal was submitted on 28th February 2014.

Learnt the basic of cyclic codes to encode and decode using the generator polynomial, generator matrix and check polynomial.

Generated cyclotomic cosets from n = 1 to n = 99 by writing a program to observe the pattern of n with different number of cyclotomic cosets and explain the reason behind it.

The interim report was completed and submitted on 4th April 2014.

Figure 1.2: Gantt chart description for Project 1

The modifications on the previous interim report started from week 1. The contents used in the interim report were used as the first three chapters in the final year project report. Since there were no classes, the meet up with the supervisor to discuss about the current progress was scheduled to be once or twice every two week. The study on secret sharing schemes were ongoing. The modifications made on the program started from the beginning of the semester and from there, we observed a certain pattern on the cyclotomic cosets for two types of prime numbers. At the end of week 7, we submitted the mid-semester monitoring form. Then for the consecutive weeks, we worked on

correcting the report and finalized it. Around week 10, we submitted our first draft of the report to the supervisor. Later, we checked the plagiarism rate of the report using Turnitin and corrected the report. At the end of week 12, we submitted the final year project report and after that we prepared for the oral presentation on Week 13.

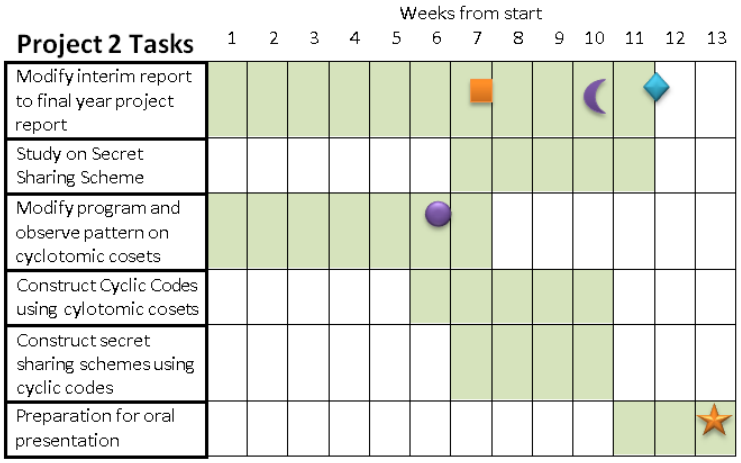


Figure 1.3: Gantt chart for Project 2

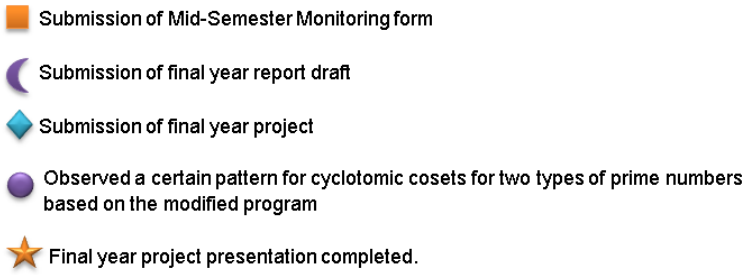


Figure 1.4: Gantt chart description for Project 2

CHAPTER 2: LITERATURE REVIEW

There was a safe in a wealthy man's house which contained jewelery, cash and important documents worth more than two billions. One day, the wealthy man fell sick and decided to tell partial information about the combination lock to his four children, Annie, Alice, Bob and Oscar but he does not trust any of them as they were greedy and afraid either one of them will possess all the assets. Hence, he wanted to design a method such that any three out of four of his children can open the safe but no individual or two children can do so. This problem can be solved by the means of secret sharing schemes and specifically a threshold secret sharing schemes.

In the year of 1979, George Blakley and Adi Shamir independently invented their own (t, w)-threshold secret sharing schemes. Shamir presented his threshold secret sharing scheme using Lagrange interpolating polynomial (refer to Shamir (1979)) while Blakley's scheme based on linear projective geometry(refer to Blakley (1979)). Since 1979, the development of secret sharing schemes have been progressing rapidly as they were used in many business-related problems. Then, in 1981, McEliece and Sarwate (refer to McEliece & Sarwate (1981)) pointed out the relationship between Shamir's threshold scheme and Reed-Solomon codes. Reed-Solomon codes is a family of cyclic codes which is also a type of error correcting codes and it was discovered that it can represent shares in Shamir's scheme.

About twelve years later, Massey (Massey (1993)) utilized linear codes for secret sharing schemes and discovered the relationship between the access structure and the minimal codewords of the dual code of the underlying code. In Massey's paper, it was shown that minimal codewords in the dual code can specify the access structure of the secret sharing scheme, and conversely. However, determining minimal codewords was extremely hard for general linear codes. Hence, this was only done for a few classes of special linear codes and one of them is cyclic codes. Several authors constructed secret sharing schemes using linear error correcting codes (refer to Yuan & Ding (2006) and refer to Li et al. (2010)). In these papers, cyclic codes became the topic of interest because of its unique algebraic and permutation structure.

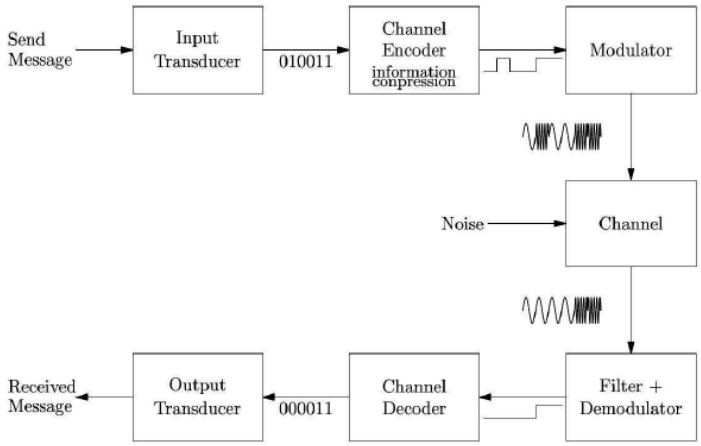
Dating back to 1948, the birth of coding theory was inspired by a classic paper

called "A Mathematical Theory of Communication" written by Shannon(refer to Shannon (1948)). Coding theory is the study of the properties of error-correcting codes which are used for data compression, cryptography and network coding. A special type of linear code is cyclic code which was first studied by Prange in 1957. In general, it was a tedious process to determine the minimum distance of a cyclic code from its generator polynomial. However, by choosing a special generator polynomial, we can categorized them into different families of cyclic codes, such as the Hamming codes, BCH codes and Reed-Solomon codes. Each family have its own characteristic to determine the minimum distance. Cyclic Hamming codes are one-error correcting which have a minimum distance of 3. However, if we want to correct more than one errors, we might need to increase the minimum distance by either lengthening or shortening the codewords. To correct multiple errors in a codeword, the family of Bose,Chaudhuri and Hocquenghem (BCH)codes was developed. BCH codes are, in fact, a generalization of the Hamming codes for multiple-error correction. The study started from binary cases for simplicity. Binary BCH codes were first discovered by A.Hocquenghem in 1959 and independently by R. C. Bose and D. K. Ray-Chaudhuri in 1960. Later,the generalizations of the binary BCH codes to q-ary codes were obtained by D. Gorenstein and N. Zierler in 1961.

CHAPTER 3: CYCLIC CODES

3-1 Introduction To Coding Theory

Without error correcting codes there would be no deep space travel, no satellite TV and no compact disc. Error-correcting codes are used to correct messages when they are transmitted through noisy channels. A *channel* is the physical medium where the information is transmitted. For example, telephone lines, air, outer-space satellite, etc. Noise are the interruptions that interfere with the channel and may alter the original message during transmission. It is impossible to send a plain message using human voice. Hence, we have to change it into a signal that can pass through a certain medium and this process is known as encoding.



This is a schematic diagram of a *communication system*. The whole idea is to protect a message from being corrupted, so we encode the message by adding some redundant information to it so when errors happen during transmission, it could be detected and possibly corrected.

The main objectives of channel coding is to construct encoders and decoders in such a way that the messages can be quickly encoded and decoded, easily transmitted with minimum cost, transmit as much information as possible, maximize the ability to detect errors and later correct them. However, transmitting more information means the chances of creating errors are higher which in turns might reduce the ability for error correction. Hence, we cannot really fulfill all these objectives at once but at least

we must achieve three or four goals to ensure successful transmission of the correct message.

In coding theory, there are codewords which is the mathematical abstraction of messages that will be sent over a channel (Ling & Xing (2004)). We define A to be a finite field, denoted as $\mathbb{F}_q$. Let $A = \{a_1, a_2, ..., a_q\}$ be a set of q symbols, which we refer to as a code alphabet and whose elements are called code symbols. A $q - ary$ block code of length n over $\mathbb{F}_q$ is a nonempty set C of $q - ary$ words having the same length n and the elements in C are known as the codewords.

A code C of length n and size M over $\mathbb{F}_q$ is known as an (n, M)-code. The size M is the maximum number of elements in a code. Usually the length and size of a code are given. There is another parameter called the minimum distance d. Hamming distance from word x to word y, denoted by $d(x, y)$ is the number of symbols at which x and y differ. d is the smallest Hamming distance and can also be denoted as $d(C)$. This minimum distance d is usually not given and we need to compute the Hamming distance on every pair of codewords in order to find the smallest distance. When the d is known, we call C as a (n, M, d)-code defined over the finite field $\mathbb{F}_q$.

The minimum distance is a very important parameter as it tell us the number of errors it can correct or detect when we transmit many codewords across a noisy channel. We have two very important theorems relating the error-correcting and error detecting capabilities of a code and $d(C)$ as follows (refer to Ling & Xing (2004)).

Theorem 3.1. (i) A code C can detect up to s errors in any codeword if $d(C) \geq s + 1$.

(ii) A code C can correct up to t errors in any codeword if $d(C) \geq 2t + 1$.

In general, there are two main types of code which are linear code and nonlinear code. A code C of length n is called a linear code if C is a subspace of a vector space $\mathbb{F}_q^n$, else, it is a nonlinear code. Since linear code is a subspace, it is also a vector space and is spanned by a basis. In coding theory, the basis for a linear code is often represented in the form of a matrix which is known as the generator matrix where the rows of the matrix are equivalent to the the basis of the code. All the codewords can be generated by this matrix. Then, from the generator matrix, we obtain the dimension k and with the formula q^k, we can get the total number of codewords for a linear code.

We often call linear code as $[n, k]$-code or if the d is known, it is called a $[n, k, d]$-code. Previously, we defined the Hamming distance. Now, we define the Hamming weight to be the number of nonzero symbols in a nonzero codeword. The minimum distance d is equals to the minimum weight of a nonzero codeword in C if C is a linear code. This property is advantageous as we do not need to compare every codeword to find the Hamming distance, instead we just look at each nonzero codeword for the Hamming weight which saves more steps and time.

3-2 Cyclotomic Cosets

Cyclotomic cosets can be used to construct cyclic codes. In each cyclotomic coset, the elements will repeat by themselves in the same sequence. Moreover, any pair of cyclotomic cosets modulo n are either disjoint or equivalent. When two integers are said to be co-prime or relatively prime to each other, it means that they have no common positive factors other than 1. Now, we introduce the formal definition of cyclotomic cosets modulo n.

Definition 3.2. (Refer to Ling & Xing (2004)) Let n be co-prime to q where q is a prime number. The *cyclotomic coset* of q (or *q-cyclotomic coset*) modulo n containing i is defined by

$$C_i = \{(i \cdot q^j (mod\, n)) \in \mathbb{F}_n : j = 0, 1, ...\}.$$

A subset $\{i_1, ..., i_t\}$ of $\mathbb{F}_n$ is called a $complete\ set\ of\ representatives$ of cyclotomic cosets of q modulo n if $C_{i_1}, ..., C_{i_t}$ are distinct and $\bigcup_{j=1}^{t} C_{i_j} = \mathbb{F}_n$.

When $q = 2$, n cannot be a multiple of 2 so they cannot be even. Hence, we can say that 2-cyclotomic coset modulo n exists if n is an odd integer.

Theorem 3.3. (a) It is easy to verify that two cyclotomic cosets are either equal or disjoint. Hence, the cyclotomic cosets partition $\mathbb{F}_n$.

(b) If $n = q^m - 1$ for some $m \geq 1$, each cyclotomic coset contains at most m elements, as $q^m \equiv 1 (mod\, q^m - 1)$.

(c) In particular where $n = q^m - 1$ for some $m \geq 1$, $|C_i| = m$ if $gcd(i, q^m - 1) = 1$.

Example 3.4. In this example, we construct the cyclotomic cosets of 2 modulo 31:

$$C_0 = \{0\}, \quad C_1 = \{1, 2, 4, 8, 16\}, \quad C_3 = \{3, 6, 12, 24, 17\},$$
$$C_5 = \{5, 10, 20, 9, 18\}, \quad C_7 = \{7, 14, 28, 25, 19\}, \quad C_{11} = \{11, 22, 13, 26, 21\},$$
$$C_{15} = \{15, 30, 29, 27, 23\}.$$

In C_1, after 16, we obtained $32 = 1(\text{mod } 31)$ and we stop the calculation as the other elements is a repeating cycle of $1, 2, 4, 8$ and 16. Then, we chose the smallest integer that is not in C_1 for the next cyclotomic coset modulo 31. The process repeats until the union of all cylotomic cosets modulo 31 is equals to $\mathbb{F}_{31}$. Clearly, we have $C_1 = C_2 = C_4 = C_8 = C_{16}$ and they are called the equivalent cosets where the elements are the same. The *complete set of representatives* of cyclotomic cosets of 2 modulo 31 is $\{0, 1, 3, 5, 7, 11, 15\}$. We see that the union of all cyclotomic cosets is equal to $\mathbb{F}_{31}$. Since $n = 31 = 2^5 - 1$, each cyclotomic coset contains at most 5 elements. In this case, since gcd$(i, 31)$=1 for all i, each cyclotomic coset has exactly 5 elements.

Example 3.5. In this example, we show that there is no 2-cyclotomic coset when $n = 6$.

$$C_0 = \{(0 \cdot 2^j (mod\, 6)) \in \mathbb{F}_6 : j = 0, 1, ...\} = \{0\},$$
$$C_1 = \{(1 \cdot 2^j (mod\, 6)) \in \mathbb{F}_6 : j = 0, 1, ...\} = \{1, 2, 4, 2, 4, 2, 4, ...\},$$
$$C_3 = \{(3 \cdot 2^j (mod\, 6)) \in \mathbb{F}_6 : j = 0, 1, ...\} = \{3, 0, 0, 0, ...\},$$
$$C_5 = \{(5 \cdot 2^j (mod\, 6)) \in \mathbb{F}_6 : j = 0, 1, ...\} = \{5, 4, ...\}.$$

Firstly, within C_1, the element 1 does not repeat after the last element 4. Secondly, C_1 and C_5 are neither equal nor disjoint. Hence, by the definition of cyclotomic coset, a complete set of representatives of cyclotomic cosets of 2 modulo 6 does not exist. The result is expected as $n = 6$ is not co-prime to $q = 2$.

As the value of n increases, hand calculation will be tedious and time-consuming. Hence, to find cyclotomic cosets for large numbers, a window application was developed. However, every program has its own limitation and this is no different. This program can only handle odd positive integer n up till 2205.

For the detailed and modified code used in the program, refer to appendix A. To simplify how the program works, we used the following algorithm:

1. We declared the variables used and initialised them with appropriate values.

   (i) A linked list called "remainder" is used because the length is dynamic and the values can be inserted either at the end or beginning of the list. Instead of the normal integer type, we are using ulong type here to prevent integer overflow which enable us to handle n up till 2205.

   (ii) An "outlist" string variable is used to store the output results.

2. When user typed in the modulus and the button is clicked, we perform the checking on it. It is invalid if it is not only numbers, it is more than 2205 and a multiple of 2. If it is invalid, error messages will pop up; else, we assign it to a local variable "modulus". If valid, we reset the required variables for the new modulus.

3. Then, we enter the first do-while loop and assigned "1" as the first element in the remainder list.

   (a) In the inner do-while loop, we found other elements to be in the list using the formula $remainder.First.Value * Math.Pow(2, j)\%modulus$.

   (b) We appended the value to the list if the value is not equals to the first value, which in this case is 1. We also appended the number to the outlist.

   (c) It looped until the latest value equals to the first value in the remainder list.

   (d) Later, we entered the while loop to find the smallest integer that is not in the current list. We used k which starts from 1 to compare with all the elements in the list. If k is equals to one of the elements, k is incremented by one; else, k is assigned as the new first value and the loop stops.

   (e) Finally, we checked whether the number of elements in the list is equals to the modulus-1. If it is true, the do-while loop terminates; else, it repeats step 3 with the new first value.

4. Lastly, we reset the previous output to be empty and assign outlist to the window text box to display the results.

In this program, instead of separating the $\mathbb{F}_n$ into distinct cyclotomic cosets which we should, we just inserted all the numbers into one list for each n. This is only a temporary solution. The following outputs are generated using the old program developed in Project 1.

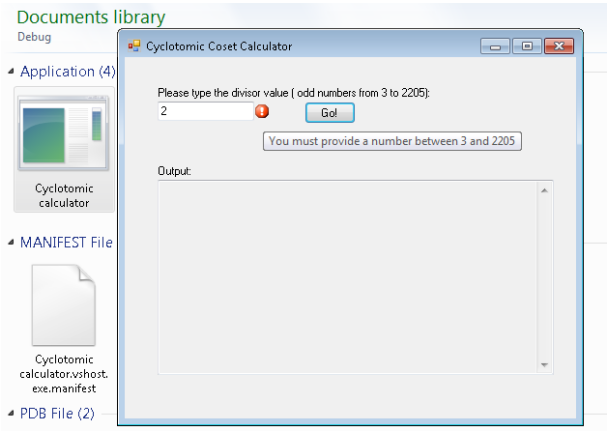


Figure 3.1: Error output when it is a number outside the range.

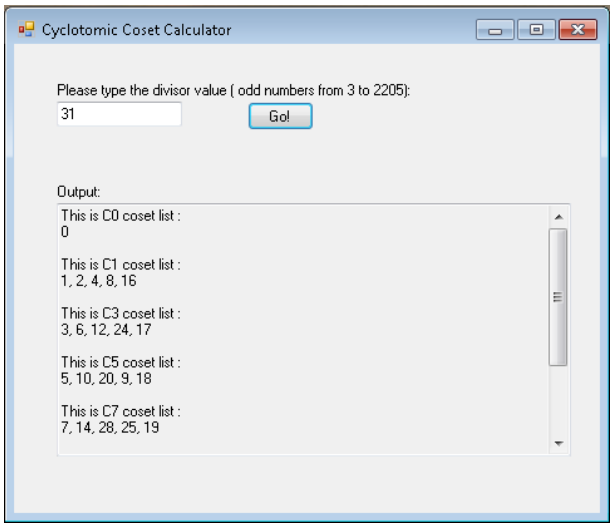


Figure 3.2: Correct output when *n=31*

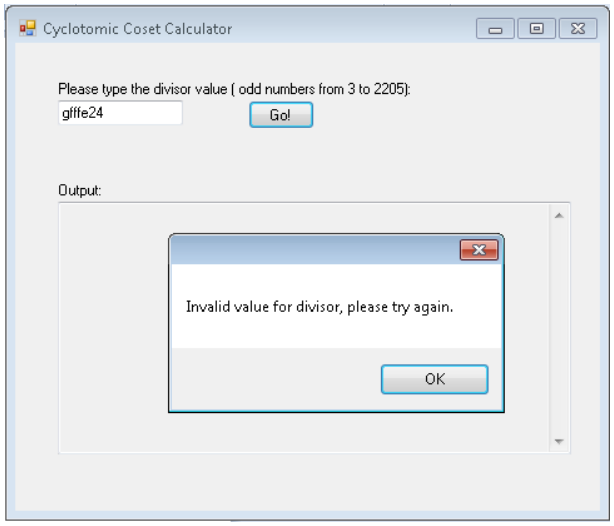


Figure 3.3: Error message box appear when input is not a number only.

3-2-1 Program Enhancement

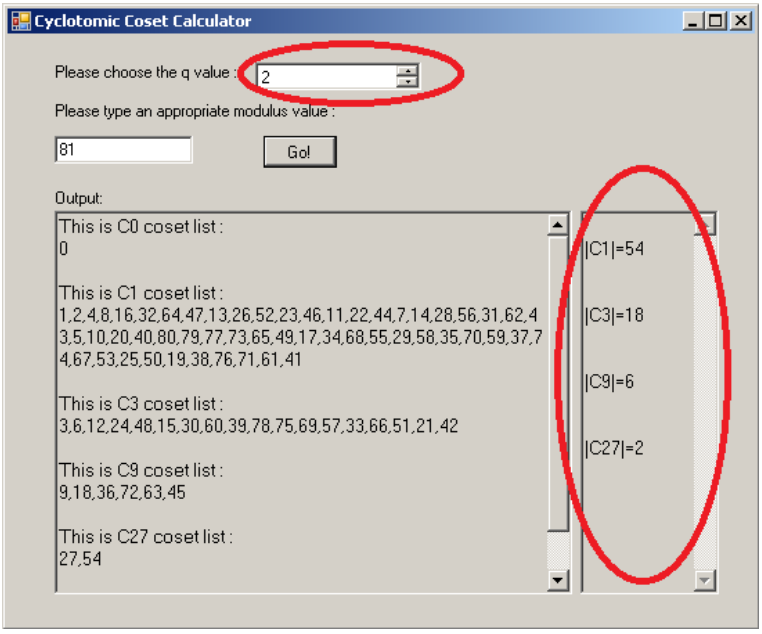


Figure 3.4: New interface of the program

In project II , slight modifications were made on the previous program to overcome the size limitation of the modulus n and assist on the observation of the pattern of cyclotomic cosets for different n. We modified the data type of the list from ulong type to BigInteger type which enables us to handle larger values of n below 49001. However, it is logical that the bigger the n value, the longer it takes to compute the result.

On the user interface, we also added in a separate output window which displays the number of elements in each coset to facilitate our observation. Previously, the choice of q was fixed to 2. Now, we modified the code so that it can handle any value of q. The purpose of this is to observe if there is any other pattern for ternary or other cases.

The algorithm remains unchanged for the calculation except we change the condition on checking the modulus. Previously, we check that the modulus must be less than 2205 and not a multiple of 2 to be valid. However, after the modification on the data type and q values, we changed the condition to be greater than 1 and not a multiple of q to be a valid modulus. There is no upper limit but in our project, the modulus below 49001 is sufficient to observe the pattern.

3-3 Finite Fields

A finite field $\mathbb{F}_q$ is a field that contains a finite number of elements. On the other hand, an integer ring is quite similar to a finite field which have the addition and multiplication operations, except that rings may or may not have a multiplicative inverse. However, an integer ring $\mathbb{Z}_m$ can be a field if and only if m is prime. A finite field can be generated by a primitive element.

3-3-1 Primitive Elements

Definition 3.6. (Refer to Ling & Xing (2004)) An element α in a finite field $\mathbb{F}_q$ is called the *primitive element* (or *generator*) of $\mathbb{F}_q$ if $\mathbb{F}_q = \{0, \alpha, \alpha^2, ..., \alpha^{q-1}\}$.

Definition 3.7. The *order* of a nonzero element $\alpha \in \mathbb{F}_q$, denoted by ord(α), is the smallest positive integer *k* such that $\alpha^k = 1$.

Example 3.8. Consider the field $\mathbb{F}_9 = \mathbb{F}_3[x]$, where α is a root of the irreducible polynomial $2 + x + x^2 \in \mathbb{F}_3[x]$. Then we have

Table 3.1: The set of elements in $\mathbb{F}_9$ generated by α and its vector representation.

Power	$\mathbb{F}_3[x]/(2+\alpha+\alpha^2)$	Vector
0	0	00
1	1	10
α	α	01
α^2	$1+2\alpha$	12
α^3	$2+2\alpha$	22
α^4	2	20
α^5	2α	02
α^6	$2+\alpha$	21
α^7	$1+\alpha$	11

Thus, $\mathbb{F}_9$=$\{0, \alpha, 1+2\alpha, 2\alpha+2, 2, 2\alpha, \alpha+2, 1+\alpha, 1\}$=$\{0, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8\}$, so α is a primitive element.

Proposition 3.9. (a) A nonzero element of $\mathbb{F}_q$ is a primitive element if and only if its order is $q - 1$.

(b) Every finite field has at least one primitive element.

Remark 3.10. Note that primitive element exist according to the proposition above, but they may not be unique.

3-3-2 Polynomial rings

A polynomial of positive degree is said to be reducible over $\mathbb{F}$ if it can be factored into two or more polynomials of lower degree. Otherwise, the polynomial is irreducible over $\mathbb{F}$. For example, the polynomial $h(x) = x^2 + 2x^3 \in \mathbb{F}_3[x]$ is of degree 3 and is reducible as $h(x) = x^2(1 + 2x)$. The factors in this case are x^2 and $1 + 2x$ and have lower degree than $h(x)$.

Another example is an irreducible polynomial $1 + x^3 + x^6$ over $\mathbb{F}_2[x]$. One of the methods to show that the polynomial is irreducible is to proof by contradiction. We can first assume the polynomial $f(x)$ is reducible and thus can be written in the form of $f(x) = a(x)b(x)$. Then, we consider all the different combinations of degree of $a(x)$ and $b(x)$ and show that it will lead to a contradiction. For this case, $deg(a(x)) = 1$ and $deg(b(x)) = 5$ is one of the consideration. However, the process of checking all the combination can be very tedious.

A *minimal polynomial* of an element $\alpha \in \mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$ is a nonzero monic polynomial $f(x)$ of the least degree in $\mathbb{F}_q[x]$ such that $f(\alpha) = 0$ (refer to Ling & Xing (2004)). Plus, a minimal polynomial is an irreducible polynomial.

Theorem 3.11. Let α be a primitive element of $\mathbb{F}_{q^m}$. Then the minimal polynomial of α^i with respect to $\mathbb{F}_q$ is

$$M^{(i)}(x) := \prod_{j \in C_i} (x - \alpha^j),$$

where C_i is the unique cyclotomic coset of q modulo $q^m - 1$ containing i.

Theorem 3.12. Let n be a positive integer with $gcd(q, n) = 1$. Suppose that m is a positive integer satisfying $n|(q^m - 1)$. Let α be a primitive element of $\mathbb{F}_{q^m}$ and let $M^{(j)}(x)$ be the minimal polynomial of α^j with respect to $\mathbb{F}_q$. Let $\{s_1, ..., s_t\}$ be a complete set of representatives of cyclotomic cosets of q modulo n. Then the polynomial $x^n - 1$ has the factorization into monic irreducible polynomials over $\mathbb{F}_q$:

$$x^n - 1 = \prod_{i=1}^{t} M^{((q^m-1)s_i/n)}(x).$$

The following result follows immediately from the above theorem.

Corollary 3.13. Let n be a positive integer with $gcd(q, n) = 1$. Then the number of monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ is equal to the number of cyclotomic cosets of q modulo n.

Example 3.14. Consider the polynomial $x^8 - 1$ over $\mathbb{F}_3$. It is easy to check that $\{0, 1, 2, 4, 5\}$ is a complete set of representatives of cyclotomic cosets of 3 modulo 8. Since 8 is a divisor of $3^2 - 1$, we consider the field $\mathbb{F}_9$. Let α be a root of $2 + x + x^2$. By Example 3.8, α is a primitive element of $\mathbb{F}_9$. Now, we list the cyclotomic cosets of 3 modulo 8 containing multiples of 1:

$$C_0 = \{0\}, \quad C_1 = \{1, 3\}, \quad C_2 = \{2, 6\}, \quad C_4 = \{4\}, \quad C_5 = \{5, 7\}.$$

Hence, we obtain

$$\begin{aligned}
M^{(0)}(x) &= 2 + x, \\
M^{(1)}(x) &= \prod_{j \in C_1} (x - \alpha^j) = x^2 + x + 2, \\
M^{(2)}(x) &= \prod_{j \in C_2} (x - \alpha^j) = x^2 + 1, \\
M^{(4)}(x) &= \prod_{j \in C_4} (x - \alpha^j) = x + 1, \\
M^{(5)}(x) &= \prod_{j \in C_5} (x - \alpha^j) = x^2 + 2x + 2,
\end{aligned}$$

By the theorem or corollary, we obtain the factorization of $x^8 - 1$ over $\mathbb{F}_3$ into monic irreducible polynomials:

$$\begin{aligned}
x^8 - 1 &= M^{(0)}(x)M^{(1)}(x)M^{(2)}(x)M^{(4)}(x)M^{(5)}(x) \\
&= (2 + x)(x^2 + x + 2)(x^2 + 1)(x + 1)(x^2 + 2x + 2).
\end{aligned}$$

3-4 Cyclic Codes

3-4-1 Introduction to Cyclic Codes

Cyclic codes are ideals of quotient ring $\mathbb{F}_q[x]/(x^n - 1)$. Quotient ring is a principal ideal commutative ring. (Refer to Ling & Xing (2004)) Let R be a commutative ring.

A nonempty subset I of R is called an ideal if both $a + b$ and $a - b$ belong to I, for all $a, b \in I$ and $r \cdot a \in I$, for all $r \in R$ and $a \in I$. An ideal I of a ring R is called a principal ideal if every element of I is a multiple of a generator g. The following is the formal definition of a cyclic code.

Definition 3.15. A code C is cyclic if it is linear and if any cyclic shift of a codeword is also a codeword, i.e., whenever $(c_0, c_1, ..., c_{n-1})$ is in C then so is $(c_{n-1}, c_0, ..., c_{n-2})$.

For example, $\{101, 011, 110\} \subset \mathbb{F}_2^3$ and $\{1202, 2021, 0212, 2120\} \subset \mathbb{F}_3^4$ are cyclic sets but they are not cyclic codes because they are not linear spaces.

Another three trivial cyclic codes are the $\{0..0\}, \{\lambda \cdot 1 : \lambda \in \mathbb{F}_q\}$ and $\mathbb{F}_q^n$. In order to convert the combinatorial structure of cyclic codes into an algebraic one, we consider the following correspondence:

$$\pi : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q[x]/(x^n - 1), (a_0, a_1, ..., a_{n-1}) \mapsto a_0 + a_1 x + ... + a_{n-1} x^{n-1}.$$

From now on, we will sometimes identify $\mathbb{F}_q^n$ with $\mathbb{F}_q[x]/(x^n - 1)$, and a vector $u = (u_0, u_1, ..., u_{n-1})$with the polynomial $u(x) = \sum_{i=0}^{n-1} u_i x^i$.

3-4-2 Generator Polynomials and Generator Matrices

Cyclic codes are a subclass of linear codes but not all linear codes has the ring structure like cyclic codes. Due to its combinatorial property, the codewords in a cyclic code can be represented by a polynomial and out of all the codewords, there will be one polynomial that acts like a basis and can generate the whole cyclic code. This polynomial is known as the generator polynomial. A generator polynomial is a unique monic polynomial of the least degree of a nonzero ideal I of $\mathbb{F}_q[x]/(x^n - 1)$(refer to Ling & Xing (2004)). For a cyclic code C, the generator polynomial of $\pi(C)$ is also called the generator polynomial of C.

Example 3.16. Given the cyclic code $C = \{000, 110, 011, 101\}$. The ideal of the cyclic code is $\pi(C) = \{0, 1 + x, x + x^2, 1 + x^2\}$. Hence, the generator polynomial is $1 + x$.

Theorem 3.17. Each monic divisor of $x^n - 1$ is the generator polynomial of some cyclic code in $\mathbb{F}_q^n$.

Corollary 3.18. There is a one-to-one correspondence between the cyclic codes in $\mathbb{F}_q^n$ and the monic divisors of $x^n - 1 \in \mathbb{F}_q[x]$.

Example 3.19. Find all binary cyclic codesof length 9.
To do so, we need to factorize the polynomial $x^9 - 1 \in \mathbb{F}_2[x]$:

$$x^9 - 1 = (1 + x)(1 + x + x^2)(1 + x^3 + x^6).$$

Factorizing the reducible polynomial above, we can use the cyclotomic coset approach in Example 3.14. Now, we list down all the monic divisors of $x^9 - 1$:

$$\begin{array}{lll} 1, & 1 + x^3 + x^6, & 1 + x + x^2, \\ 1 + x, & (1 + x)(1 + x + x^2), & (1 + x + x^2)(1 + x^3 + x^6) \\ 1 + x^9, & (1 + x)(1 + x^3 + x^6) & \end{array}$$

Thus there are eight binary cyclic codes of length 9 altogether. Based on the map π, we can easily write down all these cyclic codes. For instance, the cyclic code corresponding to the polynomial $(1 + x + x^2)(1 + x^3 + x^6)$ is $\{000000000, 111111111\}$

From the above example, we find that the number of cyclic codes of length n can be determined if we know the factorization of $x^n - 1$. We have the following result.

Theorem 3.20. Let $x^n - 1 \in \mathbb{F}_q[x]$ have the factorization

$$x^n - 1 = \prod_{i=1}^{r} p_i^{e_i}(x),$$

where $p_1(x), p_2(x), ..., p_r(x)$ are distinct monic irreducible polynomials and $e_i \geq 1$ for all $i = 1, 2, ..., r$. Then there are $\prod_{i=1}^{r}(e_i + 1)$ cyclic codes of length n over $\mathbb{F}_q$.

Theorem 3.21. Let $g(x)$ be the generator polynomial of an ideal of $\mathbb{F}_q[x]/(x^n - 1)$. Then the corresponding cyclic code has the dimension k if the degree of $g(x)$ is $n - k$.

Example 3.22. Based on the factorization: $x^9 - 1 = (1+x)(1+x+x^2)(1+x^3+x^6) \in \mathbb{F}_2[x]$, we know that there are only one binary [9,2]-cyclic codes:

$$< (1 + x)(1 + x^3 + x^6) >= \{000000000, 110110110, 011011011, 101101101\}.$$

However, we do not have any binary [9,5]-cyclic codes.

A cyclic code can be completely determined by its generator polynomial. Since cyclic code is also a linear code, it means it is also a subspace of $\mathbb{F}_q^n$. Then, cyclic codes have a generator matrix that can also generate all the codewords. Hence, we have the following result where the generator matrix is formed using the generator polynomial.

Theorem 3.23. Let $g(x) = g_0 + g_1x + ... + g_{n-k}x^{n-k}$ be the generator polynomial of a cyclic code C in $\mathbb{F}_q^n$ with $deg(g(x)) = n - k$. Then the matrix

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & \cdots & g_{n-k} & 0 & 0 & \cdots & 0 \\ \vdots & & & & & & & & \vdots \\ 0 & 0 & \cdots & g_0 & g_1 & \cdot & \cdot & \cdot & g_{n-k} \end{bmatrix},$$

is a generator matrix of C(note that we identify a vector with a polynomial).

Proof. It is sufficient to show that $g(x), xg(x), ..., x^{k-1}g(x)$ form a basis of C. It is clear that they are linearly independent over $\mathbb{F}_q$. By Theorem 3.21, we know that $\dim(C) = k$. The desired result follows. □

Example 3.24. Consider the binary [9,2]-cyclic code with generator polynomial $g(x) = 1 + x + x^3 + x^4 + x^6 + x^7$. Then this code has a generator matrix

$$G = \begin{bmatrix} g(x) \\ xg(x) \end{bmatrix} = \begin{bmatrix} 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

Since $k = 2$, there are 2^2 elements for this cyclic code, that is, $C = \{000000000, 110110110, 011011011, 101101101\}$. Clearly, the minimum distance d is 6.

Without factoring $x^n - 1$, we can replace the generator polynomial with a polynomial $e(x)$ called the idempotent. In fact, the generator polynomial and this special idempotent polynomial are minimal polynomials. The following definition was taken from van Lint (1999).

Theorem 3.25. Let C be a cyclic code. Then there is a unique codeword $e(x)$ which is an identity element for C.

Since $e^2(x) = e(x)$, this codeword is called the idempotent. There are other elements that satisfy this equality but there is only one unique identity for the cyclic code.

Since every codeword can be written as a multiple of the $e(x)$, we see that $e(x)$ generates C and we called it as a generating idempotent. We have the following theorem that relates the generator polynomial and the generating idempotent (refer to Huffman & Pless (2003)).

Theorem 3.26. If $e(x)$ is a generating idempotent of C, then the generator polynomial $g(x) = gcd(e(x), x^n - 1)$.

CHAPTER 4: RESULTS AND DISCUSSIONS

4-1 Cyclotomic Cosets

By narrowing down our focus on prime numbers p as modulus in constructing cyclotomic cosets modulo p, we observed a certain pattern on two types of primes p. We consider the primes p where 2 has order $p-1$ modulo p or $\frac{p-1}{2}$ modulo p. Examples of p that has order $p-1$ modulo p is $3, 5, 11, 13, 19, 29, 37$ whereas $7, 17, 23, 41$ and 47 have $\frac{p-1}{2}$ modulo p. Based on the primes p, we observed a pattern on the number of elements for the cyclotomic cosets modulo p^2 and p^3. The following theorems are the result of our observations.

Theorem 4.1. Let p be an odd prime. Suppose 2 is a primitive root modulo p and 2 has order p^2-p modulo p^2. Then, there are exactly two distinct nonzero 2-cyclotomic cosets modulo p^2.

Proof. The 2-cyclotomic coset modulo p^2 with coset representative 1 is

$$C_1 = \{1, 2, 2^2, ..., 2^{t_1-1}\},$$

where $2^{t_1} \equiv 1 (\text{mod } p^2)$. Since 2 has order p^2-p modulo p^2, i.e. $2^{p^2-p} \equiv 1 (\text{mod } p^2)$, then we have $t_1 = p^2-p$, and so $|C_1| = p^2-p$.

Next, since all the elements in C_1 is either 1 or even, we see that p being an odd prime is not in C_1. Thus, we construct the second 2-cyclotomic coset modulo p^2 with coset representative p, that is,

$$C_p = \{p, 2p, 2^2p, ..., 2^{t_p-1}p\},$$

where $2^{t_p}p \equiv p \,(\text{mod } p^2)$. The condition $2^{t_p}p \equiv p \,(\text{mod } p^2)$ is equivalent to $p^2 | 2^{t_p}p - p$, that is, $p | 2^{t_p} - 1$. Since 2 is a primitive root modulo p, then $t_p = \phi(p) = p-1$ where ϕ is the Euler-phi function, and so $|C_p| = p-1$. Now we have

$$C_1 = \{1, 2, 2^2, ..., 2^{p^2-p-1}\},$$

and

$$C_p = \{p, 2p, 2^2p, ..., 2^{p-2}p\},$$

If $y \in C_1 \cap C_p$, then $y \in C_1$ and $y \in C_p$, and so $y = 2^j$ and $y = 2^k p$ for some integers j, k (w.l.o.g we may assume that $j > k$). Then, we have $2^j = 2^k p$ that implies $2^{j-k} = p$, which is a contradiction as an odd prime p cannot be even. Therefore, we conclude that $C_1 \cap C_p = \emptyset$. Next, clearly for all $z \in \mathbb{Z}_{p^2} \subseteq C_1 \cup C_p \cup \{0\}$ as we have $|C_1 \cup C_p \cup \{0\}| = p^2 - p + p - 1 + 1 = p^2 = |\mathbb{Z}_{p^2}|$. Therefore, we conclude that $\mathbb{Z}_{p^2} = C_1 \cup C_p \cup \{0\}$. The results follows directly. □

Theorem 4.2. Let p be an odd prime. Suppose 2 has order $p^3 - p^2$ modulo p^3. Then, there are exactly three distinct nonzero 2-cyclotomic cosets modulo p^3.

Proof. Given 2 has order $p^3 - p^2$ modulo p^3, then

$$2^{p^3-p^2} \equiv 1(mod\, p^3). \tag{4.1}$$

Thus, by Euler's Theorem together with the definition of order, we have

$$2^{p^2-p} \equiv 1(mod\, p^2), \tag{4.2}$$

and

$$2^{p-1} \equiv 1(mod\, p). \tag{4.3}$$

The first 2-cyclotomic coset modulo p^3 with coset representative 1 is

$$C_1 = \{1, 2, 2^2, ..., 2^{t_1-1}\},$$

where $2^{t_1} \equiv 1 \pmod{p^3}$. From (4.1), we see that $t_1 = p^3 - p^2$ and so $|C_1| = p^3 - p^2$. Next, since $p \notin C_1$, we construct

$$C_p = \{p, 2p, 2^2p, ..., 2^{t_p-1}p\},$$

where $2^{t_p}p \equiv p \pmod{p^3}$ which is equivalent to $2^{t_p} \equiv 1 \pmod{p^2}$ and so $t_p = p^2 - p = |C_p|$ (follows from (4.2)). If $p^2 \in C_p$, then $p^2 = 2^i p$ for some i implies that $p = 2^i$ which is a contradiction. Hence, $p^2 \notin C_p$. Finally, as $p^2 \notin C_1$ and $p^2 \notin C_p$, we consider

$$C_{p^2} = \{p^2, 2p^2, 2^2p^2, ..., 2^{t_{p^2}-1}p^2\},$$

where $2^{t_{p^2}}p^2 \equiv p^2 \pmod{p^3}$ which is equivalent to $2^{t_{p^2}} \equiv 1 \pmod{p}$ and so $t_{p^2} = p - 1$ (follows from (4.3)). Now, we have

$$|C_1| = p^3 - p^2,$$

$$|C_p| = p^2 - p,$$

$$|C_{p^2}| = p - 1,$$

and so

$$|C_1| + |C_p| + |C_{p^2}| + |\{0\}| = p^3 - p^2 + p^2 - p + p - 1 + 1 = p^3 = |\mathbb{Z}_{p^3}|.$$

Suppose that $x \in C_1 \cap C_p$. Then $x \in C_1$ and $x \in C_p$ which implies $x = 2^j$ and $x = 2^k p$ for some integers j, k (w.l.o.g assume $j \geq k$). It follows that $2^j = 2^k p$ and then $2^{j-k} = p$, which is a contradiction as an odd prime p cannot be even. Hence, $C_1 \cap C_p = \emptyset$.

Next, suppose that $y \in C_1 \cap C_{p^2}$. Then $y \in C_1$ and $y \in C_{p^2}$ which implies $y = 2^j$ and $y = 2^k p^2$ for some integers j, k (w.l.o.g assume $j \geq k$). It follows that $2^j = 2^k p^2$ implies $2^{j-k} = p^2$, is a contradiction as the square of odd prime p is odd and cannot be even. Hence, $C_1 \cap C_{p^2} = \emptyset$.

Finally, suppose that $z \in C_p \cap C_{p^2}$. Then $z \in C_p$ and $z \in C_{p^2}$ which implies $z = p2^j$ and $z = p^2 2^k$ for some integers j, k (w.l.o.g assume $j \geq k$). It follows that $p2^j = p^2 2^k$ and it implies $2^{j-k} = p$ since $p \neq 0$, is a contradiction. Hence, $C_p \cap C_{p^2} = \emptyset$.

Therefore, we can conclude that $\mathbb{Z}_{p^3} = C_1 \cup C_p \cup C_{p^2} \cup \{0\}$ and $C_i \cap C_j = \emptyset$ for all $i,\ j \in \{1, p, p^2\}$. And hence, C_1, C_p and C_{p^2} are the required 2-cyclotomic cosets modulo p^3. □

Theorem 4.3. Let p be an odd prime and $n \geq 2$. Suppose 2 is a primitive root modulo p^n. Then there are exactly n nonzero 2-cyclotomic cosets modulo p^n with

$$\begin{aligned} |C_1| &= p^n - p^{n-1}, \\ |C_p| &= p^{n-1} - p^{n-2}, \\ &\vdots \\ |C_{p^{n-1}}| &= p - 1. \end{aligned}$$

Proof. Let p be an odd prime and $n \geq 2$. Let $P(n)$ be the statement "Suppose 2 is a primitive root modulo p^n. Then there are exactly n nonzero cylcotomic cosets modulo p^n."

For the basis step, when $n = 2$, we shown that there are exactly 2 nonzero cyclotomic cosets modulo p^2 by Theorem 4.1. Hence, $P(2)$ is true.

Inductively, suppose $P(k)$ is true for some $k \geq 2$, that is, there are exactly k nonzero cyclotomic cosets modulo p^k provided 2 is a primitive root modulo p^k. Hence,

when $n = k + 1$, we suppose that 2 is a primitive root modulo p^{k+1}. From $P(k)$, we have k nonzero cyclotomic cosets modulo p^k, that is $C_1, C_p, C_{p^2}, ...$ and $C_{p^{k-1}}$ and in total there are $p^k - 1$ elements. When we increase the modulus from p^k to p^{k+1}, the same elements remain in the same cyclotomic cosets but the same cosets can now be filled with more elements from $\mathbb{Z}_{p^{k+1}}$.

Suppose there are exactly k nonzero cyclotomic cosets modulo p^{k+1}. Then, $C_1 \cup C_p \cup C_{p^2} \cup ... \cup C_{p^{k-1}} = \mathbb{Z}_{p^{k+1}} = \{1, 2, ..., p^k, p^k + 1, ..., p^{k+1} - 1\}$. Since $p^k + 1$ is not a multiple of p so it is not in $C_p, C_{p^2}, ...,$ and $C_{p^{k-1}}$ and it is forced to be in C_1. Same goes for other elements in $\mathbb{Z}_{p^{k+1}}$ that is not a multiple of p must be in C_1. Then, the remaining elements like $\{..., p^k + p, .., p^k + p^2, ..., p^k + p^k, ...\}$ which are multiples of p modulo p^{k+1} will be in their respective cyclotomic cosets modulo p^{k+1}. For example, $p^k + p^2 \in C_{p^2}$ but not in C_p because it is in the form of $2^j p^2$ instead of $2^i p$ for some integers i and j.

However, p^k is not in any of these k cyclotomic cosets. Suppose we assume that p^k is in one of these cosets. Then, $p^k = p^l 2^t$ for some integers l and t where $0 \leq l < k$, implies $p^{k-l} = 2^t$ which is a contradiction. Hence, p^k must be the smallest integer that is in the new cyclotomic coset modulo p^{k+1} that is C_{p^k}. This contradicts the assumption that there are exactly k nonzero cyclotomic cosets modulo p^{k+1}. Hence, there are exactly $k + 1$ nonzero cyclotomic cosets modulo p^{k+1}.

Hence, $P(k+1)$ is true. By mathematical induction, $P(n)$ is true for all $n \geq 2$. □

Theorem 4.4. Let p be an odd prime. Suppose 2 has order $\frac{p-1}{2}$ modulo p and 2 has order $\frac{p(p-1)}{2}$ modulo p^2. Then there are exactly 4 distinct nonzero 2-cyclotomic cosets modulo p^2.

Proof. The cyclotomic coset modulo p^2 with coset representative 1 is

$$C_1 = \{1, 2, 2^2, ..., 2^{t_1 - 1}\},$$

where $2^{t_1} \equiv 1 \pmod{p^2}$. Since 2 has order $\frac{p(p-1)}{2}$ modulo p^2, then we have $t_1 = \frac{p(p-1)}{2}$ and so $|C_1| = \frac{p(p-1)}{2}$.

Next, for all $x \in C_1$, $x = 1$ or x is even, we choose an odd prime q that is the smallest quadratic non-residue modulo p where $q \notin C_1$ and $q < \sqrt{p} + 1$. Thus, we next construct the second 2-cyclotomic coset modulo p^2 with coset representative q,

that is,

$$C_q = \{q, 2q, 2^2q, ..., 2^{t_q-1}q\},$$

where $2^{t_q}q \equiv q \pmod{p^2}$. The condition $2^{t_q}q \equiv q \pmod{p^2}$ can be reduced to $2^{t_q} \equiv 1 \pmod{p^2}$, which gives us $t_q = \frac{p(p-1)}{2}$ and also $|C_q| = \frac{p(p-1)}{2}$.

Next, since $p \notin C_1$ and $p \notin C_q$, we consider

$$C_p = \{p, 2p, 2^2p, ..., 2^{t_p-1}p\},$$

where $2^{t_p}p \equiv p \pmod{p^2}$ which is equivalent to $2^{t_p} \equiv 1 \pmod{p}$. Since 2 has order $\frac{p-1}{2}$ modulo p, then we have $t_p = \frac{p-1}{2}$ and so $|C_p| = \frac{p-1}{2}$.

Finally, as $pq \notin C_1 \cup C_q \cup C_p$, we construct the last cyclotomic coset modulo p^2 with coset representative pq, that is,

$$C_{pq} = \{pq, 2pq, 2^2pq, ..., 2^{t_{pq}-1}pq\},$$

where $2^{t_{pq}}pq \equiv pq \pmod{p^2}$ which is equivalent to $2^{t_{pq}}q \equiv q \pmod{p}$. Similarly, it can be reduced to $2^{t_{pq}} \equiv 1 \pmod{p}$. Then we have that $t_{pq} = \frac{p-1}{2}$ and so $|C_{pq}| = \frac{p-1}{2}$.
Now, we have

$$|C_1| = |C_q| = \frac{p(p-1)}{2},$$

and

$$|C_p| = |C_{pq}| = \frac{p-1}{2},$$

and clearly, $|C_1| + |C_q| + |C_p| + |C_{pq}| + |\{0\}| = |\mathbb{Z}_{p^2}|$. The proof that all cyclotomic cosets are mutually disjoint are similar to the previous theorems. Hence, C_1, C_q, C_p and C_{pq} are the required 2-cyclotomic cosets modulo p^2. □

Theorem 4.5. Let p be an odd prime. Suppose 2 has order $\frac{p^2(p-1)}{2}$ modulo p^3. Then there are exactly 6 distinct nonzero 2-cyclotomic cosets modulo p^3.

Proof. Given 2 has order $\frac{p^2(p-1)}{2}$ modulo p^3, then

$$2^{\frac{p^2(p-1)}{2}} \equiv 1(mod\, p^3). \tag{4.4}$$

Thus, by Euler's Theorem together with the definition of order, we have

$$2^{\frac{p(p-1)}{2}} \equiv 1(mod\, p^2), \tag{4.5}$$

and

$$2^{\frac{p-1}{2}} \equiv 1(mod\, p). \tag{4.6}$$

The cyclotomic coset modulo p^3 with coset representative 1 is

$$C_1 = \{1, 2, 2^2, ..., 2^{t_1-1}\},$$

where $2^{t_1} \equiv 1 \pmod{p^3}$. From above, we have $t_1 = \frac{p^2(p-1)}{2}$ and so $|C_1| = \frac{p^2(p-1)}{2}$.

Next, we choose an odd prime q that is the smallest quadratic non-residue modulo p where $q < \sqrt{p} + 1$. Obviously, $q \notin C_1$, so we construct

$$C_q = \{q, 2q, 2^2q, ..., 2^{t_q-1}q\},$$

where $2^{t_q}q \equiv q \pmod{p^3}$ which can be reduced to $2^{t_q} \equiv 1 \pmod{p^3}$, which gives us $t_q = \frac{p^2(p-1)}{2}$ and so $|C_q| = \frac{p^2(p-1)}{2}$.

Moving forward, since $p \notin C_1 \cup C_q$, we consider the third cyclotomic coset modulo p^3 with coset representative p, that is,

$$C_p = \{p, 2p, 2^2p, ..., 2^{t_p-1}p\},$$

where $2^{t_p}p \equiv p \pmod{p^3}$ which is equivalent to $2^{t_p} \equiv 1 \pmod{p^2}$. Then, we have $t_p = \frac{p(p-1)}{2}$ and so $|C_p| = \frac{p(p-1)}{2}$ (follows from (4.5)).

Similar to previous theorem, we consider pq which is not in any of the three cyclotomic cosets. We then construct

$$C_{pq} = \{pq, 2pq, 2^2pq, ..., 2^{t_{pq}-1}pq\},$$

where $2^{t_{pq}}pq \equiv pq \pmod{p^3}$ which is equivalent to $2^{t_{pq}}q \equiv q \pmod{p^2}$. It can be reduced to $2^{t_{pq}} \equiv 1 \pmod{p}$. Then we have that $t_{pq} = \frac{p(p-1)}{2}$ and so $|C_{pq}| = \frac{p(p-1)}{2}$.

Next, as $p^2 \notin C_1 \cup C_q \cup C_p \cup C_{pq}$, we consider

$$C_{p^2} = \{p^2, 2p^2, 2^2p^2, ..., 2^{t_{p^2}-1}p^2\},$$

where $2^{t_{p^2}}p^2 \equiv p^2 \pmod{p^3}$ which is equivalent to $2^{t_{p^2}} \equiv 1 \pmod{p}$ and so $t_{p^2} = \frac{p-1}{2}$ (follows from (4.6)). Finally, we consider p^2q as it is also not in the other five cyclotomic cosets modulo p^3 and hereby construct the cyclotomic coset modulo p^3, that is,

$$C_{p^2q} = \{p^2q, 2p^2q, 2^2p^2q, ..., 2^{t_{p^2q}-1}p^2q\},$$

where $2^{t_{p^2q}}p^2q \equiv p^2q \pmod{p^3}$ which is equivalent to $2^{t_{p^2q}}q \equiv q \pmod{p}$. Later, it is reduced to $2^{t_{p^2q}} \equiv 1 \pmod{p}$. Clearly, we see that $t_{p^2q} = \frac{p-1}{2} = |C_{p^2q}|$ (follows from (4.6)).

The sum of all six cyclotomic cosets with $|\{0\}|$ gives the size of $\mathbb{Z}_{p^3}$. The verification of all cyclotomic cosets to be mutually disjoint sets can be done using the technique in previous theorems. Hence, the required 2-cyclotomic cosets modulo p^3 are $C_1, C_q, C_p, C_{pq}, C_{p^2}$, and C_{p^2q}. □

4-2 Construction of Cyclic Codes

In this section, we will illustrate the construction of $[9, k, d]$and $[25, k, d]$ cyclic codes using Theorem 4.1 while for $[49, k, d]$ cyclic codes, we are using Theorem 4.4 from previous section. Throughout this whole section, we are dealing with binary cyclic codes.

4-2-1 Construction of [$9, k, d$]-Cyclic Codes

Now, we construct the cyclic codes with $n = 9$. Using Theorem 4.1, we verified that 2 is a primitive root modulo 3. Hence, there are exactly two nonzero cyclotomic cosets modulo 9. The following are the 2-cyclotomic cosets modulo 9.

$$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 7, 5\} \text{ and } C_3 = \{3, 6\}.$$

To represent these cosets in term of group ring, we let $\Omega_1 = \sum_{s \in C_1} g^s \in \mathbb{F}[\mathbb{Z}_9]$ and $\Omega_2 = \sum_{r \in C_3} g^r \in \mathbb{F}[\mathbb{Z}_9]$. In term of group ring, the cyclotomic cosets of $\mathbb{F}[\mathbb{Z}_9]$ are

$$\begin{aligned}
\Omega_0 &= g^0, \\
\Omega_1 &= g^1 + g^2 + g^4 + g^8 + g^7 + g^5, \\
\Omega_2 &= g^3 + g^6.
\end{aligned}$$

We can see that $\Omega_0^2 = 1^2 = 1 = \Omega_0$ and easily verify that $\Omega_1^2 = \Omega_1$ and $\Omega_2^2 = \Omega_2$ as well as the union of different Ω are also idempotent. These idempotent are called the generating idempotent as each of them can generate a cyclic code.

There are two ways to find the dimension and minimum distance of a cyclic code from each generating idempotent. The first way is to form a matrix by cyclic shifting the generating idempotent until it is the same as the original generating idempotent. Then, we perform Gaussian elimination to obtain the row echelon form and get the

dimension k. The second method to obtain the dimension is by using Theorem 3.26 to find the generator polynomial.

After obtaining k, we find the weight for all combination of the generator polynomial or idempotent; or we can list down all the elements for the cyclic code to find the minimum distance d. It is preferable to use the second method as we can avoid handling large matrix which consumes more time and effort for latter cases.

Clearly, the generator polynomial for Ω_0 is 1 so <Ω_0> is a $[9, 9, 1]$-cyclic code.

For Ω_1, the generator matrix G is found as follows:

$$\begin{pmatrix} 1&0&1&1&0&1&1&0&1 \\ 1&1&0&1&1&0&1&1&0 \\ 0&1&1&0&1&1&0&1&1 \end{pmatrix} \xrightarrow{R_2 \to R_2 + R_1} \begin{pmatrix} 1&0&1&1&0&1&1&0&1 \\ 0&1&1&0&1&1&0&1&1 \\ 0&1&1&0&1&1&0&1&1 \end{pmatrix}$$

$$\xrightarrow{R_3 \to R_3 + R_2} \begin{pmatrix} 1&0&1&1&0&1&1&0&1 \\ 0&1&1&0&1&1&0&1&1 \\ 0&0&0&0&0&0&0&0&0 \end{pmatrix} = \begin{pmatrix} G \\ 0 \end{pmatrix}$$

From above, we found that the dimension of the cyclic code is 2. So the only four codewords are the three codewords in each row of the frist matrix and the zero codeword. Clearly, the minimum distance is 6. <Ω_1> is a $[9, 2, 6]$-cyclic code.

Next, we find the generator polynomial for <Ω_2> using Theorem 3.26.

$$g(x) = gcd(g^{49} - 1, g^3 + g^6) = gcd(g^3 + g^6, 1 + g^3) = 1 + g^3.$$

The dimension of the cyclic code is 6 and the minimum distance is 2. Hence, <Ω_2> is a $[9, 6, 2]$-cyclic code.

Since $\Omega_0 + \Omega_1$ is also a generating idempotent, we have the corresponding generator polynomial.

$$\begin{aligned} g(x) =& gcd(g^{49} - 1, 1 + g^1 + g^2 + g^4 + g^8 + g^7 + g^5) \\ =& gcd(1 + g^1 + g^2 + g^4 + g^8 + g^7 + g^5, g^3 + g^4 + g^6 + g^7) \\ =& gcd(g^3 + g^4 + g^6 + g^7, 1 + g + g^2) \\ =& 1 + g + g^2. \end{aligned}$$

The dimension of this code is 7 and the minimum distance is 2. <$\Omega_0 + \Omega_1$> is a $[9, 7, 2]$-cyclic code. Later, we found that <$\Omega_0 + \Omega_2$> is a $[9, 3, 3]$-cyclic code as $1 + g^3 + g^6$ divides $g^9 - 1$ completely so the generating idempotent is the generator polynomial itself.

Next, we obtained the generator polynomial for <$\Omega_1 + \Omega_2$> by the following steps:

$$\begin{aligned} g(x) =& gcd(g^{49} - 1, g^1 + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8) \\ =& gcd(g^1 + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8, 1 + g) \\ =& 1 + g. \end{aligned}$$

Clearly, the dimension of the code is $9 - 1 = 8$ while the minimum distance is 2. Hence, <$\Omega_1 + \Omega_2$> is a $[9, 8, 2]$-cyclic code.

Finally, we have <$\Omega_0 + \Omega_1 + \Omega_2$>=$\{000000000, 111111111\}$ which tells us that it is a $[9, 1, 9]$-binary cyclic code.

4-2-2 Construction of $[25, k, d]$-Cyclic Codes

Next, we consider the case $p = 5$. From Theorem 4.1, we verified that 2 is a primitive root modulo 5, so there are exactly two nonzero cyclotomic cosets modulo 25. Hence, we let $\Omega_1 = \sum_{h \in C_1} g^h \in \mathbb{F}[\mathbb{Z}_{25}]$ and $\Omega_2 = \sum_{k \in C_5} g^k \in \mathbb{F}[\mathbb{Z}_{25}]$. Then, we see that all 2-cyclotomic cosets modulo 25 are as follows:

$$\begin{aligned} &C_0 = \{0\}, C_5 = \{5, 10, 20, 15\} \text{ and} \\ &C_1 = \{1, 2, 4, 8, 16, 7, 14, 3, 6, 12, 24, 23, 21, 17, 9, 18, 11, 22, 19, 13\}. \end{aligned}$$

In term of group ring, the cyclotomic cosets of $\mathbb{F}[\mathbb{Z}_{25}]$ are

$$\begin{aligned} \Omega_0 =& g^0, \\ \Omega_1 =& g^1 + g^2 + g^4 + g^8 + g^{16} + g^7 + g^{14} + g^3 + g^6 + g^{12} + \\ & g^{24} + g^{23} + g^{21} + g^{17} + g^9 + g^{18} + g^{11} + g^{22} + g^{19} + g^{13}, \\ \Omega_2 =& g^5 + g^{10} + g^{20} + g^{15}. \end{aligned}$$

Using Theorem 3.26, we find the generator polynomial with respect to $< \Omega_0 >$ to be

$$g(x) = gcd(\Omega_0, g^{25} - 1) = gcd(1, g^{25} - 1) = 1.$$

From Theorem 3.21, this cyclic code has dimension 25. Clearly, the minimum distance here is 1 as the minimum weight of all nonzero codewords for this cyclic code is 1. Hence, we obtained a $[25, 25, 1]$-binary cyclic code.

Next, for Ω_1, we perform Gaussian elimination on the matrix formed by the generating idempotent to obtain k.

$$\begin{pmatrix}
0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1\\
1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1\\
1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1\\
1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1\\
1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0
\end{pmatrix}$$

$$\xrightarrow[R_4\to R_4+R_2]{R_3\to R_3+R_2 \atop R_5\to R_5+R_2}
\begin{pmatrix}
0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1\\
1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1\\
0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0\\
0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0\\
0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1
\end{pmatrix}$$

$$\xrightarrow[R_4\to R_4+R_5]{R_1\to R_1+R_5 \atop R_3\to R_3+R_5}
\begin{pmatrix}
0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0\\
1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1\\
0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1\\
0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1\\
0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1
\end{pmatrix}$$

$$\xrightarrow{R_1\to R_1+R_3}
\begin{pmatrix}
0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1\\
1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1\\
0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1\\
0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1\\
0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1
\end{pmatrix}$$

$$\xrightarrow{R_1\leftrightarrow R_5}
\begin{pmatrix}
0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1\\
1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1\\
0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1\\
0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1\\
0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1
\end{pmatrix}$$

$$\xrightarrow[R_5\to R_5+R_4]{R_1\leftrightarrow R_2 \atop R_5\to R_5+R_4}
\begin{pmatrix}
1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1&1&0&1&1&1\\
0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1\\
0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1&0&0&1&0&1\\
0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1&0&0&0&1&1\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0
\end{pmatrix}.$$

From the row echelon form of the matrix, the dimension is 4. Then we have $2^4 = 16$ codewords. We easily list down all the elements as follows:

$$\begin{aligned}
<\Omega_1> = \{&0000000000000000000000000, 1101111011110111101111011,\\
&1110111101111011110111101, 1111011110111101111011110,
\end{aligned}$$

$$011110111101111101111101111, 101111011110111101111011110111,$$
$$101001010010100101001010010100, 010100101001010010100101001010,$$
$$001010010100101001010010100101, 100101001010010100101001010010,$$
$$010010100101001010010100101001, 100011000110001100011000110001,$$
$$110001100011000110001100011000, 011000110001100011000110001100,$$
$$001100011000110001100011000110, 000110001100011000110001100011\}.$$

From these codewords, we can see that the minimum distance is 10. Hence, $< \Omega_1 >$ is a $[25, 4, 10]$-binary cyclic code.

Since Ω_2 is a generating idempotent, we have

$$\begin{aligned} g(x) &= gcd(g^{25} + 1, g^5 + g^{10} + g^{20} + g^{15}) \\ &= gcd(g^5 + g^{10} + g^{20} + g^{15}, g^5 + 1) \\ &= g^5 + 1. \end{aligned}$$

The corresponding cyclic code to <Ω_2> is a $[25, 20, 2]$-binary cyclic code. Similarly, $\Omega_0 + \Omega_1$ is a generating idempotent, we have the following generator polynomial.

$$\begin{aligned} g(x) =& gcd(g^{25} + 1, 1 + g^1 + g^2 + g^4 + g^8 + g^{16} + g^7 + g^{14} + g^3 + g^6 + \\ & g^{12} + g^{24} + g^{23} + g^{21} + g^{17} + g^9 + g^{18} + g^{11} + g^{22} + g^{19} + g^{13}) \\ =& gcd(1 + g^1 + g^2 + g^4 + g^8 + g^{16} + g^7 + g^{14} + g^3 + g^6 + g^{12} + \\ & g^{24} + g^{23} + g^{21} + g^{17} + g^9 + g^{18} + g^{11} + g^{22} + g^{19} + g^{13}, \\ & g^5 + g^6 + g^{10} + g^{11} + g^{15} + g^{16} + g^{20} + g^{21}) \\ =& gcd(g^5 + g^6 + g^{10} + g^{11} + g^{15} + g^{16} + g^{20} + g^{21}, 1 + g + g^2 + g^3 + g^4) \\ =& 1 + g + g^2 + g^3 + g^4. \end{aligned}$$

Clearly, the dimension is 21. Minimum distance can be difficult to find by listing all the elements as there are 2^{21} of them. However, we can observe from the generator polynomial. By adding $g^i g(x)$ and $g^{i+1} g(x)$ for any i, we still get the minimum weight of 2. For example, $g(x) + g \cdot g(x) = 1 + g^5$. Hence, <$\Omega_0 + \Omega_1$> is a $[25, 21, 2]$-binary cyclic code.

Since $\Omega_0 + \Omega_2$ is a generating idempotent, we have

$$g(x) = gcd(g^{25} + 1, 1 + g^5 + g^{10} + g^{20} + g^{15}) = 1 + g^5 + g^{10} + g^{20} + g^{15}.$$

Clearly, the dimension is 5 and we can list all the elements as follows:

$$\begin{aligned}< \Omega_0 + \Omega_2 >= \{&000000000000000000000000, 100001000010000100001000010000,\\ &010000100001000010000100001000, 001000010000100001000010000100,\\ &000100001000010000100001000010, 000010000100001000010000100001,\\ &001100011000110001100011000110, 000110001100011000110001100011,\\ &100011000110001100011000110001, 110001100011000110001100011000,\\ &011000110001100011000110001100, 010010100101001010010100101001,\\ &101001010010100101001010010100, 010100101001010010100101001010,\\ &001010010100101001010010100101, 100101001010010100101001010010,\\ &111011110111101111011101111101, 111101111011110111101111011110,\\ &011110111101111011101111011111, 101111011110111101111011110111,\\ &110111101111011110111101111011, 001110011100111001110011100111,\\ &100111001110011100111001110011, 110011100111001110011100111001,\\ &111001110011100111001110011100, 011100111001110011100111001110,\\ &010110101101011010110101101011, 101011010110101101011010110101,\\ &110101101011010110101101011010, 011010110101101011010110101101,\\ &101101011010110101101011010110, 111111111111111111111111111\}.\end{aligned}$$

Hence, <$\Omega_0 + \Omega_2$> is a $[25, 5, 5]$-binary cyclic code. Next, we have $\Omega_1 + \Omega_2$ which is also a generating idempotent, we have the following

$$\begin{aligned}g(x) =&gcd(g^{25} + 1, g^1 + g^2 + g^4 + g^8 + g^{16} + g^7 + g^{14} + g^3 + g^6 + g^{12} + g^{24} +\\ &g^{23} + g^{21} + g^{17} + g^9 + g^{18} + g^{11} + g^{22} + g^{19} + g^{13} + g^5 + g^{10} + g^{20} + g^{15})\\ =&gcd(g^1 + g^2 + g^4 + g^8 + g^{16} + g^7 + g^{14} + g^3 + g^6 + g^{12} + g^{24} + g^{23} + g^{21} +\\ &g^{17} + g^9 + g^{18} + g^{11} + g^{22} + g^{19} + g^{13} + g^5 + g^{10} + g^{20} + g^{15}, 1 + g)\\ =&1 + g.\end{aligned}$$

We see that $k = 24$. Again, listing all the elements by hand will be very tedious. However, we can observe from the generator polynomial and we see that the minimum distance is 2. Hence, <$\Omega_1 + \Omega_2$> is a $[25, 24, 2]$-binary cyclic code. Finally, we have $< \Omega_0 + \Omega_1 + \Omega_2 >= \{000000000000000000000000, 111111111111111111111111\}$ which tells us that it is a $[25, 1, 25]$-binary cyclic code.

4-2-3 Construction of [$49, k, d$]-Cyclic Codes

From Theorem 4.4, we let $\Omega_1 = \sum_{s\in C_1} g^s \in \mathbb{F}[\mathbb{Z}_{p^2}]$, $\Omega_2 = \sum_{r\in C_q} g^r \in \mathbb{F}[\mathbb{Z}_{p^2}]$, $\Omega_3 = \sum_{t\in C_p} g^t \in \mathbb{F}[\mathbb{Z}_{p^2}]$ and $\Omega_4 = \sum_{v\in C_{pq}} g^v \in \mathbb{F}[\mathbb{Z}_{p^2}]$. Consider the case $p = 7$. Then, we see that all 2-cyclotomic cosets modulo 49 are

$C_0 = \{0\}, C_1 = \{1, 2, 4, 8, 16, 32, 15, 30, 11, 22, 44, 39, 29, 9, 18, 36, 23, 46, 43, 37, 25\}$,

$C_3 = \{3, 6, 12, 24, 48, 47, 45, 41, 33, 17, 34, 19, 38, 27, 5, 10, 20, 40, 31, 13, 26\}$,

$C_7 = \{7, 14, 28\}$ and $C_{21} = \{21, 42, 35\}$.

In term of group ring, the cyclotomic cosets of $\mathbb{F}[\mathbb{Z}_{49}]$ are

$$\begin{aligned}
\Omega_0 =& g^0,\\
\Omega_1 =& g^1 + g^2 + g^4 + g^8 + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{22} + g^{44} +\\
& g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25},\\
\Omega_2 =& g^3 + g^6 + g^{12} + g^{24} + g^{48} + g^{47} + g^{45} + g^{41} + g^{33} + g^{17} + g^{34} +\\
& g^{19} + g^{38} + g^{27} + g^5 + g^{10} + g^{20} + g^{40} + g^{31} + g^{13} + g^{26},\\
\Omega_3 =& g^7 + g^{14} + g^{28} \text{ and } \Omega_4 = g^{21} + g^{42} + g^{35}.
\end{aligned}$$

We can easily verify that all these cyclotomic cosets in term of group ring are idempotent and since they generate a cyclic code, they are known as the generating idempotent. Clearly, for $\Omega_0 = 1$, we have a $[49, 49, 1]$-binary cyclic code.

Next, we have the following generator polynomial for $< \Omega_1 >$.

$$\begin{aligned}
g(x) =& gcd(g^{49} - 1, g^1 + g^2 + g^4 + g^8 + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{22} +\\
& g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25})\\
=& gcd(g^1 + g^2 + g^4 + g^8 + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{22} + g^{44} + g^{39} +\\
& g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25}, 1 + g + g^3 + g^7 +\\
& g^8 + g^{10} + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24} + g^{28} + g^{29} + g^{31} +\\
& g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45})\\
=& gcd(1 + g + g^3 + g^7 + g^8 + g^{10} + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24} + g^{28} +\\
& g^{29} + g^{31} + g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45}, 0)\\
=& 1 + g + g^3 + g^7 + g^8 + g^{10} + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24} + g^{28} +\\
& g^{29} + g^{31} + g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45}.
\end{aligned}$$

From above, we see that $k = 4$ and we have 16 codewords as follows:

$< \Omega_1 >=$

$\{0000000000000000000000000000000000000000000000000, 1111111111111111111111111111111111111111111111111,$

$1101000110100011010001101000110100011010001101000, 0110100011010001101000110100011010001101000110100,$

$0011010001101000110100011010001101000110100011010, 0001101000110100011010001101000110100011010001101,$

$1000110100011010001101000110100011010001101000110, 0100011010001101000110100011010001101000110100011,$

$1010001101000110100011010001101000110100011010001, 0101110010111001011100101110010111001011100101110,$

$0010111001011100101110010111001011100101110010111, 1001011100101110010111001011100101110010111001011,$

$1100101110010111001011100101110010111001011100101, 1110010111001011100101110010111001011100101110010,$

$0111001011100101110010111001011100101110010111001, 1011100101110010111001011100101110010111001011100\}.$

From above, we found that the minimum distance is 21. Hence, we obtained a $[49, 4, 21]$-binary cyclic code.

The generator matrix based on the generating idempotent Ω_2 is as follows and we performed Gaussian Elimination on it.

$$\begin{pmatrix}
1000101100010110001011000101100010110001011000101\\
1100010110001011000101100010110001011000101100010\\
0110001011000101100010110001011000101100010110001\\
1011000101100010110001011000101100010110001011000\\
0101100010110001011000101100010110001011000101100\\
0010110001011000101100010110001011000101100010110\\
0001011000101100010110001011000101100010110001011
\end{pmatrix}$$

$$\xrightarrow[R_3 \to R_3 + R_1]{R_2 \to R_2 + R_1}
\begin{pmatrix}
1000101100010110001011000101100010110001011000101\\
0100111010011101001110100111010011101001110100111\\
0110001011000101100010110001011000101100010110001\\
0011101001110100111010011101001110100111010011101\\
0101100010110001011000101100010110001011000101100\\
0010110001011000101100010110001011000101100010110\\
0001011000101100010110001011000101100010110001011
\end{pmatrix}$$

$$\xrightarrow[R_5 \to R_5 + R_2]{R_3 \to R_3 + R_2}
\begin{pmatrix}
1000101100010110001011000101100010110001011000101\\
0100111010011101001110100111010011101001110100111\\
0010110001011000101100010110001011000101100010110\\
0011101001110100111010011101001110100111010011101\\
0001011000101100010110001011000101100010110001011\\
0010110001011000101100010110001011000101100010110\\
0001011000101100010110001011000101100010110001011
\end{pmatrix}$$

$$\xrightarrow[R_7 \to R_7 + R_5]{R_4 \to R_4 + R_3 \\ R_6 \to R_6 + R_3}
\begin{pmatrix}
1000101100010110001011000101100010110001011000101\\
0100111010011101001110100111010011101001110100111\\
0010110001011000101100010110001011000101100010110\\
0001011000101100010110001011000101100010110001011\\
0001011000101100010110001011000101100010110001011\\
0000000000000000000000000000000000000000000000000\\
0000000000000000000000000000000000000000000000000
\end{pmatrix}$$

$$\xrightarrow{R_5 \to R_5 + R_4}
\begin{pmatrix}
1000101100010110001011000101100010110001011000101\\
0100111010011101001110100111010011101001110100111\\
0010110001011000101100010110001011000101100010110\\
0001011000101100010110001011000101100010110001011\\
0000000000000000000000000000000000000000000000000\\
0000000000000000000000000000000000000000000000000\\
0000000000000000000000000000000000000000000000000
\end{pmatrix}$$

$$= \begin{pmatrix} G_2 \\ 0 \end{pmatrix}.$$

Once again, the dimension is 4 so there are 16 codewords. If we perform cyclic shift on the first two rows, we will get 14 different codewords. Then we include 0 and 1, we will have exactly 16 codewords. Hence, from the matrix G_2, $d = 21$. Again, we obtained a $[49, 4, 21]$-binary cyclic code.

The generator polynomial for <Ω_3> using Theorem 3.26 is as follows:

$$\begin{aligned} g(x) =& gcd(g^{49} - 1, g^7 + g^{14} + g^{28}) \\ =& gcd(g^7 + g^{14} + g^{28}, 1 + g^7 + g^{21}) \\ =& gcd(1 + g^7 + g^{21}, 0) \\ =& 1 + g^7 + g^{21}. \end{aligned}$$

Based on $g(x)$, the Hamming distance is at least 3. So, we have a $[49, 28, 3]$-binary cyclic code.

The generator polynomial for <Ω_4> using Theorem 3.26 is as follows:

$$\begin{aligned} g(x) =& gcd(g^{49} - 1, g^{21} + g^{35} + g^{42}) \\ =& gcd(g^{21} + g^{35} + g^{42}, 1 + g^{21} + g^{28} + g^{35}) \\ =& gcd(1 + g^{21} + g^{28} + g^{35}, g^7 + g^{21} + g^{28}) \\ =& gcd(g^7 + g^{21} + g^{28}, 1 + g^{14} + g^{21}) \\ =& 1 + g^{14} + g^{21}. \end{aligned}$$

Based on $g(x)$, the minimum distance is 3. So, we have a $[49, 28, 3]$-binary cyclic code.

The generator polynomial for <$\Omega_0 + \Omega_1$> using Theorem 3.26 is as follows:

$$\begin{aligned} g(x) =& gcd(g^{49} - 1, 1 + g^1 + g^2 + g^4 + g^8 + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{22} + \\ & g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25}) \\ =& gcd(1 + g^1 + g^2 + g^4 + g^8 + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{22} + g^{44} + g^{39} + \\ & g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25}, g^7 + g^8 + g^{10} + g^{14} + g^{15} + \\ & g^{17} + g^{21} + g^{22} + g^{24} + g^{28} + g^{29} + g^{31} + g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45}) \\ =& gcd(g^7 + g^8 + g^{10} + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24} + g^{28} + g^{29} + \\ & g^{31} + g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45}, 1 + g + g^2 + g^4) \\ =& 1 + g + g^2 + g^4. \end{aligned}$$

Based on $g(x)$, the dimension is 45 while the minimum distance is 4. Hence, we have a $[49, 45, 4]$-binary cyclic code.

The generator polynomial for <$\Omega_0 + \Omega_2$> using Theorem 3.26 is as follows:

$$\begin{aligned}
g(x) =& gcd(g^{49}-1, 1+g^3+g^6+g^{12}+g^{24}+g^{48}+g^{47}+g^{45}+g^{41}+g^{33}+g^{17}+\\
& g^{34}+g^{19}+g^{38}+g^{27}+g^5+g^{10}+g^{20}+g^{40}+g^{31}+g^{13}+g^{26})\\
=& gcd(1+g^3+g^6+g^{12}+g^{24}+g^{48}+g^{47}+g^{45}+g^{41}+g^{33}+g^{17}+g^{34}+g^{19}+\\
& g^{38}+g^{27}+g^5+g^{10}+g^{20}+g^{40}+g^{31}+g^{13}+g^{26}, g+g^3+g^4+g^5+g^7+\\
& g^{10}+g^{11}+g^{12}+g^{14}+g^{17}+g^{18}+g^{19}+g^{21}+g^{24}+g^{25}+g^{26}+g^{28}+g^{31}+\\
& g^{32}+g^{33}+g^{35}+g^{38}+g^{39}+g^{40}+g^{42}+g^{45}+g^{46}+g^{47})\\
=& gcd(g+g^3+g^4+g^5+g^7+g^{10}+g^{11}+g^{12}+g^{14}+g^{17}+g^{18}+g^{19}+g^{21}+\\
& g^{24}+g^{25}+g^{26}+g^{28}+g^{31}+g^{32}+g^{33}+g^{35}+g^{38}+g^{39}+g^{40}+g^{42}+g^{45}+\\
& g^{46}+g^{47}, 1+g^2+g^3+g^4+g^8+g^{10}+g^{11}+g^{15}+g^{17}+g^{18}+g^{22}+g^{24}+\\
& g^{25}+g^{29}+g^{31}+g^{32}+g^{36}+g^{38}+g^{39}+g^{43}+g^{45}+g^{46})\\
=& gcd(1+g^2+g^3+g^4+g^8+g^{10}+g^{11}+g^{15}+g^{17}+g^{18}+g^{22}+g^{24}+g^{25}+\\
& g^{29}+g^{31}+g^{32}+g^{36}+g^{38}+g^{39}+g^{43}+g^{45}+g^{46}, g^7+g^9+g^{10}+g^{14}+g^{16}+\\
& g^{17}+g^{21}+g^{23}+g^{24}+g^{28}+g^{30}+g^{31}+g^{35}+g^{37}+g^{38}+g^{42}+g^{44}+g^{45})\\
=& gcd(g^7+g^9+g^{10}+g^{14}+g^{16}+g^{17}+g^{21}+g^{23}+g^{24}+g^{28}+g^{30}+g^{31}+\\
& g^{35}+g^{37}+g^{38}+g^{42}+g^{44}+g^{45}, 1+g^2+g^3+g^4)\\
=& 1+g^2+g^3+g^4.
\end{aligned}$$

Based on the generator polynomial, the cyclic code has a dimension of 45 and Hamming distance at least 4. So, $< \Omega_0 + \Omega_2 >$ is a $[49, 45, 4]$-binary cyclic code.

$\Omega_0 + \Omega_3 = 1 + g^7 + g^{14} + g^{28}$ divides $g^{49} - 1$ completely. So, the dimension is 21 and $d = 4$. Hence, <$\Omega_0 + \Omega_3$> is a $[49, 21, 4]$-binary cyclic code.

Next, the generator polynomial for <$\Omega_0 + \Omega_4$> is

$$\begin{aligned}
g(x) =& gcd(g^{49}-1, 1+g^{21}+g^{35}+g^{42})\\
=& gcd(1+g^{21}+g^{35}+g^{42}, g^7+g^{21}+g^{28}+g^{35})\\
=& gcd(g^7+g^{21}+g^{28}+g^{35}, 1+g^{14}+g^{21}+g^{28})\\
=& 1+g^{14}+g^{21}+g^{28}.
\end{aligned}$$

Similarly, we obtained a $[49, 21, 4]$-binary cyclic code.

Next, the generator polynomial for $<\Omega_1 + \Omega_2>$ is as follows:

$$
\begin{aligned}
& g(x) \\
=& gcd(g^{49}-1, g^1+g^2+g^4+g^8+g^{16}+g^{32}+g^{15}+g^{30}+g^{11}+g^{22}+g^{44}+ \\
& +g^{39}+g^{29}+g^9+g^{18}+g^{36}+g^{23}+g^{46}+g^{43}+g^{37}+g^{25}+g^3+g^5+g^6+ \\
& g^{10}+g^{12}+g^{13}+g^{17}+g^{19}+g^{20}+g^{24}+g^{26}+g^{27}+g^{31}+g^{33}+g^{34}+ \\
& g^{38}+g^{40}+g^{41}+g^{45}+g^{47}+g^{48}) \\
=& gcd(g^1+g^2+g^3+g^4+g^5+g^6+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{15}+g^{16}+ \\
& g^{17}+g^{18}+g^{19}+g^{20}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27}+g^{29}+g^{30}+g^{31}+g^{32} \\
& +g^{33}+g^{34}+g^{36}+g^{37}+g^{38}+g^{39}+g^{40}+g^{41}+g^{43}+g^{44}+g^{45}+g^{46}+g^{47}+ \\
& g^{48}, 1+g+g^7+g^8+g^{14}+g^{15}+g^{21}+g^{22}+g^{28}+g^{29}+g^{35}+g^{36}+g^{42}+g^{43}) \\
=& gcd(1+g+g^7+g^8+g^{14}+g^{15}+g^{21}+g^{22}+g^{28}+g^{29}+g^{35}+g^{36}+g^{42}+g^{43}, 0) \\
=& 1+g+g^7+g^8+g^{14}+g^{15}+g^{21}+g^{22}+g^{28}+g^{29}+g^{35}+g^{36}+g^{42}+g^{43}.
\end{aligned}
$$

The dimension of the code is 6 so there are 2^6 codewords in this cyclic code. The following are all 64 codewords.

$< \Omega_1 + \Omega_2 >$

$=\{0000000000000000000000000000000000000000000000000000, 1100000110000011000001100000110000011000001100000,$
$0110000011000001100000110000011000001100000110000, 0011000001100000110000011000001100000110000011000,$
$0001100000110000011000001100000110000011000001100, 0000110000011000001100000110000011000001100000110,$
$0000011000001100000110000011000001100000110000011, 1000001100000110000011000001100000110000011000001,$
$0010100001010000101000010100001010000101000010100, 0001010000101000010100001010000101000010100001010,$
$0000101000010100001010000101000010100001010000101, 1000010100001010000101000010100001010000101000010,$
$0100001010000101000010100001010000101000010100001, 1010000101000010100001010000101000010100001010000,$
$0101000010100001010000101000010100001010000101000, 0100010010001001000100100010010001001000100100010,$
$0010001001000100100010010001001000100100010010001, 1001000100100010010001001000100100010010001001000,$
$0100100010010001001000100100010010001001000100100, 0010010001001000100100010010001001000100100010010,$
$0001001000100100010010001001000100100010010001001, 1000100100010010001001000100100010010001001000100,$
$1110010111001011100101110010111001011100101110010, 0111001011100101110010111001011100101110010111001,$
$1011100101110010111001011100101110010111001011100, 0101110010111001011100101110010111001011100101110,$
$0010111001011100101110010111001011100101110010111, 1001011100101110010111001011100101110010111001011,$
$1100101110010111001011100101110010111001011100101, 1110100111010011101001110100111010011101001110100,$
$0111010011101001110100111010011101001110100111010, 0011101001110100111010011101001110100111010011101,$
$1001110100111010011101001110100111010011101001110, 0100111010011101001110100111010011101001110100111,$
$1010011101001110100111010011101001110100111010011, 1101001110100111010011101001110100111010011101001,$
$0011110001111000111100011110001111000111100011110, 0001111000111100011110001111000111100011110001111,$
$1000111100011110001111000111100011110001111000111, 1100011110001111000111100011110001111000111100011,$

11100011110001111000111100011110001111000111100011110001, 11110001111000111100011110001111000111100011110001111000,
01111000111100011110001111000111100011110001111000111100, 11011001101100110110011011001101100110110011011001101100,
01101100110110011011001101100110110011011001101100110110, 00110110011011001101100110110011011001101100110110011011,
10011011001101100110110011011001101100110110011011001101, 11001101100110110011011001101100110110011011001101100110,
01100110110011011001101100110110011011001101100110110011, 10110011011001101100110110011011001101100110110011011001,
10101101010110101011010101101010110101011010101101010110, 01010110101011010110101101010110101011010101101010110101011,
10101011010101101010110101011010101101010110101011010101, 11010101101010110101011010101101010110101011010101101010,
01101010110101011010101101010110101011010101101010110101, 10110101011010101101010110101011010101101010110101011010,
01011010101101010110101011010101101010110101011010101101, 11111011111101111101111101111101111101111101111101111101,
11111101111110111111011111101111110111111011111101111110, 01111110111111011111101111110111111011111101111110111111,
10111111011111101111110111111011111101111110111111011111, 11011111101111110111111011111101111110111111011111101111,
11101111110111111011111101111110111111011111101111110111, 11110111111011111101111110111111011111101111110111111011}.

Based on the list of elements above, the minimum distance is 14. $<\Omega_1 + \Omega_2>$ is a $[49, 6, 14]$-binary cyclic code.

We constructed the generator polynomial for $<\Omega_1 + \Omega_3>$ as follows:

$$\begin{aligned}
g(x) =& gcd(g^{49} - 1, g^1 + g^2 + g^4 + g^7 + g^8 + g^{14} + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + \\
& g^{22} + g^{28} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25}) \\
=& gcd(g^1 + g^2 + g^4 + g^7 + g^8 + g^{14} + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{22} + \\
& g^{28} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25}, \\
& 1 + g + g^3 + g^{21} + g^{22} + g^{24} + g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45}) \\
=& gcd(1 + g + g^3 + g^{21} + g^{22} + g^{24} + g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45}, \\
& g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{15} + g^{16} + g^{18} + g^{28} + g^{29} + g^{30} + g^{32}) \\
=& gcd(g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{15} + g^{16} + g^{18} + g^{28} + g^{29} + g^{30} + g^{32}, \\
& 1 + g + g^3 + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24} + g^{28} + g^{29} + g^{31}) \\
=& gcd(1 + g + g^3 + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24} + g^{28} + g^{29} + g^{31}, \\
& g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{22} + g^{23} + g^{25} + g^{28}) \\
=& gcd(g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{22} + g^{23} + g^{25} + g^{28}, \\
& 1 + g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{21} + g^{22} + g^{23} + g^{25}) \\
=& gcd(1 + g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{21} + g^{22} + g^{23} + g^{25}, 0) \\
=& 1 + g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{21} + g^{22} + g^{23} + g^{25}.
\end{aligned}$$

From the degree of the generator polynomial, the dimension is 24 and the Hamming distance should be at least 12. $<\Omega_1 + \Omega_3>$ is a $[49, 24, 12]$-binary cyclic code.

Next, the <$\Omega_1 + \Omega_4$> has the following generator polynomial:

$$\begin{aligned}
g(x) =& gcd(g^{49}-1, g^1+g^2+g^4+g^8+g^{16}+g^{32}+g^{15}+g^{30}+g^{11}+g^{21}+g^{22}+\\
& g^{35}+g^{42}+g^{44}+g^{39}+g^{29}+g^9+g^{18}+g^{36}+g^{23}+g^{46}+g^{43}+g^{37}+g^{25})\\
=& gcd(g^1+g^2+g^4+g^8+g^{16}+g^{32}+g^{15}+g^{30}+g^{11}+g^{21}+g^{22}+g^{35}+\\
& g^{42}+g^{44}+g^{39}+g^{29}+g^9+g^{18}+g^{36}+g^{23}+g^{46}+g^{43}+g^{37}+g^{25},\\
& 1+g+g^3+g^7+g^8+g^{10}+g^{14}+g^{15}+g^{17}+g^{28}+g^{29}+g^{31})\\
=& gcd(1+g+g^3+g^7+g^8+g^{10}+g^{14}+g^{15}+g^{17}+g^{28}+g^{29}+g^{31},\\
& g+g^2+g^4+g^7+g^{15}+g^{16}+g^{18}+g^{21}+g^{22}+g^{23}+g^{25}+g^{28})\\
=& gcd(g+g^2+g^4+g^7+g^{15}+g^{16}+g^{18}+g^{21}+g^{22}+g^{23}+g^{25}+g^{28},\\
& 1+g+g^2+g^4+g^{14}+g^{15}+g^{16}+g^{18}+g^{21}+g^{22}+g^{23}+g^{25})\\
=& gcd(1+g+g^2+g^4+g^{14}+g^{15}+g^{16}+g^{18}+g^{21}+g^{22}+g^{23}+g^{25}, 0)\\
=& 1+g+g^2+g^4+g^{14}+g^{15}+g^{16}+g^{18}+g^{21}+g^{22}+g^{23}+g^{25}.
\end{aligned}$$

From the degree of the generator polynomial, the dimension is 24 and the Hamming distance should be at least 12. <$\Omega_1 + \Omega_4$> is a $[49, 24, 12]$-binary cyclic code.

Next, we have $\Omega_3 + \Omega_4 = g^7 + g^{14} + g^{21} + g^{28} + g^{35} + g^{42}$. We constructed the generator polynomial as follows:

$$\begin{aligned}
g(x) &= gcd(g^{49}-1, g^7+g^{14}+g^{21}+g^{28}+g^{35}+g^{42})\\
&= gcd(g^7+g^{14}+g^{21}+g^{28}+g^{35}+g^{42}, 1+g^7)\\
&= gcd(1+g^7, 0)\\
&= 1+g^7.
\end{aligned}$$

Clearly,<$\Omega_3 + \Omega_4$> is a $[49, 42, 2]$-binary cyclic code.

By adding Ω_0 to the previous generating idempotent, we have $1 + g^7 + g^{14} + g^{21} + g^{28} + g^{35} + g^{42}$ which is a factor of $g^{49} - 1$ as we found that

$$(1+g^7+g^{14}+g^{21}+g^{28}+g^{35}+g^{42})(1+g^4) = g^{49}-1.$$

Hence, <$\Omega_0 + \Omega_3 + \Omega_4$> is a $[49, 7, 7]$-binary cyclic code.

We found that $< \Omega_2 + \Omega_4 >$ is a $[49, 24, 12]$-binary cyclic code based on the

generator polynomial with degree 25 and weight 12 found below.

$$
\begin{aligned}
g(x) =& gcd(g^{49}-1, g^3+g^5+g^6+g^{10}+g^{12}+g^{13}+g^{17}+g^{19}+g^{20}+g^{21}+g^{24}+ \\
& g^{26}+g^{27}+g^{31}+g^{33}+g^{34}+g^{35}+g^{38}+g^{40}+g^{41}+g^{42}+g^{45}+g^{47}+g^{48}) \\
=& gcd(g^3+g^5+g^6+g^{10}+g^{12}+g^{13}+g^{17}+g^{19}+g^{20}+g^{21}+g^{24}+g^{26}+ \\
& g^{27}+g^{31}+g^{33}+g^{34}+g^{35}+g^{38}+g^{40}+g^{41}+g^{42}+g^{45}+g^{47}+g^{48}, 1+g^3 \\
& +g^4+g^5+g^7+g^{10}+g^{11}+g^{12}+g^{14}+g^{17}+g^{18}+g^{19}+g^{22}+g^{24}+g^{25}+ \\
& g^{26}+g^{28}+g^{31}+g^{32}+g^{33}+g^{36}+g^{38}+g^{39}+g^{40}+g^{43}+g^{45}+g^{46}+g^{47}) \\
=& gcd(1+g^3+g^4+g^5+g^7+g^{10}+g^{11}+g^{12}+g^{14}+g^{17}+g^{18}+g^{19}+g^{22}+ \\
& g^{24}+g^{25}+g^{26}+g^{28}+g^{31}+g^{32}+g^{33}+g^{36}+g^{38}+g^{39}+g^{40}+g^{43}+g^{45}+ \\
& g^{46}+g^{47}, g+g^3+g^4+g^8+g^{10}+g^{11}+g^{15}+g^{17}+g^{18}+g^{21}+g^{23}+g^{24}+ \\
& g^{25}+g^{29}+g^{31}+g^{32}+g^{35}+g^{37}+g^{38}+g^{39}+g^{42}+g^{44}+g^{45}+g^{46}) \\
=& gcd(g+g^3+g^4+g^8+g^{10}+g^{11}+g^{15}+g^{17}+g^{18}+g^{21}+g^{23}+g^{24}+g^{25}+ \\
& g^{29}+g^{31}+g^{32}+g^{35}+g^{37}+g^{38}+g^{39}+g^{42}+g^{44}+g^{45}+g^{46}, \\
& 1+g^2+g^3+g^7+g^9+g^{10}+g^{14}+g^{16}+g^{17}+g^{28}+g^{30}+g^{31}) \\
=& gcd(1+g^2+g^3+g^7+g^9+g^{10}+g^{14}+g^{16}+g^{17}+g^{28}+g^{30}+g^{31}, g+g^3+ \\
& g^4+g^7+g^8+g^9+g^{15}+g^{17}+g^{18}+g^{21}+g^{23}+g^{24}+g^{25}+g^{28}+g^{29}+g^{30}) \\
=& gcd(g+g^3+g^4+g^7+g^8+g^9+g^{15}+g^{17}+g^{18}+g^{21}+g^{23}+g^{24}+g^{25}+ \\
& g^{28}+g^{29}+g^{30}, 1+g^3+g^4+g^5+g^7+g^8+g^{14}+g^{17}+g^{18}+g^{19}+g^{22}+ \\
& g^{24}+g^{25}+g^{26}+g^{28}+g^{29}) \\
=& gcd(1+g^3+g^4+g^5+g^7+g^8+g^{14}+g^{17}+g^{18}+g^{19}+g^{22}+g^{24}+g^{25}+g^{26} \\
& +g^{28}+g^{29}, g^3+g^5+g^6+g^7+g^{17}+g^{19}+g^{20}+g^{21}+g^{24}+g^{26}+g^{27}+g^{28}) \\
=& gcd(g^3+g^5+g^6+g^7+g^{17}+g^{19}+g^{20}+g^{21}+g^{24}+g^{26}+g^{27}+g^{28}, \\
& 1+g^3+g^5+g^6+g^{14}+g^{17}+g^{19}+g^{20}+g^{21}+g^{24}+g^{26}+g^{27}) \\
=& gcd(1+g^3+g^5+g^6+g^{14}+g^{17}+g^{19}+g^{20}+g^{21}+g^{24}+g^{26}+g^{27}, \\
& g+g^3+g^4+g^5+g^{15}+g^{17}+g^{18}+g^{19}+g^{22}+g^{24}+g^{25}+g^{26}) \\
=& gcd(g+g^3+g^4+g^5+g^{15}+g^{17}+g^{18}+g^{19}+g^{22}+g^{24}+g^{25}+g^{26}, \\
& 1+g^2+g^3+g^4+g^{14}+g^{16}+g^{17}+g^{18}+g^{21}+g^{23}+g^{24}+g^{25}) \\
=& gcd(1+g^2+g^3+g^4+g^{14}+g^{16}+g^{17}+g^{18}+g^{21}+g^{23}+g^{24}+g^{25}, 0) \\
=& 1+g^2+g^3+g^4+g^{14}+g^{16}+g^{17}+g^{18}+g^{21}+g^{23}+g^{24}+g^{25}.
\end{aligned}
$$

Next, we constructed the generator polynomial based on the two generating idempotent $\Omega_2 + \Omega_3$ and the result is as follows:

$$
\begin{aligned}
g(x) =& gcd(g^{49} - 1, g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} + \\
& g^{24} + g^{26} + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} + g^{38} + g^{40} + g^{41} + g^{45} + g^{47} + g^{48}) \\
=& gcd(g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} + g^{24} + g^{26} \\
& + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} + g^{38} + g^{40} + g^{41} + g^{45} + g^{47} + g^{48}, 1 + g^3 + \\
& g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{15} + g^{17} + g^{18} + g^{19} + g^{21} + g^{24} + g^{25} + \\
& g^{26} + g^{29} + g^{31} + g^{32} + g^{33} + g^{35} + g^{38} + g^{39} + g^{40} + g^{42} + g^{45} + g^{46} + g^{47}) \\
=& gcd(1 + g^3 + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{15} + g^{17} + g^{18} + g^{19} + g^{21} + \\
& g^{24} + g^{25} + g^{26} + g^{29} + g^{31} + g^{32} + g^{33} + g^{35} + g^{38} + g^{39} + g^{40} + g^{42} + g^{45} + \\
& g^{46} + g^{47}, g + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{22} + \\
& g^{24} + g^{25} + g^{28} + g^{30} + g^{31} + g^{32} + g^{36} + g^{38} + g^{39} + g^{43} + g^{45} + g^{46}) \\
=& gcd(g + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{22} + g^{24} \\
& + g^{25} + g^{28} + g^{30} + g^{31} + g^{32} + g^{36} + g^{38} + g^{39} + g^{43} + g^{45} + g^{46}, 1 + g^2 + \\
& g^3 + g^{21} + g^{23} + g^{24} + g^{35} + g^{37} + g^{38} + g^{42} + g^{44} + g^{45}) \\
=& gcd(1 + g^2 + g^3 + g^{21} + g^{23} + g^{24} + g^{35} + g^{37} + g^{38} + g^{42} + g^{44} + g^{45}, \\
& g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{28} + g^{30} + g^{31} + g^{32}) \\
=& gcd(g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{28} + g^{30} + g^{31} + g^{32}, \\
& 1 + g^2 + g^3 + g^{14} + g^{16} + g^{17} + g^{21} + g^{23} + g^{24} + g^{28} + g^{30} + g^{31}) \\
=& gcd(1 + g^2 + g^3 + g^{14} + g^{16} + g^{17} + g^{21} + g^{23} + g^{24} + g^{28} + g^{30} + g^{31}, \\
& g + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{15} + g^{16} + g^{22} + g^{24} + g^{25} + \\
& g^{28} + g^{29} + g^{30}) \\
=& gcd(g + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{15} + g^{16} + g^{22} + g^{24} + g^{25} + \\
& g^{28} + g^{29} + g^{30}, 1 + g^3 + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{14} + g^{15} + g^{21} + \\
& g^{24} + g^{25} + g^{26} + g^{28} + g^{29}) \\
=& gcd(1 + g^3 + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{14} + g^{15} + g^{21} + g^{24} + \\
& g^{25} + g^{26} + g^{28} + g^{29}, g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{24} + \\
& g^{26} + g^{27} + g^{28})
\end{aligned}
$$

$$
\begin{aligned}
&=gcd(g^3+g^5+g^6+g^7+g^{10}+g^{12}+g^{13}+g^{14}+g^{24}+g^{26}+g^{27}+g^{28},\\
&\quad 1+g^3+g^5+g^6+g^7+g^{10}+g^{12}+g^{13}+g^{21}+g^{24}+g^{26}+g^{27})\\
&=gcd(1+g^3+g^5+g^6+g^7+g^{10}+g^{12}+g^{13}+g^{21}+g^{24}+g^{26}+g^{27},\\
&\quad g+g^3+g^4+g^5+g^8+g^{10}+g^{11}+g^{12}+g^{22}+g^{24}+g^{25}+g^{26})\\
&=gcd(g+g^3+g^4+g^5+g^8+g^{10}+g^{11}+g^{12}+g^{22}+g^{24}+g^{25}+g^{26},\\
&\quad 1+g^2+g^3+g^4+g^7+g^9+g^{10}+g^{11}+g^{21}+g^{23}+g^{24}+g^{25})\\
&=gcd(1+g^2+g^3+g^4+g^7+g^9+g^{10}+g^{11}+g^{21}+g^{23}+g^{24}+g^{25},0)\\
&=1+g^2+g^3+g^4+g^7+g^9+g^{10}+g^{11}+g^{21}+g^{23}+g^{24}+g^{25}.
\end{aligned}
$$

From the $g(x)$, the dimension of the cyclic code is 24 and the minimum distance is 12. Hence, $<\Omega_2+\Omega_3>$ is a $[49,24,12]$-binary cyclic code.

For <$\Omega_0+\Omega_1+\Omega_2$>, the generator polynomial is as follows:

$$
\begin{aligned}
&g(x)\\
&=gcd(g^{49}-1,1+g^1+g^2+g^4+g^8+g^{16}+g^{32}+g^{15}+g^{30}+g^{11}+g^{22}+g^{44}+\\
&\quad +g^{39}+g^{29}+g^9+g^{18}+g^{36}+g^{23}+g^{46}+g^{43}+g^{37}+g^{25}+g^3+g^5+g^6+\\
&\quad g^{10}+g^{12}+g^{13}+g^{17}+g^{19}+g^{20}+g^{24}+g^{26}+g^{27}+g^{31}+g^{33}+g^{34}+g^{38}+\\
&\quad g^{40}+g^{41}+g^{45}+g^{47}+g^{48})\\
&=gcd(1+g^1+g^2+g^3+g^4+g^5+g^6+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{15}+\\
&\quad g^{16}+g^{17}+g^{18}+g^{19}+g^{20}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27}+g^{29}+g^{30}+g^{31}\\
&\quad +g^{32}+g^{33}+g^{34}+g^{36}+g^{37}+g^{38}+g^{39}+g^{40}+g^{41}+g^{43}+g^{44}+g^{45}+g^{46}+\\
&\quad g^{47}+g^{48},g^7+g^8+g^{14}+g^{15}+g^{21}+g^{22}+g^{28}+g^{29}+g^{35}+g^{36}+g^{42}+g^{43})\\
&=gcd(g^7+g^8+g^{14}+g^{15}+g^{21}+g^{22}+g^{28}+g^{29}+g^{35}+g^{36}+g^{42}+g^{43},\\
&\quad 1+g+g^2+g^3+g^4+g^5+g^6)\\
&=gcd(1+g+g^2+g^3+g^4+g^5+g^6,0)\\
&=1+g+g^2+g^3+g^4+g^5+g^6.
\end{aligned}
$$

Clearly, the dimension is 43. It can be found that the minimum distance is 2. For example, we can use $g(x)+g\cdot g(x)=1+g^7$. Hence, the corresponding cyclic code is a $[49,43,2]$-cyclic code.

For <$\Omega_0 + \Omega_1 + \Omega_3$>, the generator polynomial is as follows:

$$\begin{aligned}
g(x) =& gcd(g^{49} - 1, 1 + g^1 + g^2 + g^4 + g^7 + g^8 + g^{14} + g^{16} + g^{32} + g^{15} + \\
& g^{30} + g^{11} + g^{22} + g^{28} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + \\
& g^{46} + g^{43} + g^{37} + g^{25}) \\
=& gcd(1 + g^1 + g^2 + g^4 + g^7 + g^8 + g^{14} + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + \\
& g^{22} + g^{28} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + \\
& g^{25}, g^{21} + g^{22} + g^{24} + g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45}) \\
=& gcd(g^{21} + g^{22} + g^{24} + g^{35} + g^{36} + g^{38} + g^{42} + g^{43} + g^{45}, 1 + g + g^2 + g^4 \\
& + g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{15} + g^{16} + g^{18} + g^{28} + g^{29} + g^{30} + g^{32}) \\
=& gcd(1 + g + g^2 + g^4 + g^7 + g^8 + g^9 + g^{11} + g^{14} + g^{15} + g^{16} + g^{18} + g^{28} \\
& + g^{29} + g^{30} + g^{32}, g^7 + g^8 + g^{10} + g^{21} + g^{22} + g^{24} + g^{28} + g^{29} + g^{31}) \\
=& gcd(g^7 + g^8 + g^{10} + g^{21} + g^{22} + g^{24} + g^{28} + g^{29} + g^{31}, 1 + g + g^2 + \\
& g^4 + g^7 + g^{14} + g^{15} + g^{16} + g^{18} + g^{22} + g^{23} + g^{25} + g^{28}) \\
=& gcd(1 + g + g^2 + g^4 + g^7 + g^{14} + g^{15} + g^{16} + g^{18} + g^{22} + g^{23} + g^{25} + g^{28}, \\
& g + g^2 + g^4 + g^{15} + g^{16} + g^{18} + g^{22} + g^{23} + g^{25}) \\
=& gcd(g + g^2 + g^4 + g^{15} + g^{16} + g^{18} + g^{22} + g^{23} + g^{25}, \\
& 1 + g + g^3 + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24}) \\
=& gcd(1 + g + g^3 + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24}, 0) \\
=& 1 + g + g^3 + g^{14} + g^{15} + g^{17} + g^{21} + g^{22} + g^{24}.
\end{aligned}$$

Clearly, the dimension is 25. The Hamming distance is at least 9 by looking at the generator polynomial. Hence, <$\Omega_0 + \Omega_1 + \Omega_3$> is $[49, 25, 9]$-cyclic code.

Most of the calculations were done by hand but it became harder to perform polynomial division as the number of elements increased, so we used a Matlab code to help us calculate the remainder for the division of two polynomials as follows:

```
[q,r]=gfdeconv(g,u,2)
```

`g` is the numerator while `u` is the denominator, the third parameter is the division over which finite field. By default, it is 2(binary). Then, it will produce two result :quotient and remainder. Since we just need the remainder, we just display the remainder. Ba-

sically, to get the results for all idempotent in one run, we loop the function multiple times using a for loop.

For <$\Omega_0 + \Omega_1 + \Omega_4$>, the generator polynomial is as follows:

$$
\begin{aligned}
& g(x) \\
=& gcd(g^{49} - 1, 1 + g^1 + g^2 + g^4 + g^8 + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{21} + g^{22} + \\
& g^{35} + g^{42} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25}) \\
=& gcd(1 + g^1 + g^2 + g^4 + g^8 + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{21} + g^{22} + g^{35} + \\
& g^{42} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25}, \\
& g^7 + g^8 + g^{10} + g^{14} + g^{15} + g^{17} + g^{28} + g^{29} + g^{31}) \\
=& gcd(g^7 + g^8 + g^{10} + g^{14} + g^{15} + g^{17} + g^{28} + g^{29} + g^{31}, 1 + g + g^2 + g^4 + g^8 + \\
& g^9 + g^{11} + g^{14} + g^{21} + g^{22} + g^{23} + g^{25} + g^{28}) \\
=& gcd(1 + g + g^2 + g^4 + g^8 + g^9 + g^{11} + g^{14} + g^{21} + g^{22} + g^{23} + g^{25} + g^{28}, \\
& g + g^2 + g^4 + g^8 + g^9 + g^{11} + g^{22} + g^{23} + g^{25}) \\
=& gcd(g + g^2 + g^4 + g^8 + g^9 + g^{11} + g^{22} + g^{23} + g^{25}, \\
& 1 + g + g^3 + g^7 + g^8 + g^{10} + g^{21} + g^{22} + g^{24}) \\
=& gcd(1 + g + g^3 + g^7 + g^8 + g^{10} + g^{21} + g^{22} + g^{24}, 0) \\
=& 1 + g + g^3 + g^7 + g^8 + g^{10} + g^{21} + g^{22} + g^{24}.
\end{aligned}
$$

The dimension of the cyclic code is $49 - 24 = 25$. From the generator polynomial, the Hamming distance should be at least 9. Hence, the code is a $[49, 25, 9]$-binary cyclic code.

Next, we found that $< \Omega_0 + \Omega_2 + \Omega_3 >$ is a $[49, 25, 9]$-binary cyclic code by constructing the generator polynomial as follows:

$$
\begin{aligned}
& g(x) \\
=& gcd(g^{49} - 1, 1 + g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} \\
& + g^{24} + g^{26} + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} + g^{38} + g^{40} + g^{41} + g^{45} + g^{47} + g^{48}) \\
=& gcd(1 + g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} + g^{24} + \\
& g^{26} + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} + g^{38} + g^{40} + g^{41} + g^{45} + g^{47} + g^{48}, g + g^3 \\
& + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{15} + g^{17} + g^{18} + g^{19} + g^{21} + g^{24} + g^{25} + \\
& g^{26} + g^{29} + g^{31} + g^{32} + g^{33} + g^{35} + g^{38} + g^{39} + g^{40} + g^{42} + g^{45} + g^{46} + g^{47})
\end{aligned}
$$

$$
\begin{aligned}
&= gcd(g + g^3 + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{15} + g^{17} + g^{18} + g^{19} + g^{21} + \\
&\quad g^{24} + g^{25} + g^{26} + g^{29} + g^{31} + g^{32} + g^{33} + g^{35} + g^{38} + g^{39} + g^{40} + g^{42} + g^{45} + \\
&\quad g^{46} + g^{47}, 1 + g^2 + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + \\
&\quad g^{22} + g^{24} + g^{25} + g^{28} + g^{30} + g^{31} + g^{32} + g^{36} + g^{38} + g^{39} + g^{43} + g^{45} + g^{46}) \\
&= gcd(1 + g^2 + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{22} + \\
&\quad g^{24} + g^{25} + g^{28} + g^{30} + g^{31} + g^{32} + g^{36} + g^{38} + g^{39} + g^{43} + g^{45} + g^{46}, g^{21} + \\
&\quad g^{23} + g^{24} + g^{35} + g^{37} + g^{38} + g^{42} + g^{44} + g^{45}) \\
&= gcd(g^{21} + g^{23} + g^{24} + g^{35} + g^{37} + g^{38} + g^{42} + g^{44} + g^{45}, 1 + g^2 + g^3 + g^4 + \\
&\quad g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{28} + g^{30} + g^{31} + g^{32}) \\
&= gcd(1 + g^2 + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{28} + \\
&\quad g^{30} + g^{31} + g^{32}, g^7 + g^9 + g^{10} + g^{21} + g^{23} + g^{24} + g^{28} + g^{30} + g^{31}) \\
&= gcd(g^7 + g^9 + g^{10} + g^{21} + g^{23} + g^{24} + g^{28} + g^{30} + g^{31}, 1 + g^2 + g^3 + g^4 + \\
&\quad g^7 + g^8 + g^9 + g^{14} + g^{16} + g^{17} + g^{18} + g^{22} + g^{24} + g^{25} + g^{28} + g^{29} + g^{30}) \\
&= gcd(1 + g^2 + g^3 + g^4 + g^7 + g^8 + g^9 + g^{14} + g^{16} + g^{17} + g^{18} + g^{22} + g^{24} + \\
&\quad g^{25} + g^{28} + g^{29} + g^{30}, g + g^3 + g^4 + g^5 + g^7 + g^8 + g^{15} + g^{17} + g^{18} + g^{19} + \\
&\quad g^{21} + g^{24} + g^{25} + g^{26} + g^{28} + g^{29}) \\
&= gcd(g + g^3 + g^4 + g^5 + g^7 + g^8 + g^{15} + g^{17} + g^{18} + g^{19} + g^{21} + g^{24} + g^{25} + \\
&\quad g^{26} + g^{28} + g^{29}, 1 + g^3 + g^5 + g^6 + g^7 + g^{14} + g^{17} + g^{19} + g^{20} + g^{24} + g^{26} + \\
&\quad g^{27} + g^{28}) \\
&= gcd(1 + g^3 + g^5 + g^6 + g^7 + g^{14} + g^{17} + g^{19} + g^{20} + g^{24} + g^{26} + g^{27} + g^{28}, \\
&\quad g^3 + g^5 + g^6 + g^{17} + g^{19} + g^{20} + g^{24} + g^{26} + g^{27}) \\
&= gcd(g^3 + g^5 + g^6 + g^{17} + g^{19} + g^{20} + g^{24} + g^{26} + g^{27}, 1 + g^3 + g^4 + g^5 + \\
&\quad g^{14} + g^{17} + g^{18} + g^{19} + g^{21} + g^{24} + g^{25} + g^{26}) \\
&= gcd(1 + g^3 + g^4 + g^5 + g^{14} + g^{17} + g^{18} + g^{19} + g^{21} + g^{24} + g^{25} + g^{26}, \\
&\quad g + g^3 + g^4 + g^{15} + g^{17} + g^{18} + g^{22} + g^{24} + g^{25}) \\
&= gcd(g + g^3 + g^4 + g^{15} + g^{17} + g^{18} + g^{22} + g^{24} + g^{25}, \\
&\quad 1 + g^2 + g^3 + g^{14} + g^{16} + g^{17} + g^{21} + g^{23} + g^{24}) \\
&= gcd(1 + g^2 + g^3 + g^{14} + g^{16} + g^{17} + g^{21} + g^{23} + g^{24}, 0) \\
&= 1 + g^2 + g^3 + g^{14} + g^{16} + g^{17} + g^{21} + g^{23} + g^{24}.
\end{aligned}
$$

Similarly, we found that $< \Omega_0 + \Omega_2 + \Omega_4 >$ is a $[49, 25, 9]$-binary cyclic code by finding the generator polynomial as follows:

$$
\begin{aligned}
& g(x) \\
=& gcd(g^{49} - 1, 1 + g^3 + g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{17} + g^{19} + g^{20} + g^{21} + g^{24} \\
& + g^{26} + g^{27} + g^{31} + g^{33} + g^{34} + g^{35} + g^{38} + g^{40} + g^{41} + g^{42} + g^{45} + g^{47} + g^{48}) \\
=& gcd(1 + g^3 + g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{17} + g^{19} + g^{20} + g^{21} + g^{24} + g^{26} + \\
& g^{27} + g^{31} + g^{33} + g^{34} + g^{35} + g^{38} + g^{40} + g^{41} + g^{42} + g^{45} + g^{47} + g^{48}, g + g^3 + \\
& g^4 + g^5 + g^7 + g^{10} + g^{11} + g^{12} + g^{14} + g^{17} + g^{18} + g^{19} + g^{22} + g^{24} + g^{25} + \\
& g^{26} + g^{28} + g^{31} + g^{32} + g^{33} + g^{36} + g^{38} + g^{39} + g^{40} + g^{43} + g^{45} + g^{46} + g^{47}) \\
=& gcd(g + g^3 + g^4 + g^5 + g^7 + g^{10} + g^{11} + g^{12} + g^{14} + g^{17} + g^{18} + g^{19} + g^{22} + \\
& g^{24} + g^{25} + g^{26} + g^{28} + g^{31} + g^{32} + g^{33} + g^{36} + g^{38} + g^{39} + g^{40} + g^{43} + g^{45} + \\
& g^{46} + g^{47}, 1 + g^2 + g^3 + g^4 + g^8 + g^{10} + g^{11} + g^{15} + g^{17} + g^{18} + g^{21} + g^{23} + \\
& g^{24} + g^{25} + g^{29} + g^{31} + g^{32} + g^{35} + g^{37} + g^{38} + g^{39} + g^{42} + g^{44} + g^{45} + g^{46}) \\
=& gcd(1 + g^2 + g^3 + g^4 + g^8 + g^{10} + g^{11} + g^{15} + g^{17} + g^{18} + g^{21} + g^{23} + g^{24} + \\
& g^{25} + g^{29} + g^{31} + g^{32} + g^{35} + g^{37} + g^{38} + g^{39} + g^{42} + g^{44} + g^{45} + g^{46}, \\
& g^7 + g^9 + g^{10} + g^{14} + g^{16} + g^{17} + g^{28} + g^{30} + g^{31}) \\
=& gcd(g^7 + g^9 + g^{10} + g^{14} + g^{16} + g^{17} + g^{28} + g^{30} + g^{31}, 1 + g^2 + g^3 + g^4 + \\
& g^8 + g^{10} + g^{11} + g^{14} + g^{15} + g^{16} + g^{21} + g^{23} + g^{24} + g^{25} + g^{28} + g^{29} + g^{30}) \\
=& gcd(1 + g^2 + g^3 + g^4 + g^8 + g^{10} + g^{11} + g^{14} + g^{15} + g^{16} + g^{21} + g^{23} + g^{24} + \\
& g^{25} + g^{28} + g^{29} + g^{30}, g + g^3 + g^4 + g^5 + g^7 + g^{10} + g^{11} + g^{12} + g^{14} + g^{15} + \\
& g^{22} + g^{24} + g^{25} + g^{26} + g^{28} + g^{29}) \\
=& gcd(g + g^3 + g^4 + g^5 + g^7 + g^{10} + g^{11} + g^{12} + g^{14} + g^{15} + g^{22} + g^{24} + g^{25} + \\
& g^{26} + g^{28} + g^{29}, 1 + g^3 + g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{14} + g^{21} + g^{24} + \\
& g^{26} + g^{27} + g^{28}) \\
=& gcd(1 + g^3 + g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{14} + g^{21} + g^{24} + g^{26} + g^{27} + g^{28}, \\
& g^3 + g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{24} + g^{26} + g^{27}) \\
=& gcd(g^3 + g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{24} + g^{26} + g^{27}, \\
& 1 + g^3 + g^4 + g^5 + g^7 + g^{10} + g^{11} + g^{12} + g^{21} + g^{24} + g^{25} + g^{26})
\end{aligned}
$$

$$
\begin{aligned}
&=gcd(1+g^3+g^4+g^5+g^7+g^{10}+g^{11}+g^{12}+g^{21}+g^{24}+g^{25}+g^{26},\\
&\quad g+g^3+g^4+g^8+g^{10}+g^{11}+g^{22}+g^{24}+g^{25})\\
&=gcd(g+g^3+g^4+g^8+g^{10}+g^{11}+g^{22}+g^{24}+g^{25},1+g^2+g^3+g^7+\\
&\quad g^9+g^{10}+g^{21}+g^{23}+g^{24})\\
&=gcd(1+g^2+g^3+g^7+g^9+g^{10}+g^{21}+g^{23}+g^{24},0)\\
&=1+g^2+g^3+g^7+g^9+g^{10}+g^{21}+g^{23}+g^{24}.
\end{aligned}
$$

For $< \Omega_1 + \Omega_2 + \Omega_3 >$, the generator polynomial of this code is as follows:

$$
\begin{aligned}
g(x) =&gcd(g^{49}-1, g^1+g^2+g^4+g^7+g^8+g^{14}+g^{16}+g^{32}+g^{15}+g^{30}+g^{11}+\\
&g^{22}+g^{28}+g^{44}+g^{39}+g^{29}+g^9+g^{18}+g^{36}+g^{23}+g^{46}+g^{43}+g^{37}+g^{25}+\\
&g^3+g^5+g^6+g^{10}+g^{12}+g^{13}+g^{17}+g^{19}+g^{20}+g^{24}+g^{26}+g^{27}+g^{31}+\\
&g^{33}+g^{34}+g^{38}+g^{40}+g^{41}+g^{45}+g^{47}+g^{48})\\
=&gcd(g^1+g^2+g^3+g^4+g^5+g^6+g^7+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{14}\\
&+g^{15}+g^{16}+g^{17}+g^{18}+g^{19}+g^{20}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27}+\\
&g^{28}+g^{29}+g^{30}+g^{31}+g^{32}+g^{33}+g^{34}+g^{36}+g^{37}+g^{38}+g^{39}+g^{40}+g^{41}+\\
&g^{43}+g^{44}+g^{45}+g^{46}+g^{47}+g^{48},1+g+g^{21}+g^{22}+g^{35}+g^{36}+g^{42}+g^{43})\\
=&gcd(1+g+g^{21}+g^{22}+g^{35}+g^{36}+g^{42}+g^{43},g^7+g^8+g^9+g^{10}+g^{11}+\\
&g^{12}+g^{13}+g^{14}+g^{15}+g^{16}+g^{17}+g^{18}+g^{19}+g^{20}+g^{28}+g^{29}+g^{30}+\\
&g^{31}+g^{32}+g^{33}+g^{34})\\
=&gcd(g^7+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{14}+g^{15}+g^{16}+g^{17}+g^{18}+\\
&g^{19}+g^{20}+g^{28}+g^{29}+g^{30}+g^{31}+g^{32}+g^{33}+g^{34},1+g+g^{14}+g^{15}+\\
&g^{21}+g^{22}+g^{28}+g^{29})\\
=&gcd(1+g+g^{14}+g^{15}+g^{21}+g^{22}+g^{28}+g^{29},g+g^2+g^3+g^4+g^5+g^6+g^7+\\
&g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{14}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27}+g^{28})\\
=&gcd(g+g^2+g^3+g^4+g^5+g^6+g^7+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{14}+\\
&g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27}+g^{28},1+g+g^2+g^3+g^4+g^5+g^6+g^7+\\
&g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{21}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27})\\
=&1+g+g^2+g^3+g^4+g^5+g^6+g^7+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+\\
&g^{21}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27}.
\end{aligned}
$$

Clearly, the dimension of the code is 22. If we take $g(x) + g \cdot g(x)$, we will get $1 + g^{14} + g^{21} + g^{28}$ which is actually the generator polynomial of <$\Omega_0 + \Omega_4$>. Hence, the minimum distance is 4. So, <$\Omega_1 + \Omega_2 + \Omega_3$> is a $[49, 22, 4]$-binary cyclic code.

Next, we have <$\Omega_1 + \Omega_2 + \Omega_4$> as a generating idempotent. By Theorem 3.26, the generator polynomial is related as follows:

$$\begin{aligned}
g(x) =& gcd(g^{49} - 1, g^1 + g^2 + g^4 + g^8 + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{21} + g^{22} + \\
& g^{35} + g^{42} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25} + \\
& g^3 + g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{17} + g^{19} + g^{20} + g^{24} + g^{26} + g^{27} + g^{31} + \\
& g^{33} + g^{34} + g^{38} + g^{40} + g^{41} + g^{45} + g^{47} + g^{48}) \\
=& gcd(g^1 + g^2 + g^3 + g^4 + g^5 + g^6 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{15} + \\
& g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + \\
& g^{29} + g^{30} + g^{31} + g^{32} + g^{33} + g^{34} + g^{35} + g^{36} + g^{37} + g^{38} + g^{39} + g^{40} + \\
& g^{41} + g^{42} + g^{43} + g^{44} + g^{45} + g^{46} + g^{47} + g^{48}, 1 + g + g^7 + g^8 + g^{14} + \\
& g^{15} + g^{28} + g^{29}) \\
=& gcd(1 + g + g^7 + g^8 + g^{14} + g^{15} + g^{28} + g^{29}, g + g^2 + g^3 + g^4 + g^5 + g^6 + \\
& g^7 + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + \\
& g^{26} + g^{27} + g^{28}) \\
=& gcd(g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + \\
& g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28}, 1 + g + g^2 + g^3 + g^4 + g^5 + \\
& g^6 + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + \\
& g^{25} + g^{26} + g^{27}) \\
=& gcd(1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + \\
& g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27}, 0) \\
=& 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + \\
& g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27}.
\end{aligned}$$

Clearly, the dimension is 22. If we sum up $g(x)$ and $g \cdot g(x)$, we get $1 + g^7 + g^{14} + g^{28}$ again. Hence, <$\Omega_1 + \Omega_2 + \Omega_4$> is a $[49, 22, 4]$-binary cyclic code.

For <$\Omega_1 + \Omega_3 + \Omega_4$>, the generator polynomial can be easily found as follows:

$$\begin{aligned}
g(x) =& gcd(g^{49} - 1, g^1 + g^2 + g^4 + g^7 + g^8 + g^{14} + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + \\
& g^{21} + g^{22} + g^{28} + g^{35} + g^{42} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + \\
& g^{43} + g^{37} + g^{25}) \\
=& gcd(g^1 + g^2 + g^4 + g^7 + g^8 + g^{14} + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{21} + g^{22} + \\
& g^{28} + g^{35} + g^{42} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + \\
& g^{25}, 1 + g + g^3) \\
=& gcd(1 + g + g^3, 0) \\
=& 1 + g + g^3.
\end{aligned}$$

The dimension of the code is 46 and $d = 3$. Hence, <$\Omega_1 + \Omega_3 + \Omega_4$> is a $[49, 46, 3]$-binary cyclic code. For <$\Omega_2 + \Omega_3 + \Omega_4$>, the generator polynomial is found as follows:

$$\begin{aligned}
g(x) =& gcd(g^{49} - 1, g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + \\
& g^{20} + g^{21} + g^{24} + g^{26} + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} + g^{35} + g^{38} + g^{40} + \\
& g^{41} + g^{42} + g^{45} + g^{47} + g^{48}) \\
=& gcd(g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} + g^{21} + \\
& g^{24} + g^{26} + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} + g^{35} + g^{38} + g^{40} + g^{41} + g^{42} + \\
& g^{45} + g^{47} + g^{48}, 1 + g^3 + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{15} + g^{17} + \\
& g^{18} + g^{19} + g^{22} + g^{24} + g^{25} + g^{26} + g^{29} + g^{31} + g^{32} + g^{33} + g^{36} + g^{38} + \\
& g^{39} + g^{40} + g^{43} + g^{45} + g^{46} + g^{47}) \\
=& gcd(1 + g^3 + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{15} + g^{17} + g^{18} + g^{19} + \\
& g^{22} + g^{24} + g^{25} + g^{26} + g^{29} + g^{31} + g^{32} + g^{33} + g^{36} + g^{38} + g^{39} + g^{40} + \\
& g^{43} + g^{45} + g^{46} + g^{47}, g + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + \\
& g^{17} + g^{18} + g^{21} + g^{23} + g^{24} + g^{25} + g^{28} + g^{30} + g^{31} + g^{32} + g^{35} + g^{37} + \\
& g^{38} + g^{39} + g^{42} + g^{44} + g^{45} + g^{46}) \\
=& gcd(g + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{21} + \\
& g^{23} + g^{24} + g^{25} + g^{28} + g^{30} + g^{31} + g^{32} + g^{35} + g^{37} + g^{38} + g^{39} + g^{42} + \\
& g^{44} + g^{45} + g^{46}, 1 + g^2 + g^3) \\
=& 1 + g^2 + g^3.
\end{aligned}$$

The dimension of this code is 46 and the minimum distance is 3. $<\Omega_2 + \Omega_3 + \Omega_4>$ is a $[49, 46, 3]$-binary cyclic code.

For $< \Omega_0 + \Omega_1 + \Omega_2 + \Omega_3 >$, the generator polynomial of this code is constructed by Theorem 3.26 as follows:

$$\begin{aligned}
g(x) =& gcd(g^{49} - 1, 1 + g^1 + g^2 + g^4 + g^7 + g^8 + g^{14} + g^{16} + g^{32} + g^{15} + g^{30} + \\
& g^{11} + g^{22} + g^{28} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + \\
& g^{37} + g^{25} + g^3 + g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{17} + g^{19} + g^{20} + g^{24} + \\
& g^{26} + g^{27} + g^{31} + g^{33} + g^{34} + g^{38} + g^{40} + g^{41} + g^{45} + g^{47} + g^{48}) \\
=& gcd(1 + g^1 + g^2 + g^4 + g^7 + g^8 + g^{14} + g^{16} + g^{32} + g^{15} + g^{30} + g^{11} + g^{22} + \\
& g^{28} + g^{44} + g^{39} + g^{29} + g^9 + g^{18} + g^{36} + g^{23} + g^{46} + g^{43} + g^{37} + g^{25} + g^3 + \\
& g^5 + g^6 + g^{10} + g^{12} + g^{13} + g^{17} + g^{19} + g^{20} + g^{24} + g^{26} + g^{27} + g^{31} + g^{33} + \\
& g^{34} + g^{38} + g^{40} + g^{41} + g^{45} + g^{47} + g^{48}, g^{21} + g^{22} + g^{35} + g^{36} + g^{42} + g^{43}) \\
=& gcd(g^{21} + g^{22} + g^{35} + g^{36} + g^{42} + g^{43}, 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + \\
& g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + \\
& g^{28} + g^{29} + g^{30} + g^{31} + g^{32} + g^{33} + g^{34}) \\
=& gcd(1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + g^{13} + \\
& g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{28} + g^{29} + g^{30} + g^{31} + g^{32} + g^{33} + \\
& g^{34}, g^7 + g^8 + g^{21} + g^{22} + g^{28} + g^{29}) \\
=& gcd(g^7 + g^8 + g^{21} + g^{22} + g^{28} + g^{29}, 1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + \\
& g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + \\
& g^{27} + g^{28}) \\
=& gcd(1 + g + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + \\
& g^{20} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28}, g + g^2 + g^3 + g^4 + g^5 + g^6 + \\
& g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27}) \\
=& gcd(g + g^2 + g^3 + g^4 + g^5 + g^6 + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{22} + \\
& g^{23} + g^{24} + g^{25} + g^{26} + g^{27}, 1 + g + g^{14} + g^{15} + g^{21} + g^{22}) \\
=& 1 + g + g^{14} + g^{15} + g^{21} + g^{22}.
\end{aligned}$$

The dimension of the cyclic code is 27 and the minimum distance is 6. $< \Omega_0 + \Omega_1 + \Omega_2 + \Omega_3 >$ is a $[49, 27, 6]$-binary cyclic code.

Next, we have <$\Omega_0 + \Omega_1 + \Omega_2 + \Omega_4$> as a generating idempotent. By Theorem 3.26, the generator polynomial is constructed as follows:

$$\begin{aligned}
g(x) =& gcd(g^{49}-1, 1+g^1+g^2+g^4+g^8+g^{16}+g^{32}+g^{15}+g^{30}+g^{11}+g^{21}+\\
& g^{22}+g^{35}+g^{42}+g^{44}+g^{39}+g^{29}+g^9+g^{18}+g^{36}+g^{23}+g^{46}+g^{43}+\\
& g^{37}+g^{25}+g^3+g^5+g^6+g^{10}+g^{12}+g^{13}+g^{17}+g^{19}+g^{20}+g^{24}+\\
& g^{26}+g^{27}+g^{31}+g^{33}+g^{34}+g^{38}+g^{40}+g^{41}+g^{45}+g^{47}+g^{48})\\
=& gcd(1+g^1+g^2+g^4+g^8+g^{16}+g^{32}+g^{15}+g^{30}+g^{11}+g^{21}+g^{22}+\\
& g^{35}+g^{42}+g^{44}+g^{39}+g^{29}+g^9+g^{18}+g^{36}+g^{23}+g^{46}+g^{43}+g^{37}+\\
& g^{25}+g^3+g^5+g^6+g^{10}+g^{12}+g^{13}+g^{17}+g^{19}+g^{20}+g^{24}+g^{26}+\\
& g^{27}+g^{31}+g^{33}+g^{34}+g^{38}+g^{40}+g^{41}+g^{45}+g^{47}+g^{48},\\
& g^7+g^8+g^{14}+g^{15}+g^{28}+g^{29})\\
=& gcd(g^7+g^8+g^{14}+g^{15}+g^{28}+g^{29}, 1+g+g^2+g^3+g^4+g^5+g^6+\\
& g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{14}+g^{21}+g^{22}+g^{23}+g^{24}+g^{25}+\\
& g^{26}+g^{27}+g^{28})\\
=& gcd(1+g+g^2+g^3+g^4+g^5+g^6+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+\\
& g^{14}+g^{21}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27}+g^{28}, g+g^2+g^3+g^4+g^5+\\
& g^6+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{22}+g^{23}+g^{24}+g^{25}+g^{26}+g^{27})\\
=& gcd(g+g^2+g^3+g^4+g^5+g^6+g^8+g^9+g^{10}+g^{11}+g^{12}+g^{13}+g^{22}+\\
& g^{23}+g^{24}+g^{25}+g^{26}+g^{27}, 1+g+g^7+g^8+g^{21}+g^{22})\\
=& 1+g+g^7+g^8+g^{21}+g^{22}.
\end{aligned}$$

The dimension of the cyclic code is 27 and the minimum distance is 6. $< \Omega_0 + \Omega_1 + \Omega_2 + \Omega_4 >$ is a $[49, 27, 6]$-binary cyclic code.

$< \Omega_0 + \Omega_1 + \Omega_3 + \Omega_4 >$ can be written as

$$\begin{aligned}
(1+g+g^3)(1+g^1+g^2+g^4+g^7+g^8+g^{14}+g^{16}+\\
g^{32}+g^{15}+g^{30}+g^{11}+g^{21}+g^{22}+g^{28}+\\
g^{35}+g^{42}+g^{44}+g^{39}+g^{29}+g^9+g^{18}+\\
g^{36}+g^{23}+g^{46}+g^{43}+g^{37}+g^{25}) = g^{49}-1
\end{aligned}$$

From this, the generating idempotent is the generator polynomial for a $[49, 3, 28]$ cyclic code.

Next, we constructed the generator polynomial for <$\Omega_0 + \Omega_2 + \Omega_3 + \Omega_4$>.

$$
\begin{aligned}
g(x) =& gcd(g^{49} - 1, 1 + g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} \\
& + g^{20} + g^{21} + g^{24} + g^{26} + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} + g^{35} + g^{38} + g^{40} \\
& + g^{41} + g^{42} + g^{45} + g^{47} + g^{48}) \\
=& gcd(1 + g^3 + g^5 + g^6 + g^7 + g^{10} + g^{12} + g^{13} + g^{14} + g^{17} + g^{19} + g^{20} + g^{21} + \\
& g^{24} + g^{26} + g^{27} + g^{28} + g^{31} + g^{33} + g^{34} + g^{35} + g^{38} + g^{40} + g^{41} + g^{42} + \\
& g^{45} + g^{47} + g^{48}, g + g^3 + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{15} + g^{17} + \\
& g^{18} + g^{19} + g^{22} + g^{24} + g^{25} + g^{26} + g^{29} + g^{31} + g^{32} + g^{33} + g^{36} + g^{38} + \\
& g^{39} + g^{40} + g^{43} + g^{45} + g^{46} + g^{47}) \\
=& gcd(g + g^3 + g^4 + g^5 + g^8 + g^{10} + g^{11} + g^{12} + g^{15} + g^{17} + g^{18} + g^{19} + \\
& g^{22} + g^{24} + g^{25} + g^{26} + g^{29} + g^{31} + g^{32} + g^{33} + g^{36} + g^{38} + g^{39} + g^{40} + \\
& g^{43} + g^{45} + g^{46} + g^{47}, 1 + g^2 + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + \\
& g^{16} + g^{17} + g^{18} + g^{21} + g^{23} + g^{24} + g^{25} + g^{28} + g^{30} + g^{31} + g^{32} + g^{35} + \\
& g^{37} + g^{38} + g^{39} + g^{42} + g^{44} + g^{45} + g^{46}) \\
=& 1 + g^2 + g^3 + g^4 + g^7 + g^9 + g^{10} + g^{11} + g^{14} + g^{16} + g^{17} + g^{18} + g^{21} + \\
& g^{23} + g^{24} + g^{25} + g^{28} + g^{30} + g^{31} + g^{32} + g^{35} + g^{37} + g^{38} + g^{39} + g^{42} + \\
& g^{44} + g^{45} + g^{46}
\end{aligned}
$$

The dimension of the code is 3 which gives us 8 codewords in total. By cyclic shifting the generator polynomial, we get 7 distinct codewords. Hence, we have the minimum distance to be 28 and <$\Omega_0 + \Omega_2 + \Omega_3 + \Omega_4$> is a $[49, 3, 28]$-binary cyclic code.

For $< \Omega_1 + \Omega_2 + \Omega_3 + \Omega_4 >$, the generator polynomial is found to be as follows:

$$
\begin{aligned}
g(x) =& gcd(g^{49} - 1, g^1 + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + \\
& g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + \\
& g^{24} + g^{25} + g^{26} + g^{27} + g^{28} + g^{29} + g^{30} + g^{31} + g^{32} + g^{33} + g^{34} + g^{35} + \\
& g^{36} + g^{37} + g^{38} + g^{39} + g^{40} + g^{41} + g^{42} + g^{43} + g^{44} + g^{45} + g^{46} + g^{47} + g^{48}) \\
=& gcd(1 + g^1 + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 + g^{10} + g^{11} + g^{12} + \\
& g^{13} + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} + g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + \\
& g^{25} + g^{26} + g^{27} + g^{28} + g^{29} + g^{30} + g^{31} + g^{32} + g^{33} + g^{34} + g^{35} + g^{36} +
\end{aligned}
$$

$$g^{37} + g^{38} + g^{39} + g^{40} + g^{41} + g^{42} + g^{43} + g^{44} + g^{45} + g^{46} + g^{47} + g^{48}, 1 + g)$$
$$= 1 + g.$$

Dimension of the cyclic code is 48 while the minimum distance is 2. Hence, $< \Omega_1 + \Omega_2 + \Omega_3 + \Omega_4 >$ is a $[49, 48, 2]$-binary cyclic code.

$< \Omega_0 + \Omega_1 + \Omega_2 + \Omega_3 + \Omega_4 >$ can be written as

$$(1 + g)(1 + g^1 + g^2 + g^3 + g^4 + g^5 + g^6 + g^7 + g^8 + g^9 +$$
$$g^{10} + g^{11} + g^{12} + g^{13} + g^{14} + g^{15} + g^{16} + g^{17} + g^{18} + g^{19} +$$
$$g^{20} + g^{21} + g^{22} + g^{23} + g^{24} + g^{25} + g^{26} + g^{27} + g^{28} + g^{29} +$$
$$g^{30} + g^{31} + g^{32} + g^{33} + g^{34} + g^{35} + g^{36} + g^{37} + g^{38} + g^{39} +$$
$$g^{40} + g^{41} + g^{42} + g^{43} + g^{44} + g^{45} + g^{46} + g^{47} + g^{48}) = g^{49} - 1$$

From this, the generating idempotent is the generator polynomial for a $[49, 1, 49]$ cyclic code.

4-3 Construction of Secret Sharing Schemes

In this section, we construct secret sharing schemes based on the cyclic codes constructed in the previous section. Secret sharing scheme is used to break down a secret into smaller portions call shares and later distributed to other participants by a dealer. The group of participants who hold the shares that can reconstruct the secret is called the access set. If a group of participants can recover the secret by combining their shares, then any group of participants containing this group can also recover the secret. The group of participants is known as the minimal access set if they can recover the secret with their shares, while any of its proper subgroups cannot do so (Yuan & Ding (2006)). In this case, a proper subgroup has fewer members than this group. Before we can construct this set, we need to introduce two new terms called support and minimal codewords.

The support of a vector $c \in \mathbb{F}_q^n$ is defined to be $\{0 \leq i \leq n-1 : c_i \neq 0\}$ (Yuan & Ding (2006)). In other words, support is a set of positions of symbols in a codeword that are nonzero. A codeword c_2 covers a codeword c_1 if the support of c_2 contains that of c_1.The Hamming weight is actually the size of the support.

If a nonzero codeword c covers only its multiples, but no other nonzero codewords, then it is called a minimal vector. Then, a codeword c is called a minimal codeword if its first coordinate is 1 and covers no other codeword whose first coordinate is 1. Clearly, a minimal codeword is a minimal vector but the opposite is not true.

The following is a secret sharing scheme constructed based on balanced incomplete block design which gives a nice access structure. (X, A) is called a $(\nu, \kappa, \lambda) - BIBD$ if and only if

1. $|X| = \nu$.
2. For any nonempty subset $B \in A$ called block, $|B| = \kappa$.
3. Any pair of distinct points occur in exactly λ blocks.

Furthermore,

4. $|A| = \frac{\nu}{\kappa}\frac{\lambda(\nu-1)}{\kappa-1}$.
5. Every point occur in exactly $\frac{\lambda(\nu-1)}{\kappa-1}$ blocks.

From the results developed by Ding(Yuan & Ding (2006)), we observed the following results on secret sharing scheme.

The secret sharing scheme based on a $(\nu, \kappa, \lambda) - BIBD$ is for sharing secrets among ν participants. There are $\frac{\nu}{\kappa}\frac{\lambda(\nu-1)}{\kappa-1}$ minimal access sets. Each minimal access set consists of κ participants, and each participants is a member of exactly $\frac{\lambda(\nu-1)}{\kappa-1}$ minimal access set.

Now, we construct our own secret sharing scheme based on some of the cyclic codes constructed in the previous section. From subsection 4-2-1, we randomly choose $<\Omega_1>$ to construct our first secret sharing scheme. $<\Omega_1>$ is a $[9, 2, 6]$-binary cyclic code which have the following codewords:

$$\{000000000, 101101101, 110110110, 011011011\}.$$

In the secret sharing scheme based on $[9, 2, 6]$-cyclic code, there are 8 participants and a dealer involved. There are only two access sets as follows:

$$\{1, 3, 4, 6, 7\} \text{ and } \{2, 3, 5, 6, 8\}$$

$\{1, 3, 4, 6, 7\}$ denotes the access set $\{P_1, P_3, P_4, P_6, P_7\}$. From above, we can see that participants 3 and 6 are involved in all the access sets. Hence, whoever who need to find the secret must include these two participants. In each access set, there are exactly $d-1 = 6-1 = 5$ participants. Every participant in the set $\{1, 2, 4, 5, 7, 8\}$ is in exactly one access set.

Now, we consider $<\Omega_2>$, a $[9, 6, 2]$ cyclic code. Again, we list down all the codewords for the cyclic code as follows:

$$\{000000000, 010010000, 001001000, 000100100, 000010010, 000001001,$$
$$100000100, 010000010, 001000001, 100100000, 010111101, 101011110,$$
$$010101111, 101010111, 110101011, 111010101, 111101010, 011110101,$$
$$101111010, 101100001, 110110000, 011011000, 001101100, 000110110,$$
$$000011011, 100001101, 110000110, 011000011, 110100010, 011010001,$$
$$101101000, 010110100, 001011010, 000101101, 100010110, 010001011,$$
$$101000101, 100111011, 110011101, 111001110, 011100111, 101110011,$$
$$110111001, 111011100, 011101110, 001110111, 100011111, 110001111,$$
$$111000111, 111100011, 111110001, 111111000, 011111100, 001111110,$$
$$000111111, 101001100, 010100110, 001010011, 100101001, 110010100,$$
$$011001010, 001100101, 100110010, 010011001\}$$

Throughout all these codewords, there are only two minimal codewords. So, there are only 2 access sets as follows:$\{3\}$ and $\{6\}$. Both participants 3 and 6 can solely determine the secret. If participant 3 cheats and recover the secret by himself, there is no one to govern his actions. Hence, this secret sharing scheme may expose the secret easily. To describe in a more business-related way, there are two business partner A and B which represent participants 3 and 6 here where both of them have full access right to their shared account. Since A has the full access right, if A became greedy, he can take all the money invested and run away.

Next, we take $\mathbb{F}[\mathbb{Z}_{25}]$, $<\Omega_1>$ is a $[25, 4, 10]$-binary cyclic code from subsection 4-2-2. Since the dimension of $<\Omega_1>$ is 4, then $|<\Omega_1>|=2^4=16$. Then we have 16 codewords

as follows:

$$\begin{aligned}
<\Omega_1> = \{&000000000000000000000000, 100011000110001100011000 1,\\
&110001100011000110001100 0, 011000110001100011000110 0,\\
&001100011000110001100011 0, 000110001100011000110001 1,\\
&010010100101001010010010 01, 101001010010100101001010 0,\\
&010100101001010010100101 0, 001010010100101001010010 1,\\
&100101001010010100101001 0, 111011110111101111011101 1,\\
&111101111011110111101111 0, 011110111101111011110111 1,\\
&101111011110111101111011 1, 110111101111011110111101 1\}
\end{aligned}$$

We also have the generator matrix as follows:

$$G = \begin{pmatrix} 011110111101111011101111 \\ 101111011110111101111011 \\ 110111101111011110111101 \\ 111011110111101111011110 \end{pmatrix}.$$

We let g_i to be the ith row of the generator matrix and g_j to be the jth row of the generator matrix. Then, $g_i + g_j$ will be sum of the two rows in generator matrix. We only consider g_i, g_j, g_k and g_l because the rows of G which represents the basis of the cyclic code is at most 4. From the generator matrix we see that

$$\begin{aligned}
wt(g_i) &= 20 \ \forall i,\\
wt(g_i + g_j) &= 10 \ \forall i, j,\\
wt(g_i + g_j + g_k) &= 10 \ \forall i, j, k,\\
wt(g_i + g_j + g_k + g_l) &= 20.
\end{aligned}$$

From above, we can conclude that $<\Omega_1>$ is a 2-constant weight code as it only has two type of weight which are 10 and 20. Now, we proceed with the secret sharing scheme.

Now, we construct the secret sharing scheme based on a $[25, 4, 10]$-code where the secrets are shared among 24 participants. One of the 25 participants is a trusted dealer that distributes the secrets so he is excluded. The access set corresponding to the minimal codewords are as follows:

$$\{4, 5, 9, 10, 14, 15, 19, 20, 24\}, \{1, 5, 6, 10, 11, 15, 16, 20, 21\},$$
$$\{2, 5, 7, 10, 12, 15, 17, 20, 22\}, \{3, 5, 8, 10, 13, 15, 18, 20, 23\}.$$

$\{4, 5, 9, 10, 14, 15, 19, 20, 24\}$ denotes the group of participants $\{P_4, P_5, P_9, P_{10}, P_{14}, P_{15}, P_{19}, P_{20}, P_{24}\}$. Only the participants $P_5, P_{10}, P_{15}, P_{20}$ is in all the 4 access sets. So in order to recover the secret, these four participants must be included. Each access set contains exactly 9 participants.

The first example for $n = 49$, we take $<\Omega_1>$ which is a $[49, 4, 21]$-code from subsection 4-2-3. The secret sharing scheme is shared among 48 participants and one dealer is involved. As the dimension is 4, we have 16 codewords as follows:

$< \Omega_1 >=$

{0000000000000000000000000000000000000000000000000, 1111111111111111111111111111111111111111111111111,
1101000110100011010001101000110100011010001101000, 0110100011010001101000110100011010001101000110100,
0011010001101000110100011010001101000110100011010, 0001101000110100011010001101000110100011010001101,
1000110100011010001101000110100011010001101000110, 0100011010001101000110100011010001101000110100011,
1010001101000110100011010001101000110100011010001, 0101110010111001011100101110010111001011100101110,
0010111001011100101110010111001011100101110010111, 1001011100101110010111001011100101110010111001011,
1100101110010111001011100101110010111001011100101, 1110010111001011100101110010111001011100101110010,
0111001011100101110010111001011100101110010111001, 1011100101110010111001011100101110010111001011100}.

In the secret sharing constructed based on $[49, 4, 21]$-code, the 7 access sets are as follows:

$\{1, 3, 7, 8, 10, 14, 15, 17, 21, 22, 24, 28, 29, 31, 35, 36, 38, 42, 43, 45\}$,

$\{4, 5, 7, 11, 12, 14, 18, 19, 21, 25, 26, 28, 32, 33, 35, 39, 40, 42, 46, 47\}$,

$\{2, 6, 7, 9, 13, 14, 16, 20, 21, 23, 27, 28, 30, 34, 35, 37, 41, 42, 44, 48\}$,

$\{1, 4, 6, 7, 8, 11, 13, 14, 15, 18, 20, 21, 22, 25, 27, 28, 29, 32, 34, 35, 36, 39, 41, 42, 43, 46, 48\}$,

$\{1, 2, 5, 7, 8, 9, 12, 14, 15, 16, 19, 21, 22, 23, 26, 28, 29, 30, 33, 35, 36, 37, 40, 42, 43, 44, 47\}$,

$\{2, 3, 4, 7, 9, 10, 11, 14, 16, 17, 18, 21, 23, 24, 25, 28, 30, 31, 32, 35, 37, 38, 39, 42, 44, 45, 46\}$,

$\{3, 5, 6, 7, 10, 12, 13, 14, 17, 19, 20, 21, 24, 26, 27, 28, 31, 33, 34, 35, 38, 40, 41, 42, 45, 47, 48\}$.

Participants $7, 14, 21, 28, 35, 42$ appears in all access sets. Hence, any group who can determine the secret must include these 6 participants. Each participant in the set $\{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48\}$ is in exactly $k - 1 = 3$ access sets. Such a secret sharing scheme can be useful in big corporate where there are a few major shareholders to make a decision.

For the second example, we randomly choose $< \Omega_1 + \Omega_2 >$ which is a $[49, 6, 14]$-cyclic code to construct the secret sharing schemes. As the dimension is 6, there is 64 codewords which are listed in the previous section, so we are not going to list it again here. Similarly, the dealer distributes the shares of the secret among 48 participants. In the secret sharing scheme constructed based on $[49, 6, 14]$-code, the $k = 6$ access sets are as follows:

$$\{1, 7, 8, 14, 15, 21, 22, 28, 29, 35, 36, 42, 43\},$$
$$\{2, 7, 9, 14, 16, 21, 23, 28, 30, 35, 37, 42, 44\},$$
$$\{3, 7, 10, 14, 17, 21, 24, 28, 31, 35, 38, 42, 45\},$$
$$\{4, 7, 11, 14, 18, 21, 25, 28, 32, 35, 39, 42, 46\},$$
$$\{5, 7, 12, 14, 19, 21, 26, 28, 33, 35, 40, 42, 47\},$$
$$\{6, 7, 13, 14, 20, 21, 27, 28, 34, 35, 41, 42, 48\}.$$

Clearly, participants $7, 14, 21, 28, 35, 42$ appears in all access sets. Hence, any group who can determine the secret must include these 6 participants. Each participant in the set $\{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48\}$ is in exactly 1 access set. The number of participants in each access set is $d - 1 = 14 - 1 = 13$. There might be a pattern.

Now, we construct the secret sharing based on $[49, 3, 28]$-cyclic code constructed in previous section. The secret are distributed as shares to 48 participants by a dealer. To find the access set, we first find the minimal codeword from the following list of codewords:

$$\{0000000000000000000000000000000000000000000000000,$$
$$0111010011101001110100111010011101001110100111010,$$
$$0011101001110100111010011101001110100111010011101,$$
$$0100111010011101001110100111010011101001110100111,$$
$$1001110100111010011101001110100111010011101001110,$$
$$1010011101001110100111010011101001110100111010011,$$
$$1101001110100111010011101001110100111010011101001,$$
$$1110100111010011101001110100111010011101001110100\}$$

In the secret sharing constructed based on $[49, 3, 28]$-code, the 4 access sets are as follows:

$\{3, 4, 5, 7, 10, 11, 12, 14, 17, 18, 19, 21, 24, 25, 26, 28, 31, 32, 33, 35, 38, 39, 40, 42, 45, 46, 47\}$,

$\{2, 5, 6, 7, 8, 12, 13, 14, 16, 19, 20, 21, 23, 26, 27, 28, 30, 33, 34, 35, 37, 40, 41, 42, 44, 47, 48\}$,

$\{1, 3, 6, 7, 8, 10, 13, 14, 15, 17, 20, 21, 22, 24, 27, 28, 29, 31, 34, 35, 36, 38, 41, 42, 43, 45, 48\}$,

$\{1, 2, 4, 7, 8, 9, 11, 14, 15, 16, 18, 21, 22, 23, 25, 28, 29, 30, 32, 35, 36, 37, 39, 42, 43, 44, 46\}$.

Participants $7, 14, 21, 28, 35, 42$ appears in all access sets. Hence, any group who can determine the secret must include these 6 participants. Each participant in the set $\{1, 2, 3, 4, 5, 6, 8, 9, 10, 11, 12, 13, 15, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 29, 30, 31, 32, 33, 34, 36, 37, 38, 39, 40, 41, 43, 44, 45, 46, 47, 48\}$ is in exactly $k - 1 = 2$ access sets. In each access set, there are 27 participants. Such a secret sharing scheme can be useful in big corporate where there are a few major shareholders to make a decision.

CHAPTER 5: CONCLUSION

Table 5.1: List of generating idempotents and its corresponding cyclic codes of length $n = 9, 25$ and 49

n	Generating Idempotent	$[n, k, d]$-Cyclic Code	Construct Secret Sharing Scheme (✓/✗)
9	$< \Omega_0 >$	$[9, 9, 1]$	✗
	$< \Omega_1 >$	$[9, 2, 6]$	✓
	$< \Omega_2 >$	$[9, 6, 2]$	✓
	$< \Omega_0 > + < \Omega_1 >$	$[9, 7, 2]$	✗
	$< \Omega_0 > + < \Omega_2 >$	$[9, 3, 3]$	✗
	$< \Omega_1 > + < \Omega_2 >$	$[9, 8, 2]$	✗
	$< \Omega_0 > + < \Omega_1 > + < \Omega_2 >$	$[9, 1, 9]$	✗
25	$< \Omega_0 >$	$[25, 25, 1]$	✗
	$< \Omega_1 >$	$[25, 4, 10]$	✓
	$< \Omega_2 >$	$[25, 20, 2]$	✗
	$< \Omega_0 > + < \Omega_1 >$	$[25, 21, 2]$	✗
	$< \Omega_0 > + < \Omega_2 >$	$[25, 5, 5]$	✗
	$< \Omega_1 > + < \Omega_2 >$	$[25, 24, 2]$	✗
	$< \Omega_0 > + < \Omega_1 > + < \Omega_2 >$	$[25, 1, 25]$	✗
49	$< \Omega_0 >$	$[49, 49, 1]$	✗
	$< \Omega_1 >$	$[49, 4, 21]$	✓
	$< \Omega_2 >$	$[49, 4, 21]$	✗
	$< \Omega_3 >$	$[49, 28, 3]$	✗
	$< \Omega_4 >$	$[49, 28, 3]$	✗
	$< \Omega_0 + \Omega_1 >$	$[49, 45, 4]$	✗
	$< \Omega_0 + \Omega_2 >$	$[49, 45, 4]$	✗
	$< \Omega_0 + \Omega_3 >$	$[49, 21, 4]$	✗
	$< \Omega_0 + \Omega_4 >$	$[49, 49, 1]$	✗
	$< \Omega_1 + \Omega_2 >$	$[49, 6, 14]$	✓
	$< \Omega_1 + \Omega_3 >$	$[49, 24, 12]$	✗
	$< \Omega_1 + \Omega_4 >$	$[49, 24, 12]$	✗
	$< \Omega_2 + \Omega_3 >$	$[49, 24, 12]$	✗
	$< \Omega_2 + \Omega_4 >$	$[49, 24, 12]$	✗
	$< \Omega_3 + \Omega_4 >$	$[49, 42, 2]$	✗
	$< \Omega_0 + \Omega_1 + \Omega_2 >$	$[49, 43, 2]$	✗
	$< \Omega_0 + \Omega_1 + \Omega_3 >$	$[49, 25, 9]$	✗
	$< \Omega_0 + \Omega_1 + \Omega_4 >$	$[49, 25, 9]$	✗
	$< \Omega_0 + \Omega_2 + \Omega_3 >$	$[49, 25, 9]$	✗
	$< \Omega_0 + \Omega_2 + \Omega_4 >$	$[49, 25, 9]$	✗
	$< \Omega_0 + \Omega_3 + \Omega_4 >$	$[49, 7, 7]$	✗
	$< \Omega_1 + \Omega_2 + \Omega_3 >$	$[49, 22, 4]$	✗
	$< \Omega_1 + \Omega_2 + \Omega_4 >$	$[49, 22, 4]$	✗
	$< \Omega_1 + \Omega_3 + \Omega_4 >$	$[49, 46, 3]$	✗
	$< \Omega_2 + \Omega_3 + \Omega_4 >$	$[49, 46, 3]$	✗
	$< \Omega_0 + \Omega_1 + \Omega_2 + \Omega_3 >$	$[49, 27, 6]$	✗
	$< \Omega_0 + \Omega_1 + \Omega_2 + \Omega_4 >$	$[49, 27, 6]$	✗
	$< \Omega_0 + \Omega_1 + \Omega_3 + \Omega_4 >$	$[49, 3, 28]$	✓
	$< \Omega_0 + \Omega_2 + \Omega_3 + \Omega_4 >$	$[49, 3, 28]$	✗
	$< \Omega_1 + \Omega_2 + \Omega_3 + \Omega_4 >$	$[49, 48, 2]$	✗
	$< \Omega_0 + \Omega_1 + \Omega_2 + \Omega_3 + \Omega_4 >$	$[49, 1, 49]$	✗

In this project, we constructed the families of binary cyclic codes for $n = 9, 25$ and 49 as listed in the table above and marked those cyclic codes that were used to construct secret sharing schemes. Then, we also determined the access structure of the secret sharing schemes based on these cyclic codes where there are always a number of participants who must be in all access sets to recover the secret. In our project, we only chose the cyclic codes which we can list out all the codewords by hand so that all the minimal codewords were determined.

The program created to generate cyclotomic cosets modulo n greatly helped us in observing a certain pattern on the size of cyclotomic cosets for two types of prime number p. The first type of prime number p satisfy 2 is a primitive root modulo p while the second type of p satisfy that 2 has order $\frac{p-1}{2}$ modulo p. We generalized the number of cyclotomic cosets modulo p^2, p^3 and p^n as well as the number of elements in each cosets. In terms of group ring, we represented the cyclotomic cosets in a polynomial form which eased the construction of cyclic codes. As expected, the polynomial base properties of cyclic codes did eased the implementation of secret sharing schemes. In the future, it would be nice if we could generalize the cyclic codes for p^2 and the secret sharing schemes based on them have nice access structures.

REFERENCES

Blakley, G. R., 1979. 'Safeguarding cryptographic keys', *Proc. NCC AFIPS* pp. 313–317.

Huffman, W. C. & Pless, V., 2003. *Fundamentals of error-correcting codes*, Cambridge, UK: Cambridge University Press.

Li, Z., Xue, T. & Lai, H., 2010. 'Secret sharing schemes from binary linear codes', *Information Sciences* **180**(22), 4412–4419.

Ling, S. & Xing, C. P., 2004. *Coding Theory: a first course*, Cambridge University Press, Cambridge, UK.

MacWilliams, F. J. & Sloane, N. J. A., 1977. *The Theory of Error-Correcting Codes*, Vol. 16, North-Holland.

Massey, J. L., 1993. 'Minimal codewords and secret sharing', *Proceedings of the 6th Joint Swedish-Russian International Workshop on Information Theory* pp. 276–279.

McEliece, R. J. & Sarwate, D. V., 1981. 'On sharing secrets and reed-solomon codes', *Comm. ACM* **24**(9), 583–584.

Shamir, A., 1979. 'How to share a secret', *Comm. ACM* **22**(11), 612–613.

Shannon, C. E., 1948. 'A mathematical theory of communication', *The Bell System Technical Journal* **27**, 379–423,623–656.

Stinson, D. R., 2006. *Cryptography Theory and Practice*, Boca Raton: Chapman & Hall/CRC.

van Lint, J. H., 1999. *Introduction to Coding Theory*, New York: Springer-Verlag.

Yuan, J. & Ding, C. S., 2006. 'Secret sharing schemes from three classes of linear codes', *IEEE Transactions of Information Theory* **52**(1), 206–212.

APPENDIX A: PROGRAM CODE FOR CYCLOTOMIC COSETS

```
using System;
using System.Collections.Generic;
using System.ComponentModel;
using System.Data;
using System.Drawing;
using System.Linq;
using System.Text;
using System.Windows.Forms;
using System.Numerics;

namespace WindowsFormsApplication1
{
public partial class Form1 : Form
{
public Form1()
{
    InitializeComponent();
}

private void button1_Click(object sender, EventArgs e)
{   // Declaration and Initialization of variables
    LinkedList<BigInteger> remainder = new LinkedList<BigInteger>();
    int i = 1;
    int k = 1;
    int j = 1;
    BigInteger temp = 0;
    int temp2 = 0;
    int count;
    int modulus;// This modulus variable is n.
    string outlist = null;
    string outlist2 = null;
    string nl = Environment.NewLine;
    BigInteger q = 2;
    int check = 0;
    int cosetcount = 1;

    output.Text = "";
    output2.Text = "";
    modulus = 0;
    errorProvider1.Clear();
    q = (BigInteger)qvalue.Value;
    try
    {
        modulus = Convert.ToInt32(divisor1.Text);
        if (modulus % q == 0)
            errorProvider1.SetError(divisor1, "You must provide"+
       "a positive integer that is not a multiple of " + q + ".");
        else if (modulus == 1)
            errorProvider1.SetError(divisor1,"The modulus must be"+
           "greater than 1.");
        else
        {
            errorProvider1.Clear();
            check = 1;
        }
    }
    catch (FormatException)
    {
        errorProvider1.Clear();
        MessageBox.Show("Invalid value for modulus, please try again.");
    }
```

```
if (check == 1)
{
    // Reset the values of i, j and temp for every new n value.
    i = 1;
    j = 1;
    temp = 0;
    outlist += "This is C0 coset list :" + nl + "0" + nl + nl;

    do
    {
        cosetcount = 1;//reset number of elements in each coset

        remainder.AddFirst(i);
        outlist += "This is C" + i + " coset list :" + nl + i ;
        do
        {
         temp=((remainder.First.Value*BigInteger.Pow(q,j))%modulus);
         if (temp != remainder.First.Value)
         {
            remainder.AddLast(temp);
            outlist += "," + remainder.Last.Value;
            j++;
            cosetcount++;//take note number of elements in a coset

        }
        }while (temp != remainder.First.Value);
        outlist += nl+nl;
        outlist2 += nl + "|C"+i+"|=" + cosetcount + nl + nl;

        /*
            Linked list node is to declare a node to read the
            elements in the list. Below: the node is pointing
            to the first element in the list.
         */

        LinkedListNode<BigInteger> node = remainder.First;

        //Reset the value of temp2 and k
        temp2 = 0;
        k = 1;

        /*
        In this while loop,
        1. We check if the linked list is empty and temp2
           is null.If true, do the following.
           (a) Set count to 0.This counts the number of
           elements in the list that have been retrieved.
           (b) In the second while loop(inside the first
            one), we loop until the last element.Inside
            this loop, if k is not equal to the element
            in the list, we increase count by 1.Hence,
            if the total count after going through the
            list is equal to the number of elements in the
            linked list, then we assign k to be the
            smallest integer for the new cyclotomic coset.
           (c) Note: we reset the node to the first value
               every time before the comparison with new
               k value.
        */
        while (temp2 == 0 && node != null)
        {
            count = 0;
            while (node != null)
            {
                if (k != node.Value)
                    count++;
                node = node.Next;
            }
            if (count == remainder.Count)
```

```
                {
                    temp2 = k;
                    i = k;
                }
                k++;
                node = remainder.First;
            }

            // Reset the value of j for new cyclotomic coset
            j = 1;

        } while ((int)(modulus - 1) != remainder.Count);
        // Empty the linked list once all cyclomic c. is generated
        remainder.Clear();
        output.Text = outlist;
        output2.Text = outlist2;
    }

}
}
}
```