DIMENSION AND BOSE DISTANCE OF CERTAIN BCH CODES

ZHENG RUN

PhD

The Hong Kong Polytechnic University

2026

The Hong Kong Polytechnic University

Department of Applied Mathematics

Dimension and Bose distance of certain BCH codes

ZHENG Run

A thesis submitted in partial fulfilment of the requirements

for the degree of Doctor of Philosophy

August 2025

CERTIFICATE OF ORIGINALITY

I hereby declare that this thesis is my own work and that, to the best of my knowledge and belief, it reproduces no material previously published or written, nor material that has been accepted for the award of any other degree or diploma, except where due acknowledgment has been made in the text.

______________________________(Signed)

__________ZHENG Run__________(Name of student)

Publications Arising from the Thesis

- R. Zheng, N. S. Sze and Z. Huang, "The Dimension and Bose Distance of Certain Primitive BCH Codes," IEEE Transactions on Information Theory, vol. 71, no. 10, pp. 7670-7687, Oct. 2025, doi:10.1109/TIT.2025.3587496.

- R. Zheng, N. S. Sze and Z. Huang, "The dimension and Bose distance of some BCH codes of length $\frac{q^m-1}{\lambda}$," TechRxiv. October 07, 2025.
  doi: 10.36227/techrxiv.175988062.26727107/v1 (submitted)

Abstract

Error correction codes form the backbone of reliable digital communication and data storage systems. During information transmission, errors are inevitable due to channel noise and interference. Error correction codes provide mathematical frameworks to automatically detect and correct such errors. Their applications span a wide range of critical fields, including communication systems, computer networks, data storage, consumer electronics, and wireless networks.

Bose–Chaudhuri–Hocquenghem (BCH) codes, as a subclass of cyclic codes, play an important role in both theoretical research and practical applications. Their strong error-correcting capability and efficient encoding and decoding algorithms make BCH codes widely used in various domains including telecommunications, memory and storage technologies, and digital electronics.

Although BCH codes have been extensively studied theoretically and are widely used in practice, their key parameters, including dimension, minimum distance, and Bose distance, remain unknown in general. To date, only a limited family of BCH codes has been fully characterized in terms of these parameters. The dimension determines the number of information symbols a BCH code can carry, reflecting its data transmission efficiency. The minimum distance dictates the error-correcting capability of the code, with larger values enabling the correction of more errors. The Bose distance provides a lower bound on the minimum distance and, for certain families of BCH codes, equals it. Therefore, determining these parameters is essential for a deeper understanding and effective application of BCH codes.

Let m be a positive integer, q be a prime power and λ be a divisor of $q-1$. In this thesis, we investigate the parameters of q-ary BCH codes of length $\frac{q^m-1}{\lambda}$, which includes primitive BCH codes as a special case when $\lambda = 1$. By deriving some explicit formulas, we determine the dimension and Bose distance of BCH codes with this length $\frac{q^m-1}{\lambda}$ for $m \geq 4$ and for designed distances over a significantly wider range of designed distances than previously known. Using these formulas, we identify several optimal codes and linear codes with the best known parameters.

Keywords: Error correction codes, linear codes, cyclic codes, BCH codes, q-cyclotomic cosets, finite fields, coding theory

Acknowledgements

First and foremost, I wish to express my deepest and most sincere gratitude to my supervisor, Professor Nung-Sing Sze, for his invaluable guidance, unwavering support, rigorous mentorship, and constant encouragement throughout my PhD journey. His profound dedication to research and passionate approach to life have been a continuous source of inspiration, motivating me to overcome numerous challenges and difficulties encountered during my studies.

I am profoundly indebted to Professor Zejun Huang of Shenzhen University for his patient guidance and insightful advice. I will always cherish the memory of the time I spent conducting research in Shenzhen, which would not have been possible without his tremendous support. His assistance was instrumental in the completion of this thesis.

My special thanks go to Professor Chi-Kwong Li for providing me with the invaluable opportunity to visit the College of William & Mary and for his kind assistance during my stay. I am also deeply grateful to Professor Tin-Yau Tam of the University of Nevada, Reno, for inviting me to present my work on matrix theory, an experience that greatly enriched my academic perspective.

I extend my earnest appreciation to Professor Ying Miao, the handling editor, and the anonymous reviewers of our article "The Dimension and Bose Distance of certain Primitive BCH Codes" for their constructive comments and suggestions, which significantly improved the quality of the work.

I would like to thank Professor Luyining Gan from Beijing University of Posts and Telecommunications for her helpful discussions. My sincere thanks also go to Mr. Zhao Hui Zhang from Sichuan Normal University for his generous assistance in running Magma programs to compute the minimum distance of several code examples presented in this thesis.

I am also thankful to the faculty members of the Department of Mathematics at The Hong Kong Polytechnic University, particularly Professor Guofeng Zhang and Professor Ting Kei Pong, for their support and guidance during my PhD confirmation process.

I am deeply thankful to my family and friends for their unwavering companionship and steadfast support along this journey. Their belief in me has been my greatest strength.

Last but certainly not least, I am profoundly grateful to my girlfriend. Over the past two years, she has been my constant source of emotional support. Together, we have traveled to many places and seen many beautiful sights. The days we spent together have been the happiest and most meaningful of my PhD, and I cherish them beyond words.

Contents

Chapter 1

Introduction

1.1 Background

In the information age, the accurate transmission and storage of data are fundamental to modern society. Whether it is scientific data sent from deep-space probes, the clarity of a mobile phone call, the retrieval of digital content from optical discs, or the massive data exchanges within cloud computing centers, all rely on highly reliable information delivery. However, communication channels, such as wireless links, optical fibers, and storage devices, are all susceptible to noise, interference, and signal degradation. These issues can introduce errors into the transmitted data. Ensuring complete and accurate transmission of information under such imperfect conditions remains a major challenge in modern communication. Coding theory provides a powerful framework to address this issue.

The birth of coding theory can be traced back to Claude Shannon's seminal 1948 paper, "A Mathematical Theory of Communication." Shannon demonstrated that for any noisy communication channel, there exists a fundamental limit known as the channel capacity. Reliable communication is achievable at any rate below this capacity, provided that appropriate encoding and decoding methods are employed. The core idea of coding theory is to intentionally introduce redundancy into the transmitted data, thereby enabling the receiver to detect and correct errors that occur during transmission.

However, incorporating redundancy in an efficient and intelligent manner is far from trivial. This requires sophisticated mathematical tools to design codes that optimize the trade-off between redundancy, error-correcting capability, and computational complexity.

Throughout the development of coding theory, many classes of error correction codes have been designed. Key examples include Hamming codes [26] for single-error correction, Reed–Solomon codes [49] for burst error correction, turbo codes [7] for near-capacity iterative decoding, and polar codes [2] as the first capacity-achieving constructive codes. Among these, Bose–Chaudhuri–Hocquenghem (BCH) codes represent a particularly significant family of cyclic codes. Binary BCH codes were first independently discovered by Hocquenghem [28] in 1959 and by Bose and Ray-Chaudhuri [9, 10] in 1960. Gorenstein and Zierler [25] later extended binary BCH codes to q-ary BCH codes in 1961.

BCH codes occupy a central place in coding theory due to their remarkable properties. First, they offer great flexibility in the choice of code parameters, enabling error correction capabilities to be tailored to specific applications. Moreover, for block lengths up to a few hundred bits, many binary BCH codes are among the most powerful codes known for given length and dimension. Moreover, there exist efficient encoding and decoding algorithms for BCH codes, such as Peterson–Gorenstein–Zierler algorithm, Berlekamp–Massey algorithm, and Sugiyama Euclidean algorithm [6, 25, 43, 47]. These algorithms make BCH codes highly practical for real-world applications, such as communication systems, storage devices, and consumer electronics.

Although BCH codes have been extensively studied in the literature [1, 3, 4, 5, 11, 12, 13, 16, 17, 18, 19, 21, 22, 23, 27, 30, 31, 32, 33, 34, 35, 40, 45, 50, 52, 54, 55, 56, 58, 59] and are widely used in practice, the following fundamental questions about BCH codes remain open in general [18].

- What is the dimension of a BCH code?
- What is the Bose distance of a BCH code?
- What is the minimum distance of a BCH code?

The dimension and minimum distance offer a mathematical measure of the performance of a BCH code. Specifically, a BCH code of dimension k and minimum distance d can transmit k information symbols and correct up to $\lfloor (d-1)/2 \rfloor$ symbol errors. As noted by Charpin [14] and Ding [20], determining these two parameters of BCH codes is a very difficult problem.

Another important parameter of BCH codes is the Bose distance d_B, which is defined as the largest designed distance. The BCH bound [10, 28] indicates that $d \geq d_B$. The equality can even be obtained for some codes. For example, a narrow -sense primitive BCH code satisfies $d = d_B$ if its designed distance divides its length [41, p. 259]. Furthermore, it has been conjectured by Charpin [12] that $d \leq d_B + 4$ for a narrow-sense primitive BCH code. Therefore, determining the Bose distance is also valuable for understanding BCH codes.

1.2 Contributions

The thesis primarily focuses on the study of the dimension and Bose distance of BCH codes of length $\frac{q^m-1}{\lambda}$, where q is a prime power, m is a positive integer, and λ is a divisor of $q-1$. This family includes primitive BCH codes (i.e., $\lambda = 1$) as a special case. The main contributions are as follows.

- We determine the dimension and Bose distance of narrow-sense primitive BCH codes for $m \geq 4$ and designed distance $\delta \in \left[2, q^{\lfloor (2m-1)/3 \rfloor + 1}\right]$.

- We determine the dimension of narrow-sense BCH codes of length $\frac{q^m-1}{\lambda}$ for $m \geq 4$ and designed distance $\delta \in \left[2, \frac{q^{\lfloor (2m-1)/3 \rfloor+1}-1}{\lambda}+1\right]$.

- We determine the Bose distance of narrow-sense BCH codes of length $\frac{q^m-1}{\lambda}$ for $m \geq 4$ and designed distance $\delta \in \left[2, \frac{q^{\lfloor (2m-1)/3 \rfloor+1}-1}{\lambda}\right]$.

- As illustrations of our main results, we provide the dimension and Bose distance of BCH codes of length $\frac{q^m-1}{\lambda}$ for $m \geq 4$ and designed distance δ such that $\lambda\delta = aq^{h+k}+b$, where $h = \lfloor \frac{m}{2} \rfloor$, $m-2h \leq k \leq \lfloor (2m-1)/3 \rfloor - h$, $1 \leq a \leq q-1$, $\lambda \leq b \leq q^{m-h-k}$ and $q \nmid b$.

- We extend the results on narrow-sense BCH codes to some non-narrow-sense BCH codes of length $\frac{q^m-1}{\lambda}$.

- Using the formulas provided in our main theorems, we have identified several BCH codes that are either optimal or possess the best-known parameters compared with the tables of best-known linear codes maintained by Markus Grassl at http://www.codetables.de.

1.3 Organization

This thesis is structured into six chapters, systematically progressing from preliminary concepts to specific theoretical contributions and concluding with future research directions.

- Chapter 2. This chapter introduces the necessary preliminaries for the study, covering fundamental concepts such as communication channel models, core algebraic structures as well as an overview of error correction codes, linear codes, and cyclic codes. Finally, it provides a concise introduction to BCH codes, thereby laying the groundwork for the discussion in the subsequent chapters.

- Chapter 3. The dimension and Bose distance of BCH codes are fundamentally determined by its defining set, which is a union of some q-cyclotomic cosets. This chapter presents some results on the sizes and coset leaders of q-cyclotomic cosets modulo n, particularly for $n = q^m - 1$. These results provide the critical tools required for the determination of parameters of BCH codes in the following chapters.

- Chapter 4. Building on the results of Chapter 3, this chapter focuses on primitive BCH codes, i.e., BCH codes of length $q^m - 1$. Explicit formulas are derived for the dimension and Bose distance for a wide range of designed distances δ. The results are further illustrated for a specific family of BCH codes with designed distances of the form $\delta = aq^{h+k} + b$, where $h = \lfloor \frac{m}{2} \rfloor, m - 2h \leq k \leq \lfloor (2m-1)/3 \rfloor - h$, $1 \leq a \leq q - 1$, $1 \leq b \leq q^{m-h-k}$ and $q \nmid b$.

- Chapter 5. This chapter generalizes the results of Chapter 4 to BCH codes of length $\frac{q^m-1}{\lambda}$, where λ is a divisor of $q - 1$. The results are again illustrated for designed distances δ such that $\lambda\delta$ takes a specific form.

- Chapter 6. The final chapter provides a summary of the thesis and outlines some potential directions for future research.

Chapter 2

Preliminaries and fundamental concepts

2.1 Communication channel

In real world applications, information media, such as communication systems and data storage devices, are often affected by noise and various types of interference, which can undermine their reliability. Coding theory plays a crucial role in addressing these challenges by providing techniques for detecting and, when possible, correcting errors. Coding strategies are typically divided into two main categories: *source coding* and *channel coding*. Source coding involves converting the original message into an encoded format that facilitates efficient transmission over a communication channel.

In classical information theory, messages are usually represented as sequences of digits. One prominent example of source coding is the ASCII encoding scheme, which assigns each character a unique sequence of 8 binary digits. The basic structure of a communication system that utilizes these concepts is depicted in the following figure.

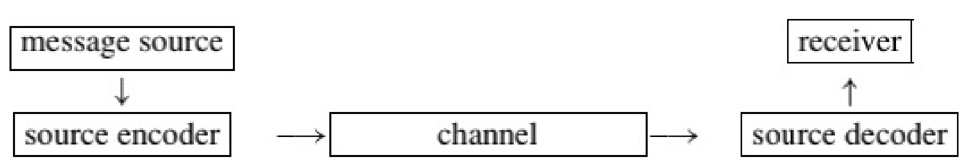
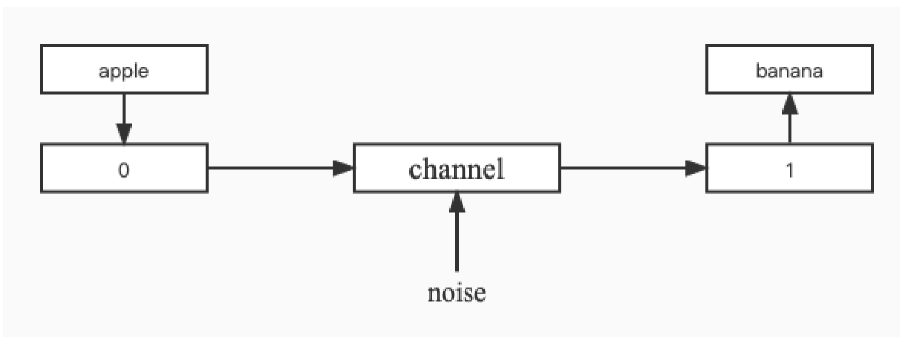


Figure 2.1: Communication without channel coding [37, Figure 1.1]

Example 2.1. *Consider the source encoding of two fruits, apple and banana, as follows:*

$$\text{apple} \to 0 \quad \textit{and} \quad \text{banana} \to 1.$$

Suppose the message "apple" is encoded as the digit "0" for transmission over a noisy channel. Due to channel noise, a single error may occur, altering the transmitted "0" to "1". Upon receiving "1", the decoder, lacking error detection capability, interprets it as a valid message without recognizing the corruption. Consequently, the communication fails. This process is illustrated in the figure below.



To mitigate the transmission errors introduced by channel noise, the channel coding is applied after source coding. The core principle of channel coding is to embed carefully designed redundancy into the data stream. This extra information allows the receiver to detect and correct certain errors arising during transmission. A revised communication model that includes a channel encoder is illustrated in the figure below.

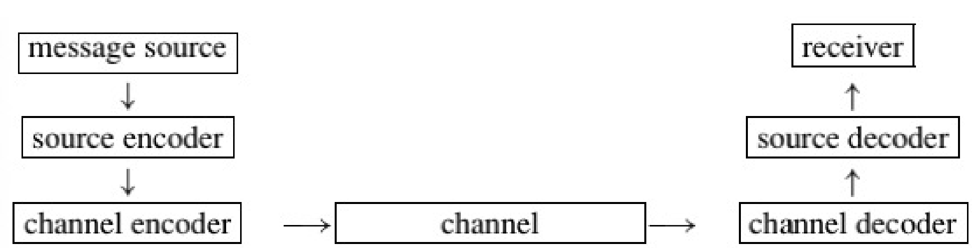
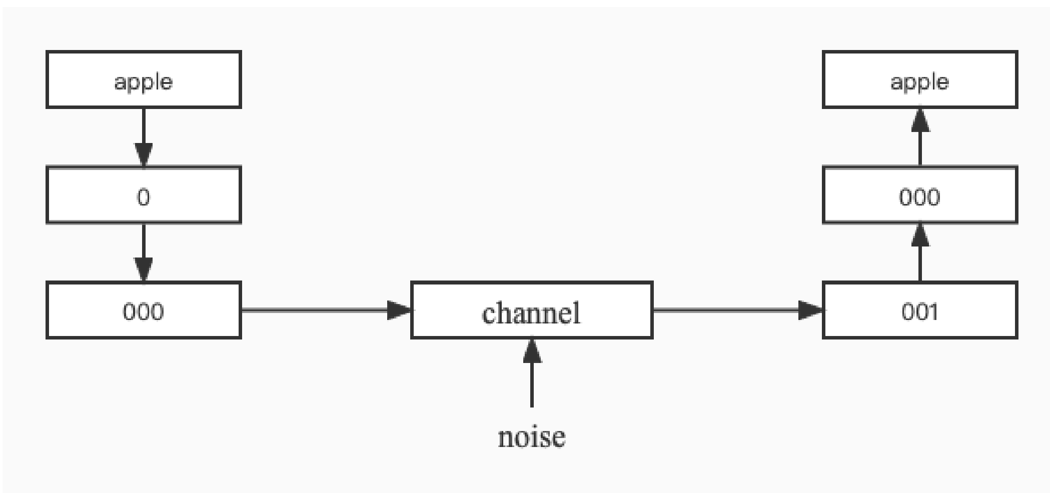


Figure 2.2: Communication with channel coding [37, Figure 1.3]

Example 2.2. *Consider the channel coding as follows:*

$$0 \to 000 \quad \textit{and} \quad 1 \to 111.$$

Suppose that the message 'apple', which is encoded as 000 *after the source and channel encoding, is transmitted over a noisy channel, and that only one digit error occurs. Then the received word must be one of the following three: 100, 010 or 001. In this way, we can detect the error, as none of 100, 010 or 001 is among our encoded messages. The whole process can be represented as follows.*



In the preceding example, the digit "0" is transmitted as the sequence "000," providing protection against one digit error. This strategy is reminiscent of ordinary conversation: when we doubt we have been heard correctly, we simply repeat ourselves.

Increasing the number of repetitions naturally boosts error tolerance. More precisely, in a later section, we will see that if each digit is repeated r times, the receiver can correct up to $\lfloor \frac{r-1}{2} \rfloor$ digit errors. Codes built on this idea are called *repetition codes*. Although repetition codes are easy to understand and implement, they are extremely inefficient in terms of information rate.

To construct more efficient codes, a range of mathematical tools, including algebra, combinatorics, and finite field theory are necessary. In the following sections, we first introduce fundamental algebraic concepts, then provide a rigorous definition of error correction codes over finite fields, and describe key parameters used to evaluate their performance. Finally, we give a brief overview of linear codes, cyclic codes, and BCH codes.

2.2 Algebraic preliminaries

Algebra underpins much of coding theory. Many powerful families of codes arise from explicit algebraic constructions. To set the stage for our treatment of error correction codes in the thesis that follows, we begin with a concise survey of the necessary algebraic concepts, including groups, rings, fields, and finite fields.

Group

Definition 2.1. *A* group *is a nonempty set G equipped with a binary operation, namely multiplication $\cdot : G \times G \longrightarrow G$ satisfying the following axioms:*

1. *Associativity. For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*
2. *Identity element. There exists an element $e \in G$ such that for every $a \in G$, $a \cdot e = e \cdot a = a$.*
3. *Inverse element. For every $a \in G$, there exists an element $b \in G$ such that $a \cdot b = b \cdot a = e$. The element b is called the* inverse *of a, denoted by a^{-1}.*

In addition, if the multiplication is commutative, i.e.,

$$a \cdot b = b \cdot a \quad \text{for all } a, b \in G,$$

then $(G, \cdot)$ is called an Abelian *or* commutative *group.*

Let G be a group. The number of elements in G is called the *order* of G, denoted by $|G|$. If $|G|$ is infinite, then G is called an *infinite group*; otherwise, G is called a *finite group*. One subset $S \subseteq G$ is called a *subgroup* if S is also a group under the operation inherited from G. The following is a fundamental result regarding the orders of a finite group and its subgroups.

Theorem 2.1 (Lagrange's Theorem)**.** *Let G be a finite group and let H be a subgroup of G. Then the order of H divides the order of G.*

Denote by $\mathbb{Z}$ and $\mathbb{Z}^*$ the sets of all integers and all positive integers, respectively. Suppose that G is a group and $a \in G$. For simplicity, we denote by a^n the product of n copies of a, i.e.,

$$a^n = \underbrace{a \cdot a \cdot \cdots \cdot a}_{n \text{ copies}} \quad \text{for } n \in \mathbb{Z}^*.$$

We also define

$$a^0 = e,$$

$$a^{(-n)} = (a^{-1})^n \quad \text{for } n \in \mathbb{Z}^*.$$

The smallest integer $n \in \mathbb{Z}^*$ such that $a^n = e$ is called the order of a, denoted by $|a|$.

One special type of group is the *cyclic group*, which is defined as follows.

Definition 2.2. *A group G is called a* cyclic group *if there exists an element $a \in G$ such that*

$$G = \{ a^n \mid n \in \mathbb{Z}\}.$$

The element a is then called a generator *of G, and we denote $G = \langle a \rangle$.*

For a finite cyclic group $G = \langle a \rangle$, we have

$$|a^k| = \frac{|G|}{\gcd(|G|, k)} \quad \text{for all } k \in \mathbb{Z}^*,$$

where gcd denotes the greatest common divisor.

Ring

Definition 2.3. *A* ring *is a non-empty set R equipped with two binary operations, namely addition $+ : R \times R \to R$ and multiplication $\cdot : R \times R \to R$ satisfying the following axioms:*

1. *$(R, +)$ is an Abelian group with an additive identity 0.*

2. *Multiplicative associativity. For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.*

3. *Multiplication distributes over addition on both the left and right. That is, for all $a, b, c \in R$,*

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \textit{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

In addition, if the multiplication is commutative, i.e.,

$$a \cdot b = b \cdot a \quad \textit{for all } a, b \in R,$$

then the ring R is called a commutative ring*; if there exists a multiplicative identity element $1 \in R$ such that*

$$1 \cdot a = a \cdot 1 = a \quad \textit{for all } a \in R,$$

then R is called a ring with unity*, and the multiplicative identity element 1 is called the* unity *of R.*

Let R be a ring with unity. An element $a \in R$ is said to be invertible *if there exists $b \in R$ such that $a \cdot b = b \cdot a = 1$. The element b is called the* inverse *of a, denoted by a^{-1}.*

Common examples of rings include the ring of integers $\mathbb{Z}$, which is a commutative ring with unity; the polynomial ring over the integers $\mathbb{Z}[x]$, which is a commutative ring with unity; and the real matrix ring $M_n(\mathbb{R})$, consisting of all real $n \times n$ matrices, which is non-commutative and has the identity matrix I_n as its unity.

Suppose that n is a positive integer. Another example is $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ equipped with addition "+" and multiplication "·" defined as

$$a + b = (a + b) \bmod n \quad \text{and} \quad a \cdot b = (ab) \bmod n. \tag{2.1}$$

This is a commutative ring with 1 as its unity.

Let R be a ring. A subset $S \subseteq R$ is called a *subring* of R if S is also a ring equipped with the multiplication and addition inherited from R. For example, the ring of integers $\mathbb{Z}$ is indeed a subring of the polynomial ring over the integers $\mathbb{Z}[x]$.

For an element $a \in R$, we denote by $-a$ its additive inverse. Define subtraction "$-$" in R as

$$a - b = a + (-b) \quad \text{for all } a, b \in R.$$

An *ideal* is another special type of subset of a ring, defined as follows.

Definition 2.4. *Let R be a ring. A non-empty subset $I \subseteq R$ is called an* ideal *of R if it satisfies the following two conditions:*

1. *I is closed under subtraction, i.e., $a - b \in I$ for any $a, b \in I$; This is equivalent to that I is an additive subgroup of R.*

2. *I is absorbing with respect to multiplication, i.e.,*

$$r \cdot a \in I \quad \textit{and} \quad a \cdot r \in I \quad \textit{for all } a \in I, r \in R.$$

Note that the intersection of any collection of ideals of a ring R is still an ideal of R. Suppose $S \subseteq R$ is a non-empty subset of the ring R. The intersection of all ideals of R that contain S is called the *ideal generated by S*, denoted by (S). In particular, if an ideal I of R is generated by a single element $a \in R$, then I is called a *principal* *ideal*, denoted by $I = (a)$. If every ideal of R is a principal ideal, then R is called a *principal ideal ring*.

Proposition 2.1. *Let R be a commutative ring with unity and $a \in R$ be an element. Then the set*

$$aR = \{\, ar \mid r \in R \,\}$$

is the principal ideal of R generated by a; therefore, it can be denoted by (a).

For example, the polynomial ring $F[x]$ over a field F is a commutative ring with unity. Therefore, the set

$$f(x)F[x] = \{f(x)g(x) \mid g(x) \in F[x]\} \tag{2.2}$$

is the principal ideal generated by $f(x)$; hence it can be denoted by $(f(x))$.

In addition, the ring of integers $\mathbb{Z}$ is also a commutative ring with unity. Hence, for any integer $n \in \mathbb{Z}$, the set

$$n\mathbb{Z} \;=\; \{\, na \mid a \in \mathbb{Z} \,\} \tag{2.3}$$

is the principal ideal of $\mathbb{Z}$ generated by n.

Definition 2.5. *Let R be a ring and $I \subseteq R$ be an ideal of R. Denote by R/I the set of all additive cosets of I in R , i.e.,*

$$R/I = \{\overline{r} : r \in R\},$$

where $\overline{r} = r + I = \{r + i : i \in I\}$ is the residue class of r. Define addition and multiplication on R/I as

$$\overline{r_1} + \overline{r_2} = \overline{r_1 + r_2}, \qquad \overline{r_1} \cdot \overline{r_2} = \overline{r_1 \cdot r_2} \quad \textit{for all } \overline{r_1}, \overline{r_2} \in R/I.$$

Then R/I is a ring equipped with the above operators, called the quotient ring *of R modulo I.*

We have the following properties of quotient rings.

Proposition 2.2. *Let R be a ring and $I \subseteq R$ be an ideal of R.*

- *If R is a ring with 1 as its unity, then R/I is a ring with $\overline{1} = 1 + I$ as its unity.*
- *If R is a commutative ring, then R/I is also a commutative ring.*
- *If R is a principal ideal ring, then R/I is also a principal ideal ring.*

Recall that $\mathbb{Z}$ is a commutative ring with 1 as its unity and the set $n\mathbb{Z}$ defined in (2.3) is an ideal of $\mathbb{Z}$. Hence the quotient $\mathbb{Z}/n\mathbb{Z}$ is a commutative ring with $\overline{1} = 1+n\mathbb{Z}$ as its unity. Moreover, one can verify that $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to $\mathbb{Z}_n$ defined in (2.1), denoted as $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Field

Definition 2.6. *A* field *is a non-empty set F equipped with two binary operators, namely addition $+ : F \times F \to F$ and multiplication $\cdot : F \times F \to F$ satisfying the following axioms:*

1. *$(F, +)$ is an Abelian group with additive identity element 0.*
2. *$(F \setminus \{0\}, \cdot)$ is an Abelian group.*
3. *Multiplication distributes over addition on both the left and right, i.e.,*

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad \text{and} \quad (a + b) \cdot c = a \cdot c + b \cdot c \quad \text{for all } a, b, c \in F.$$

Equivalently, a field is a commutative ring with unity in which every element $a \neq 0$ is invertible. In addition, if a field F contains finitely many elements, then F is called a finite field *or* Galois field.

Common examples of fields include the field of rational numbers $\mathbb{Q}$, the field of real numbers $\mathbb{R}$, and the field of complex numbers $\mathbb{C}$. We have already known that $\mathbb{Z}_n \cong \mathbb{Z}/n\mathbb{Z}$ is a commutative ring with unity for any integer $n \in \mathbb{Z}$. Furthermore, by elementary number theory, one can show that when p is prime, every nonzero element in $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ is invertible. Thus, $\mathbb{Z}_p \cong \mathbb{Z}/p\mathbb{Z}$ is a field if p is prime.

Let E be a field. A subset F of E is called a *subfield* of E if F is a field under the operations inherited from E. In this case, we say that E is an *extension field* of F, and this pair of fields is a *field extension* , denoted by E/F. For an element $a \in E$, we denote by $n \cdot a$ the sum of n copies of a. In particular, we denote by n the sum of n copies of the multiplicative identity $1 \in E$. The smallest positive integer n such that $n = 0$ is called the *characteristic* of E, denoted by $\mathrm{Char}(E)$. If no such integer n exists, the characteristic of E is defined to be 0. It is clear that if a field has characteristic 0, then it must be an infinite field. Moreover, we will see later that the characteristic of a finite field must be a prime number.

Suppose that E/F is a field extension. Then the addition in E and the scalar multiplication by elements of F satisfy the axioms of a linear space. Therefore, the field E can be regarded as a linear space over F. The *degree* of the field extension E/F, denoted by $[E : F]$, is defined to be the dimension of this linear space. If this dimension is finite, the field extension E/F is called a *finite extension*; otherwise, it is an *infinite extension.*

For example, the field of complex numbers $\mathbb{C}$ is an extension field of the field of real numbers $\mathbb{R}$. Moreover, since $\mathbb{C}$ can be seen as a 2-dimensional linear space over $\mathbb{R}$ with a basis $\{1, \mathbf{i}\}$, we also have $[\mathbb{C} : \mathbb{R}] = 2$.

To further discuss field extensions, we present the following definitions.

Definition 2.7. *Let E/F be a field extension and let $a \in E$ be an element.*

- *A non-constant polynomial $f(x) \in F[x]$ is said to be* irreducible *over F if it* *cannot be factored into a product of two non-constant polynomials in $F[x]$.*

- *The element a is said to be* algebraic over F *if there exists a non-zero polynomial $f(x) \in F[x]$ such that $f(a) = 0$.*

- *If the element a is algebraic over F, then the monic irreducible polynomial $m(x) \in F[x]$ such that $m(a) = 0$ is said to be the* minimal polynomial of a over F.

Let E/F be a field extension and let $a \in E$ be algebraic over F. Define

$$F(a) = \{\, f(a) \mid f(x) \in F[x]\}.$$

Then the set $F(a)$ is a field, and hence an extension field of F, under the operations inherited from E. Moreover, the following theorem describes the degree of the field extension $F(a)/F$.

Theorem 2.2. *Let E/F be a field extension. Suppose that $a \in E$ is algebraic over F and $m(x) \in F[x]$ is the minimal polynomial of a over F. Then*

$$[F(a) : F] = \deg m(x).$$

For example, the minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$. As a linear space over $\mathbb{Q}$, the field

$$\mathbb{Q}(\sqrt{2}) = \{\, a + b\sqrt{2} \mid a, b \in \mathbb{Q}\,\}$$

has a basis $\{1, \sqrt{2}\}$. Therefore, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, which is equal to the degree of $x^2 - 2$.

Another useful result concerning field extension is stated below.

Theorem 2.3 (Lagrange's Formula)**.** *Let F, K, E be three fields such that $F \subseteq K \subseteq E$. Then E/F is a finite extension if and only if both E/K and K/F are finite extensions. In this case, the degrees of these field extensions satisfy*

$$[E : F] = [E : K] \cdot [K : F].$$

Finite fields.

We know that a finite field is a field with finitely many elements, and we have also seen that $\mathbb{Z}_p$ is a finite field of p elements for any prime number p. We now introduce further properties of finite fields.

Suppose that F is a finite field with $\mathrm{Char}(F) = p$. Denote by 1_F the multiplicative identity of F. If p is not prime, then there exist positive integers $a > 1, b > 1$ such that $ab = p$. This implies

$$(a \cdot 1_F) \cdot (b \cdot 1_F) = (ab) \cdot 1_F = 0.$$

Hence, we have $a \cdot 1_F = 0$ or $b \cdot 1_F = 0$ in F. This is contrary to that $\mathrm{Char}(F) = p$ is the smallest positive integer such that $p \cdot 1_F = 0$. So we can conclude that p must be a prime number. In this case, $\mathbb{Z}_p$ defined in (2.1) is a field. Define a map

$$f : \mathbb{Z}_p \to F, \quad n \mapsto n \cdot 1_F,$$

This map is an injective ring homomorphism. Therefore, $\mathbb{Z}_p$ can be identified with a subfield of F. It follows that $|F| = p^m$, where $m = [F : \mathbb{Z}_p]$ is the degree of the field extension.

We summarize this property as follows.

Proposition 2.3. *Let F be a finite field. Then $\mathrm{Char}(F) = p$ for some prime number p, and the order of F is given by $|F| = p^m$ for some positive integer m.*

A natural question arises: Given a prime power p^n does there exist a finite field F such that $|F| = p^n$? The answer is yes. Moreover, the field of order p^n is unique up to isomorphism, as stated in the following two theorems:

Theorem 2.4. [29, Theorem 1.1] *Let p be a prime number and n be a positive integer. The splitting field of $x^{p^n} - x \in \mathbb{Z}_p[x]$ has exactly p^n elements.*

Theorem 2.5. [29, Theorem 1.2] *Given a prime p and an integer $n > 0$, all finite fields of order p^n are isomorphic.*

The two theorems above together guarantee the existence and uniqueness (up to isomorphism) of a finite field of order q for any prime power q. Therefore, we may unambiguously denote such a field by $\mathbb{F}_q$, where q is a prime power. Throughout the remainder of this thesis, we always assume that q is a prime power.

Additional results concerning finite fields that will be used later are stated below.

Theorem 2.6. [29, Theorem 1.3] *The multiplicative group $\mathbb{F}_{p^n}^* = \mathbb{F}_{p^n} \setminus \{0\}$ is a cyclic group.*

A generator of $\mathbb{F}_{p^n}^*$ is called a *primitive element* of $\mathbb{F}_{p^n}$.

Lemma 2.1. [29, Proposition 2.4] *Let $\alpha \in \mathbb{F}_{q^m}$ and $g(x)$ be the minimal polynomial of α over $\mathbb{F}_q$. Then*

$$g(x) = (x - \alpha)(x - \alpha^q) \cdots (x - \alpha^{q^{l-1}}),$$

where l is the smallest integer such that $\alpha^{q^l} = \alpha$.

Remark 2.1. *Notice $\deg(g(x)) = l$. By Theorem 2.2, this implies $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = l$. By Theorem 2.3, we also have $[\mathbb{F}_{q^m} : \mathbb{F}_q(\alpha)] \cdot [\mathbb{F}_q(\alpha) : \mathbb{F}_q] = [\mathbb{F}_{q^m} : \mathbb{F}_q] = m$. Therefore, the integer l divides m.*

2.3 Error correction codes over finite fields

In this thesis, we restrict our attention to error correction codes over finite fields, that is, codes whose alphabet is a finite field. This section reviews the basic concepts for such codes, including their definitions, parameters, and several bounds on these parameters.

Definition 2.8. *Let q be a prime power and $\mathbb{F}_q^n$ denote the n-dimensional vector space over $\mathbb{F}_q$.*

i. *A q-ary code $\mathcal{C}$ of length n over $\mathbb{F}_q$ is a non-empty subset of $\mathbb{F}_q^n$.*

ii. *An element of $\mathcal{C}$ is called a codeword in $\mathcal{C}$.*

iii. *The number of codewords in $\mathcal{C}$, denoted by $|\mathcal{C}|$, is called the size of $\mathcal{C}$.*

In what follows, a q-ary code is always understood to be a code over $\mathbb{F}_q$. Consequently, we will simply write "a q-ary code" instead of "a q-ary code over $\mathbb{F}_q$."

The length and size of a code can be viewed, respectively, as the resources it requires and the amount of information it can carry. A q-ary code of length n and size K is called an $(n, K)_q$ code or, equivalently, an $[n, k]_q$ code with $k = \log_q K$. An $[n, k]_q$ code can be intuitively understood as using n symbols over $\mathbb{F}_q$ to transmit k symbols over $\mathbb{F}_q$ of information. Therefore, the parameter k is also referred to as the number of information bits. For example, the code $\{000, 111\}$ introduced earlier is a $(3, 2)_2$ code, or equivalently, an $[3, 1]_2$ code. When this code is used, a single bit of information is transmitted using three bits.

In addition to the length and size of a code, the minimum distance is another fundamental parameter of a code.

Definition 2.9. *Let $c = (c_1, \ldots, c_n), c = (c'_1, \ldots, c'_n) \in \mathbb{F}_q^n$.*

- *The* Hamming weight *of c, denoted by $w(c)$, is defined by

$$w(c) = \Big|\{\ i \mid 1 \leq i \leq n \text{ and } c_i \neq 0\ \}\Big|.$$

- *The distance from c to c', denoted by $d(c, c')$ is defined by*

$$d(c, c') = \Big|\{\ i \mid 1 \leq i \leq n \text{ and } c_i \neq c'_i\ \}\Big|.$$

It is clear that $d(c, c') = w(c - c')$. Let $u, v, w \in \mathbb{F}_q^n$. One can verify that the Hamming distance has the following three properties:

Definiteness: $d(u, v) \geq 0$, and $d(u, v) = 0$ if and only if $u = v$;

Symmetry: $d(u, v) = d(v, u)$;

Triangle inequality: $d(u, w) + d(w, v) \geq d(u, v)$.

Definition 2.10 (Minimum distance)**.** *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a q-ary code. The* minimum distance *of $\mathcal{C}$, denoted by $d(\mathcal{C})$, is defined by*

$$d(\mathcal{C}) = \min\{d(c, c') \mid c, c' \in \mathcal{C} \textit{ and } c \neq c'\}.$$

Or equivalently,

$$d(\mathcal{C}) = \min\{w(c - c') \mid c, c' \in \mathcal{C} \textit{ and } c \neq c'\}. \tag{2.4}$$

One natural question is: *What kind of errors can a given error correction code $\mathcal{C} \subseteq \mathbb{F}_q^n$ detect or correct?* Mathematically, an error can be represented by a nonzero vector $\mathcal{E} \in \mathbb{F}_q^n$ that corrupts a transmitted codeword $c \in \mathcal{C}$, resulting in the received word $c + \mathcal{E}$. Suppose a codeword $c \in \mathcal{C}$ is transmitted through a communication channel, but due to errors in the channel, the received word is c', which is a vector in $\mathbb{F}_q$ and not equal to c. There are two possible scenarios:

1. $c' \notin \mathcal{C}$: In this case, the receiver can detect the presence of the error, since c' is not a valid codeword.

2. $c' \in \mathcal{C}$: In this case, the receiver cannot determine whether an error occurred during transmission, as the received word is still a valid codeword.

From the above, we can see that a non-zero vector $\mathcal{E} \in \mathbb{F}_q^n$ is an undetectable error by $\mathcal{C}$ if and only if $\mathcal{E} = c^{'} - c$ for some distinct codewords $c^{'}, c \in \mathcal{C}$. Recall equation (2.4).

Therefore, the minimum distance of $\mathcal{C}$ is exactly the minimum Hamming weight of undetectable errors by $\mathcal{C}$, that is,

$$d(\mathcal{C}) = \min\{w(\mathcal{E}) \mid \mathcal{E} \in \mathbb{F}_q^n \text{ is an undetectable error by } \mathcal{C}\}.$$

This means that the code $\mathcal{C}$ can detect any error of Hamming weight at most $d(\mathcal{C})-1$. Furthermore, the minimum distance also determines its error-correcting ability as shown by the following theorem. It can be easily derived by the triangle inequality property of the Hamming distance.

Theorem 2.7. *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a q-ary code with minimum distance d. Then $\mathcal{C}$ can correct any error of Hamming weight at most $\lfloor \frac{d-1}{2} \rfloor$.*

We have introduced the parameters of a code, including its length, size and minimum distance. For simplicity, if a q-ary code is of length n, size K and minimum distance d, then it is said to be an $(n, K, d)_q$ code or an $[n, k, d]_q$ code with $k = \log_q K$. The main goal in code design is to construct codes that require fewer resources, is to design efficient codes, that is, codes that require fewer resources, convey more information, and can correct more errors. If we momentarily ignore the complexity of encoding and decoding, the discussion above shows that this goal translates into reducing the length n, while increasing both the size K and the minimum distance d of a code. However, these parameters are mutually constrained and must satisfy certain bounds, such as the Hamming bound and Singleton bound, as follows.

Theorem 2.8 (Hamming Bound)**.** *If an $(n, K, d)_q$ code exists, then*

$$q^n \ \le\ K \sum_{i=0}^{\lfloor (d-1)/2 \rfloor} (q-1)^i \binom{n}{i}. \tag{2.5}$$

The Hamming bound is also called the *sphere-packing bound*, which was first derived by Hamming in 1950. A code that meets the Hamming bound, i.e., one for which equality holds in (2.5), is called a *perfect code.*

Theorem 2.9 (Singleton Bound)**.** *If an* $[n,k,d]_q$ *code exists, then*

$$n \ \geq \ k+d-1. \tag{2.6}$$

A code that meets the Singleton bound, i.e., one for which $n = k+d-1$, is called a *maximum distance separable* (MDS) code.

Definition 2.11. *An* $[n,k,d]_q$ *code is called* optimal *if there is no* $[n,k',d]_q$ *linear code with* $k' > k$*, or no* $[n,k,d']_q$ *linear code with* $d' > d$*.*

It is clear that both perfect codes and MDS codes are optimal.

2.4 Linear codes

Linear codes form the most widely studied family of error correction codes. They admit a compact algebraic description as follows.

Definition 2.12. *A* q*-ary code* $\mathcal{C} \subseteq \mathbb{F}_q^n$ *is called a* linear code *if* $\mathcal{C}$ *is a linear subspace of* $\mathbb{F}_q^n$*.*

Assume $\mathcal{C}$ is a linear code. By its linearity, we have $c - c' \in \mathcal{C}$ for any two distinct codewords $c, c' \in \mathcal{C}$. Hence,

$$\begin{aligned} d(\mathcal{C}) &= \min\big\{\, d(c,c') \ \big|\ c,c' \in \mathcal{C},\ c \neq c' \big\} \\ &= \min\big\{\, w(c-c') \ \big|\ c,c' \in \mathcal{C},\ c \neq c' \big\} \\ &= \min\big\{\, w(c) \ \big|\ c \in \mathcal{C},\ c \neq 0 \big\}. \end{aligned}$$

That is, the minimum distance of $\mathcal{C}$ is equal to the minimum weight of nonzero codewords in $\mathcal{C}$. If $\mathcal{C}$ has dimension k, denoted by $\dim(\mathcal{C}) = k$, then $|\mathcal{C}| = q^k$; hence $\mathcal{C}$ is an $[n,k]_q$ code. We usually quote its dimension instead of its size when discussing the parameters of a linear code.

Suppose that $\dim(\mathcal{C}) = k$. Choose a basis $\{v_1, v_2, \dots, v_k\}$ of $\mathcal{C}$, where

$$v_i = (a_{i1}, a_{i2}, \dots, a_{in}), \qquad a_{ij} \in \mathbb{F}_q.$$

Let

$$G = \begin{bmatrix} v_1 \\ v_2 \\ \vdots \\ v_k \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{k1} & a_{k2} & \cdots & a_{kn} \end{bmatrix}.$$

Then each codeword $c \in \mathcal{C}$ can be represented uniquely as

$$c = b_1 v_1 + b_2 v_2 + \cdots + b_k v_k = (b_1, b_2, \dots, b_k)\, G, \qquad b_i \in \mathbb{F}_q.$$

The matrix G is called a *generator matrix* of the linear code $\mathcal{C}$.

Let $\mathcal{C}^{\perp}$ denote the orthogonal complement of $\mathcal{C}$, i.e.,

$$\mathcal{C}^{\perp} = \left\{ u \in \mathbb{F}_q^n | u^T v = 0 \text{ for all } v \in \mathcal{C} \right\}.$$

It is clear that $\mathcal{C}^{\perp}$ is also a linear subspace of $\mathbb{F}_q^n$, thus a q-ary linear code of length n. The dimension of $\mathcal{C}^{\perp}$ is $n-k$. Choose a basis $\{u_1, u_2, \dots, u_{n-k}\}$ of $\mathcal{C}^{\perp}$, where

$$u_i = (b_{i1}, b_{i2}, \dots, b_{in}), \quad b_{ij} \in \mathbb{F}_q.$$

Let

$$H = \begin{bmatrix} u_1 \\ u_2 \\ \vdots \\ u_{n-k} \end{bmatrix} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & & \vdots \\ b_{n-k,1} & b_{n-k,2} & \cdots & b_{n-k,n} \end{bmatrix}.$$

Then $c = (c_{n-1}, c_{n-2}, \dots, c_0) \in \mathcal{C}$ if and only if

$$Hc^T = 0.$$

The matrix H is said to be a *parity-check matrix* of $\mathcal{C}$. From the definition, we can easily see that H and G are a generator matrix and a parity-check matrix of $C^{\perp}$, respectively.

The following theorem gives a useful way to find the minimum distance of a linear code from its parity-check matrix.

Theorem 2.10. [37, Corollary 4.5.7] *Let $\mathcal{C}$ be an $[n,k]_q$ linear code with a parity-check matrix H. Then the minimum distance of $\mathcal{C}$ is equal to d if and only if any set of $d-1$ columns of H is linearly independent, and there exists a set of d columns of H that is linearly dependent.*

2.5 Cyclic codes

Cyclic codes constitute a fundamental class of linear codes with widespread applications in both theory and practice. One of their key advantages lies in their algebraic structure, which allows for efficient encoding and decoding procedures using shift registers and simple logic circuits, thanks to their representation as ideals over the quotient ring $\mathbb{F}_q[x]/(x^n-1)$. This efficiency makes cyclic codes particularly attractive for implementation in hardware and real-time systems.

Several prominent families of error correction codes, such as the binary Hamming codes, BCH codes, Reed–Solomon codes, and quadratic residue codes, are either cyclic or closely related to cyclic codes.

In this section, we introduce basic concepts about cyclic codes. We first introduce some fundamental facts about the structure of the polynomial ring $\mathbb{F}_q[x]$ and its quotient rings, which play a central role in the algebraic description of cyclic codes. Let $f(x) \in \mathbb{F}_q[x]$ be a nonzero polynomial over the finite field $\mathbb{F}_q$. Recall equation (2.2). We know that

$$(f(x)) = \{f(x)g(x) \mid g(x) \in \mathbb{F}_q[x]\}$$

is a principal idea of $\mathbb{F}_q[x]$. Therefore, we have the quotient ring $\mathbb{F}_q[x]/(f(x))$. Moreover, it is straightforward to verify that every element in the quotient ring

$\mathbb{F}_q[x]/(f(x))$ has a unique representative of degree less than $\deg f(x)$. Consequently, in the following discussion, we shall simply identify each element in $\mathbb{F}_q[x]/(f(x))$ with its unique polynomial representative whose degree is less than $\deg f(x)$. In this way, we have the following result regarding ideals of $\mathbb{F}_q[x]/(f(x))$.

Theorem 2.11. *Let $f(x) \in \mathbb{F}_q[x]$ be a nonzero polynomial and I be an ideal of the quotient ring $\mathbb{F}_q[x]/(f(x))$. Then there exists a unique monic polynomial $g(x)$ such that $g(x)$ divides $f(x)$, denoted by $g(x) \mid f(x)$, and*

$$I = (g(x)) \ = \ \{g(x)\, h(x) : h(x) \in \mathbb{F}_q[x]/(f(x))\}\,. \tag{2.7}$$

Proof. Note that $\mathbb{F}_q[x]$ is a principal ideal ring. By Proposition 2.2, we can conclude that the quotient ring $\mathbb{F}_q[x]/(f(x))$ is also a principal ideal ring. This implies that I is a principal ideal. Therefore, there exists a monic polynomial $g(x)$ such that (2.7) holds.

We now show that $g(x)$ divides $f(x)$. By the division theorem, there exist polynomials $h(x), r(x) \in \mathbb{F}_q[x]$ such that $\deg r(x) < \deg g(x)$ and

$$f(x) = g(x)h(x) + r(x).$$

It follows that

$$r(x) = f(x) - g(x)h(x).$$

Note that $f(x)$ is the zero element in $\mathbb{F}_q[x]/(f(x))$. Therefore, we have $r(x) \in (g(x))$. Since $\deg r(x) < \deg g(x)$, this implies that $r(x) = 0$. Consequently, $g(x) \mid f(x)$.

Finally, suppose that there exists a monic polynomial $g^{'}(x)$ such that $(g(x)) = (g^{'}(x))$. Then we have $g(x) \mid g^{'}(x)$ and $g^{'}(x) \mid g(x)$. Since both polynomials are monic, it follows that $g(x) = g^{'}(x)$. This shows the uniqueness of $g(x)$. $\square$

We now give the definition of a cyclic code.

Definition 2.13. *A q-ary code $\mathcal{C} \subseteq \mathbb{F}_q^n$ is said to be a* cyclic code *if*

(1) $\mathcal{C}$ is a linear code, i.e., $\mathcal{C}$ is a linear subspace of $\mathbb{F}_q^n$; and

(2) $(c_{n-1}, c_{n-2}, \ldots, c_0) \in \mathcal{C}$ implies $(c_{n-2}, \ldots, c_0, c_{n-1}) \in \mathcal{C}$.

The quotient ring $\mathbb{F}_q[x]/(x^n - 1)$, equipped with the addition inherited from $\mathbb{F}_q[x]/(x^n - 1)$ and scalar multiplication by elements of $\mathbb{F}_q$, forms a vector space isomorphic to $\mathbb{F}_q^n$. Therefore, each vector $c = (c_{n-1}, c_{n-2}, \ldots, c_0) \in \mathbb{F}_q^n$ can be identified with its polynomial representation

$$c(x) = c_{n-1}x^{n-1} + c_{n-2}x^{n-2} + \cdots + c_0 \in \mathbb{F}_q[x]/(x^n - 1),$$

and a q-ary code $\mathcal{C} \subseteq \mathbb{F}_q^n$ can be identified with a subset of the quotient ring $\mathbb{F}_q[x]/(x^n - 1)$.

Suppose that $\mathcal{C} \subseteq \mathbb{F}_q[x]/(x^n - 1)$ is a cyclic code. Then $\mathcal{C}$ satisfies the conditions (1) and (2) in the above definition. Condition (1) implies that $\mathcal{C}$ is an additive subgroup of $\mathbb{F}_q[x]/(x^n - 1)$ and condition (2) implies

$$xc(x) \in \mathcal{C} \quad \text{for all } c \in \mathcal{C}.$$

It follows that

$$f(x)c(x) \in \mathcal{C} \quad \text{for all } f(x) \in \mathbb{F}_q[x]/(x^n - 1) \text{ and } c \in \mathcal{C}.$$

Therefore, we can conclude that $\mathcal{C}$ is an ideal of $\mathbb{F}_q[x]/(x^n - 1)$. By Theorem 2.11, there exists a unique monic divisor $g(x)$ of $x^n - 1$ such that

$$\mathcal{C} = (g(x)) = \{c(x)g(x) \mid c(x) \in \mathbb{F}_q[x]/(x^n - 1)\}.$$

The polynomials $g(x)$ and $h(x) = (x^n - 1)/g(x)$ are called the *generator polynomial* and *check polynomial* of $\mathcal{C}$, respectively.

Generator polynomials and check polynomials are useful for understanding and constructing cyclic codes. The following facts summarize some properties of generator and check polynomials of cyclic codes.

Proposition 2.4. *Suppose that $\mathcal{C} \subseteq \mathbb{F}_q[x]/(x^n - 1)$ is a q-ary cyclic code with generator polynomial $g(x)$ and check polynomial $h(x)$, where $g(x) = \sum_{i=0}^{k} g_i x^i$ is of degree k.*

- *For any $c(x) \in \mathbb{F}_q[x]/(x^n - 1)$,*

$$c(x) \in \mathcal{C} \iff g(x) \mid c(x) \iff (x^n - 1) \mid c(x)h(x).$$

- *As a vector space, $\mathcal{C}$ has a basis $\{g(x), xg(x), \ldots, x^{n-k-1}g(x)\}$, and hence*

$$\dim(\mathcal{C}) = n - k.$$

- *The code $\mathcal{C}$ has a generator matrix*

$$G = \begin{bmatrix} g(x) \\ xg(x) \\ \vdots \\ x^{n-k-1}g(x) \end{bmatrix} = \begin{bmatrix} g_0 & g_1 & g_2 & \cdots & g_k & 0 & \cdots & 0 \\ 0 & g_0 & g_1 & g_2 & \cdots & g_k & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \ddots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & g_0 & g_1 & g_2 & \cdots & g_k \end{bmatrix}_{(n-k)\times n}.$$

From the above, we have seen that every q-ary cyclic code of length n has a unique generator polynomial, which is a monic divisor of $x^n - 1$. Conversely, any monic divisor $g(x)$ of $x^n - 1$ generates an ideal $(g(x))$ of $\mathbb{F}_q[x]/(x^n - 1)$ that satisfies the definition of a cyclic code. Therefore, there exists a one-to-one correspondence between q-ary cyclic codes of length n and the monic divisors of $x^n - 1 \in \mathbb{F}_q[x]$ Consequently, a complete characterization of q-ary cyclic codes of length n reduces to determining all monic divisors of $x^n - 1$ in $\mathbb{F}_q[x]$.

We now restrict to the case where $\gcd(n, q) = 1$. Under this assumption, the residue class $\overline{q} \in \mathbb{Z}/n\mathbb{Z}$ is invertible. Since $\mathbb{Z}/n\mathbb{Z}$ is finite, there must exist a positive integer m such that $\overline{q}^{m+1} = \overline{q}$, which implies $\overline{q}(\overline{q}^m - \overline{1}) = \overline{0}$. As $\overline{q}$ is invertible, it follows that $\overline{q}^m = \overline{1}$, i.e.,

$$q^m \equiv 1 \pmod{n}. \tag{2.8}$$

The smallest positive integer m such that (2.8) holds is called the *multiplicative order* of q modulo n, denoted by $\mathrm{ord}_n(q)$.

Now, let $m = \mathrm{ord}_n(q)$. Recall Theorem 2.6. Let α be a primitive element of $\mathbb{F}_{q^m}$, i.e., $\mathbb{F}_{q^m}^* = \langle \alpha \rangle$. Then there exists a primitive n-th root of unity β in $\mathbb{F}_{q^m}$; for example, take $\beta = \alpha^{(q^m-1)/n}$. This yields the factorization of $x^n - 1$ in $\mathbb{F}_{q^m}[x]$:

$$x^n - 1 = \prod_{a=0}^{n-1} (x - \beta^a). \tag{2.9}$$

Definition 2.14. *Let n be an integer such that $\gcd(n, q)$=1, and let $a \in [0, n-1]$ be an integer. The q-*cyclotomic coset of a modulo n *is defined by*

$$C_n(a) = \{aq^k \bmod n \mid k = 0, \ldots, l_a - 1\}, \tag{2.10}$$

where l_a is the smallest integer such that $aq^{l_a} \equiv a \pmod{n}$. The smallest integer in $C_n(a)$ is called the coset leader *of $C_n(a)$, or simply a* coset leader modulo n.

For each integer $a \in [0, n-1]$, we denote by $m_a(x)$ the minimal polynomial of β^a over $\mathbb{F}_q$. We can apply Theorem 2.1 to obtain

$$m_a(x) = \prod_{i \in C_n(a)} (x - \beta^i). \tag{2.11}$$

Moreover, by Remark 2.1, we also have $|C_n(a)|$ divides m.

For two integers $b, c \in [0, n-1]$ with $b < c$, let $\mathcal{L}^n(b, c)$ denote the set of all coset leaders modulo n in the interval $[b, c]$. In particular, we simply denote $\mathcal{L}^n = \mathcal{L}^n(0, n-1)$. Note that each q-cyclotomic coset has a unique coset leader. We now can conclude from (2.9) and (2.11) that

$$x^n - 1 = \prod_{a \in \mathcal{L}^n} m_a(x) = \prod_{a \in \mathcal{L}^n} \prod_{i \in C_n(a)} (x - \beta^i).$$

Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be a q-ary cyclic code with generator polynomial $g(x)$. Note that $g(x)$ is a monic divisor of $x^n - 1$. Moreover, for each $a \in \mathcal{L}^n$, the minimal polynomial $m_a(x)$ is irreducible in $\mathbb{F}_q[x]$. Therefore, there exists a subset $\mathcal{I} \subseteq \mathcal{L}^n$ such that

$$g(x) = \prod_{a \in \mathcal{I}} m_a(x) = \prod_{a \in \mathcal{I}} \prod_{i \in C_n(a)} (x - \beta^i).$$

The set $\Gamma = \{0 \leq i \leq n-1 : g(\beta^i) = 0\}$ is called the *defining set* of $\mathcal{C}$ with respect to β. It is clear that $\Gamma = \bigcup_{a \in \mathcal{I}} C_n(a)$. Therefore, $\deg g(x) = \left| \bigcup_{a \in \mathcal{I}} C_n(a) \right|$ and the dimension of $\mathcal{C}$ can be given by

$$\dim(\mathcal{C}) = n - \left| \bigcup_{a \in \mathcal{I}} C_n(a) \right|. \tag{2.12}$$

2.6 BCH codes

As discussed in the previous section, the defining set of a q-ary cyclic code of length n is a union of several q-cyclotomic cosets modulo n, and the dimension of the code can be determined by the size of its defining set.

Moreover, the defining set may also provide information about the code's minimum distance. In particular, if the defining set contains a sufficient number of consecutive elements, it guarantees a lower bound on the minimum distance, as stated in the following theorem.

Theorem 2.12. [10, 28, BCH Bound] *Let $\mathcal{C} \subseteq \mathbb{F}_q^n$ be an $[n, k, d]_q$ cyclic code with defining set Γ. If Γ contains $\delta - 1$ consecutive elements for some integer $\delta \geq 2$, then $d \geq \delta$.*

This theorem can be derived from the structure of the parity-check matrix of a cyclic code by applying Theorem 2.10. It helps us design cyclic codes with strong error-correcting capability, or equivalently, with a large minimum distance. For example, BCH codes are defined as follows.

Definition 2.15. *Let q be a prime power and n be a positive integer such that* $\gcd(n,q) = 1$. *Let $m = \mathrm{ord}_n(q)$ and $\beta \in \mathbb{F}_{q^m}$ be a primitive n-th root of unity. A q-ary cyclic code of length n is called a* BCH code *with designed distance δ if its generator polynomial takes the form*

$$\mathrm{lcm}(m_b(x), m_{b+1}(x), \ldots, m_{b+\delta-2}(x))$$

for some integers b and δ with $2 \leq \delta \leq n$, where lcm *denotes the least common multiple of the polynomials. We denote such a code by $\mathcal{C}_{(q,n,\delta,b)}$. In particular, the code is called* narrow-sense *if $b = 1$, and is simply denoted by $\mathcal{C}_{(q,n,\delta)}$.*

From the definition, we can easily see that the defining set of $\mathcal{C}_{(q,n,\delta,b)}$ with respect to β is $\bigcup_{a=b}^{b+\delta-2} C_n(a)$, which contains $b, b+1, \ldots, \delta-1$ as $\delta-1$ consecutive elements. Therefore, by BCH bound, the minimum distance d of $\mathcal{C}_{(q,n,\delta,b)}$ satisfies $d \geq \delta$.

Common choices for the length n of a BCH code include:

- $n = q^m - 1$ for some positive integer m; in this case, the code is called *primitive*.
- $n = q^m + 1$ for some positive integer m; in this case, the code is called *antiprimitive*.
- $n = \frac{q^m-1}{\lambda}$, where λ is a divisor of $q-1$.

Note that there may exist distinct δ and δ' such that

$$\bigcup_{a=b}^{b+\delta-2} C_n(a) = \bigcup_{a=b}^{b+\delta'-2} C_n(a),$$

and hence the codes $\mathcal{C}(q,n,\delta,b)$ and $\mathcal{C}(q,n,\delta',b)$ are identical. The *Bose distance* of $\mathcal{C}_{(q,n,\delta,b)}$, denoted by $d_B(\mathcal{C}_{(q,n,\delta,b)})$ or simply d_B, is defined as the largest integer such that $\mathcal{C}_{(q,n,\delta,b)} = \mathcal{C}_{(q,n,d_B,b)}$. The BCH bound indicates that $d \geq d_B \geq \delta$. For some BCH codes, the Bose distance and the minimum distance can even be equal, as shown by the following results.

Theorem 2.13. [41, p. 260] *For any k with $1 \leq k \leq m-1$, a primitive BCH code of length $n = q^m - 1$ and design distance $\delta = q^k - 1$ has minimum distance $d = q^k - 1$.*

The next result was given by Kasami and Lin [31].

Theorem 2.14. *For binary primitive BCH codes of length $n = 2^m - 1$ and Bose distance $d_B = 2^{m-1-s} - 2^{m-1-s-i} - 1$ with $1 \leq i \leq m - s - 2$ and $0 \leq s \leq m - 2i$, we have $d = d_B$.*

Peterson [48] proved the following result.

Theorem 2.15. *Suppose that a q-ary narrow-sense primitive BCH code with Bose distance δ has minimum distance $d = \delta$, and $\delta + 1$ is divisible by $\mathrm{Char}(\mathbb{F}_q)$. Then the q-ary narrow-sense primitive BCH code with Bose distance $d_B = (\delta + 1)q^{m-k} - 1$, where $k \geq \delta$, has minimum distance $d = d_B$.*

One can find a proof for the following result in [8, p. 247].

Theorem 2.16. *Let $\mathcal{C}$ be a narrow-sense BCH code of length n with design distance δ. If δ divides n, then $d = d_B = \delta$.*

In addition to the results mentioned above, there is a well known conjecture regarding narrow-sense primitive BCH codes, proposed by Charpin [12].

Conjecture 2.1. *For a primitive narrow-sense BCH code, the minimum distance d and the Bose distance d_B satisfy $d \leq d_B + 4$.*

For linear codes, including BCH codes, the dimension and minimum distance are two crucial parameters. They determine the number of information symbols and the error-correcting capability of a linear code. Despite decades of research, our understanding of the dimension and minimum distance of BCH codes remains limited. As noted by Charpin [14], determining the minimum distance d of BCH codes in general is a challenging problem. In comparison, obtaining the Bose distance is relatively more tractable. Furthermore, as seen from the previous results on Bose distance, determining the Bose distance is also valuable for understanding BCH codes.

Next, we examine how to determine the Bose distance and minimum distance of a BCH code from its defining set. By equation (2.12), the dimension of $\mathcal{C}_{(q,n,\delta,b)}$ can be given by

$$\dim(\mathcal{C}_{(q,n,\delta,b)}) = n - \left| \bigcup_{a=b}^{b+\delta-2} C_n(a) \right|.$$

In particular, for a narrow-sense BCH code $\mathcal{C}_{(q,n,\delta)}$, we have

$$\dim(\mathcal{C}_{(q,n,\delta)}) = n - \left| \bigcup_{a=1}^{\delta-1} C_n(a) \right| = n - \sum_{a \in \mathcal{L}^n(1,\delta-1)} |C_n(a)|. \tag{2.13}$$

Thus, determining the coset leaders modulo n within $[1, \delta - 1]$ and the sizes of the corresponding q-cyclotomic cosets allows us to compute the dimension of $\mathcal{C}_{(q,n,\delta)}$.

Regarding the Bose distance of $\mathcal{C}(q, n, \delta)$, for $\delta' > \delta$, we observe that

$$\bigcup_{a=1}^{\delta-1} C_n(a) = \bigcup_{a=1}^{\delta'-1} C_n(a)$$

if and only if none of the integers in $[\delta, \delta' - 1]$ is a coset leader. Therefore, the Bose distance of $\mathcal{C}(q, n, \delta)$ is equal to the smallest coset leader modulo n in $[\delta, n - 1]$.

Chapter 3

Some results on q-cyclotomic cosets

We have established the relationship between q-cyclotomic cosets and both the dimension and Bose distance of BCH codes. This demonstrates that determining coset leaders and the sizes of their corresponding cosets is crucial for establishing the dimension and Bose distance of BCH codes.

In this Chapter, we present some known and new results concerning the sizes and coset leaders of q-cyclotomic cosets. These results will be applied in the subsequent chapters to determine the dimension and Bose distance of certain BCH codes.

3.1 q-cyclotomic cosets modulo n

Let n be an integer such that $\gcd(n, q) = 1$. For two integers $b, c \in [0, n-1]$ with $b < c$, recall that $\mathcal{L}^n(b, c)$ denotes the set of all coset leaders modulo n in the interval $[b, c]$. For a positive integer l, we define $\mathcal{L}_l^n(b, c)$ as the set of all coset leaders modulo n in $[b, c]$ whose corresponding coset has size l, that is,

$$\mathcal{L}_l^n(b, c) = \{a \in [b, c] : a \in \mathcal{L}^n(b, c) \text{ and } |C_n(a)| = l\}.$$

We first present a necessary condition for an integer $a \in [0, n-1]$ to be a coset leader modulo n as follows.

Lemma 3.1. *Let n be a positive integer such that $\gcd(n, q) = 1$. If a is the coset leader of $C_n(a)$, then $q \nmid a$.*

Proof. Note that if $q \mid a$, then $a/q \in C_n(a)$, which is less than a. This is contrary to that a is the coset leader of $C_n(a)$. Therefore, we must have $q \nmid a$. □

The following result originated from the proof of [60, Lemma 6]. For completeness, we provide a proof here.

Lemma 3.2. *Suppose that n and λ are two integers such that $\gcd(n, q) = 1$ and $\gcd(\lambda, q) = 1$. Let $a \in [0, n-1]$ be an integer. Then*

- *a is the coset leader of $C_n(a)$ if and only if λa is the coset leader of $C_{\lambda n}(\lambda a)$;*
- *$|C_n(a)| = |C_{\lambda n}(\lambda a)|$.*

Proof. By definition, the integer a is the coset leader of $C_n(a)$ if and only if

$$a \bmod n \le aq^i \bmod n \quad \text{for any integer } i \ge 0. \tag{3.1}$$

Noticing that $a \bmod n = a - n \cdot \lfloor \frac{a}{n} \rfloor$ and $\lambda a \bmod \lambda n = \lambda a - \lambda n \cdot \lfloor \frac{\lambda a}{\lambda n} \rfloor$, we can assert that

$$\lambda \cdot (a \bmod n) = \lambda a - \lambda n \cdot \lfloor \frac{a}{n} \rfloor = \lambda a - \lambda n \cdot \lfloor \frac{\lambda a}{\lambda n} \rfloor = \lambda a \bmod \lambda n.$$

Similarly, we also have

$$\lambda \cdot (aq^i \bmod n) = \lambda aq^i \bmod \lambda n. \tag{3.2}$$

Therefore, the inequality in (3.1) is equivalent to

$$\lambda a \bmod \lambda n \le \lambda aq^i \bmod \lambda n \quad \text{for any integer } i \ge 0.$$

By definition, this holds if and only if λa is the coset leader of $C_{\lambda n}(\lambda a)$. Therefore, the first statment follows.

In addition, the equality in (3.2) also implies that

$$aq^i \bmod n = a \quad \text{if and only if} \quad \lambda a q^i \bmod \lambda n = \lambda a.$$

It follows that the smallest integer l_a such that $aq^{l_a} \bmod n = a$ is equal to the smallest integer $l_{\lambda a}$ such that $\lambda a q^{l_{\lambda a}} \bmod \lambda n = \lambda a$. Therefore, we have $|C_n(a)| = |C_{\lambda n}(\lambda a)|$. This completes the proof. $\square$

For an integer λ, we define $\mathcal{D}_\lambda$ as the set of integers that are divisible by λ, that is,

$$\mathcal{D}_\lambda = \{a \in \mathbb{Z} : \lambda \mid a\}.$$

Then one can directly derive the following corollary from the above lemma.

Corollary 3.1. *Let n be an integer such that $\gcd(n, q) = 1$ and let λ be a positive divisor of $q-1$. Then*

$$|\mathcal{L}_l^n(b, c)| = \left|\mathcal{L}_l^{\lambda n}(\lambda b, \lambda c) \cap \mathcal{D}_\lambda\right|$$

for any positive integer l, and integers $b, c \in [0, n-1]$ with $b < c$.

Later, we will present some results on the sizes and coset leaders of q-cyclotomic cosets modulo $q^m - 1$. Applying this corollary, these findings can be extended to q-cyclotomic cosets modulo $\frac{q^m-1}{\lambda}$ for any positive divisor λ of $q-1$. This extension is useful for determining the parameters of BCH codes of length $\frac{q^m-1}{\lambda}$ in Chapter 5.

3.2 The size of q-cyclotomic cosets modulo $q^m - 1$

Throughout the remainder this chapter, we always assume that m is a positive integer, $h = \lfloor m/2 \rfloor$, and $n = q^m - 1$. We first determine the sizes of certain q-cyclotomic cosets modulo $n = q^m - 1$ by presenting the following theorem.

Theorem 3.1. *Let m be a positive integer, $h = \lfloor \frac{m}{2} \rfloor$ and $n = q^m - 1$. If m is an odd integer, then for any integer $a \in [1, q^{m-\lfloor m/3 \rfloor})$,*

$$|C_n(a)| = m.$$

If m is an even integer, then for any integer $a \in [1, q^{m-\lfloor m/3 \rfloor})$,

$$|C_n(a)| = \begin{cases} \frac{m}{2} & \text{if } aq^h \bmod n = a, \\ m & \text{if } aq^h \bmod n \neq a. \end{cases} \tag{3.3}$$

In order to prove the above theorem, we introduce some additional notations and concepts. Let Z_q be the set of all non-negative integers less than q. Each integer $a \in [0, n-1]$ can be uniquely represented by its *q-adic expansion* as $a = \sum_{\ell=0}^{m-1} a_\ell q^\ell$ with $a_\ell \in Z_q$. Let Z_q^m be the set of all length-m sequences of integers in Z_q. For simplicity, denote by $\mathbf{0}_m$ the sequence in Z_q^m whose elements are all zero. We define a lexicographic order on Z_q^m. Specifically, for any two sequences $U = (u_{m-1}, \ldots, u_1, u_0)$ and $W = (w_{m-1}, \ldots, w_1, w_0)$ in Z_q^m,

1. U and W are said to be equal, denoted as $U = W$, if $u_\ell = w_\ell$ for $\ell = 0, \ldots, m-1$;
2. U is less than W, denoted as $U < W$, if either $u_{m-1} < w_{m-1}$ or there exists an integer $i \in [0, m-2]$ such that $u_i < v_i$ and $u_\ell = w_\ell$ for all $\ell = i+1, \ldots, m-1$;
3. $U \leq W$ is denoted if $U = W$ or $U < W$.

We define a map V from the set of all integers in $[0, n-1]$ to Z_q^m as

$$V(a) = (a_{m-1}, \ldots, a_1, a_0),$$

where $\sum_{\ell=0}^{m-1} a_\ell q^\ell$ forms the q-adic expansion of the integer $a \in [0, n-1]$. Let I_{m-1} be the identity matrix of order $m-1$, and let

$$Q = \begin{bmatrix} 0 & 1 \\ I_{m-1} & 0 \end{bmatrix}.$$

It is clear that for any sequence $(a_{m-1}, a_{m-2}, \ldots, a_0) \in Z_q^m$,

$$(a_{m-1}, a_{m-2}, \ldots, a_0)Q = (a_{m-2}, \ldots, a_0, a_{m-1}).$$

Let $a, b \in [0, n-1]$ be two integers with $a < b$. We have the following observations:

Observation 3.1. *$a = b$ if and only if $V(a) = V(b)$, $a < b$ if and only if $V(a) < V(b)$, and $a \leq b$ if and only if $V(a) \leq V(b)$.*

Observation 3.2. *$V(aq^t \bmod n) = V(a)Q^t$ for any integer $t \in [1, m-1]$.*

Observation 3.3. *The integer a is a coset leader modulo n if and only if $V(a) \leq V(a)Q^t$ for all integer $t \in [1, m-1]$.*

Proof of Theorem 3.1. We first consider the case when m is an odd integer. Suppose that $a \in [1, q^{m-\lfloor m/3 \rfloor})$ is an integer. Denote by $\sum_{\ell=0}^{m-1} a_\ell q^\ell$ the q-adic expansion of a. It is clear that $a_\ell = 0$ for all $\ell = m - \lfloor m/3 \rfloor, \ldots, m-1$, and hence

$$V(a) = (\mathbf{0}_{\lfloor \frac{m}{3} \rfloor}, a_{m-\lfloor \frac{m}{3} \rfloor - 1}, \ldots, a_0). \tag{3.4}$$

By the definition of the coset $C_n(a)$, we have $aq^{l_a} \bmod n = a$. It follows that $V(a)Q^{l_a} = V(aq^{l_a} \bmod n) = V(a)$, i.e.,

$$(a_{m-1-l_a}, \ldots, a_0, a_{m-1}, \ldots, a_{m-l_a}) = (a_{m-1}, \ldots, a_1, a_0).$$

For simplicity, denote $U = (a_{m-1}, \ldots, a_{m-l_a})$. Recall $l_a \mid m$. Then we can conclude from the above equation that

$$V(a) = (U, U, \ldots, U). \tag{3.5}$$

Assume that $l_a \leq \lfloor m/3 \rfloor$. We can conclude from (3.4) that

$$U = (a_{m-1}, \ldots, a_{m-l_a}) = \mathbf{0}_{l_a}.$$

With (3.5), it follows that $V(a) = \mathbf{0}_m$, which implies $a = 0$. This contradicts the initial assumption that $a \in [1, q^{m-\lfloor m/3 \rfloor})$. Therefore, we must have $l_a > \lfloor m/3 \rfloor$. Given that m is an odd integer and $l_a \mid m$, it follows that $l_a = m$. Equivalently, $|C_n(a)| = m$.

When m is an even integer, we can use a similar argument as in the first paragraph to show that $l_a > \lfloor m/3 \rfloor$ for any integer $a \in [1, q^{m-\lfloor m/3 \rfloor})$. Note that l_a divides m and m is even. It follows that $l_a = m/2$ or m. Consequently, we have $l_a = m/2 = h$ if $aq^h \bmod n = a$, and $l_a = m$ otherwise. Equivalently, the equality in (3.3) holds. This completes the proof. □

It is straightforward to verify that $aq^h \bmod n \neq a$ for any integer $a \in [1, q^h)$ when m is even. Therefore, we can derive the following corollary, which can also be derived from [58, Lemma 5].

Corollary 3.2. *If m is an even integer, then $|C_n(a)| = m$ for any integer $a \in [1, q^h)$.*

Define $\mathcal{H}$ as the set of all coset leaders modulo $n = q^m - 1$ in the interval $[1, n-1]$ such that the corresponding coset has size $m/2$, that is,

$$\mathcal{H} = \mathcal{L}^n_{\frac{m}{2}}(1, n-1), \quad n = q^m - 1. \tag{3.6}$$

Then we also have the following corollary of Theorem 3.1.

Corollary 3.3. *Let m and k integers such that m is even $0 \leq k \leq \lfloor (2m-1)/3 \rfloor - h$. Suppose that $a \in \left[q^{h+k}, q^{h+k+1}\right)$ is an integer. Then $a \in \mathcal{H}$ if and only if $V(a)$ has the form*

$$(\mathbf{0}_{h-k-1}, a_k, \ldots, a_0, \mathbf{0}_{h-k-1}, a_k, \ldots, a_0) \tag{3.7}$$

with $a_0 > 0$ and $a_k > 0$.

Proof. Necessity part. Suppose that $a \in \mathcal{H}$. By the definition of $\mathcal{H}$ and Lemma 3.1, we first have $q \nmid a$. By applying Theorem 3.1, we also have $aq^h \bmod (q^m - 1) = a$. This is equivalent to $V(a)Q^h = V(a)$. Moreover, $V(a)$ has the form $(\mathbf{0}_{h-k-1}, a_{h+k} \ldots, a_0)$ with $a_{h+k} > 0$. Therefore,

$$(\mathbf{0}_{h-k-1}, a_{h+k} \ldots, a_0) = (a_{h-1}, \ldots, a_0, \mathbf{0}_{h-k-1}, a_{h+k} \ldots, a_h).$$

This implies that

$$(a_{h-1}, \ldots, a_{k+1}) = \mathbf{0}_{h-k-1}$$

and

$$(a_k, \ldots, a_0) = (a_{h+k}, \ldots, a_h).$$

Thus, $V(a)$ has the form specified in (3.7). Furthermore, since $q \nmid a$ and $a_{h+k} > 0$, we also have $a_0 > 0$ and $a_k = a_{h+k} > 0$.

Sufficiency part. Suppose that $V(a)$ has the form specified in (3.7) with $a_0 > 0$ and $a_k > 0$. Then it is straightforward to verify that $V(a) \leq V(a)Q^t$ for any integer $t \in [1, m-1]$. In particular, $V(a) = V(a)Q^h$, which is equivalent to $aq^h \bmod (q^m - 1) = a$. By applying Theorem 3.1 and Observation 3.3, we can conclude that a is the coset leader of $C_n(a)$ and $|C_n(a)| = m/2$ with $n = q^m - 1$, i.e., $a \in \mathcal{H}$. $\square$

By counting the sequences in Z_q^m having the form in (3.7) with $a_0 > 0$ and $a_k > 0$, we can directly derive the following corollary.

Corollary 3.4. *Let m and k be integers such that m is even and $1 \leq k \leq \lfloor (2m-1)/3 \rfloor - h$. Then we have*

$$\left| \left[q^{h+k}, q^{h+k+1} \right) \cap \mathcal{H} \right| = q^{k-1}(q-1)^2. \tag{3.8}$$

3.3 Coset leaders modulo $q^m - 1$

We now turn to the coset leaders modulo $n = q^m - 1$. By Lemma 3.1, we know that an integer a is not a coset leader modulo n if $q \mid a$. Therefore, we only need to focus on finding those integers that are neither divisible by q nor coset leaders modulo n. We define $\mathcal{S}$ as the set of all such integers in $[1, n-1]$. That is,

$$\mathcal{S} = \{a \in [1, n-1] : q \nmid a \text{ and } a \notin \mathcal{L}^n\}, \quad n = q^m - 1. \tag{3.9}$$

Notably, the following lemma demonstrates that the condition $q \nmid a$ is also sufficient for a being a coset leader when a is sufficiently small.

Lemma 3.3. [57, Theorem 2.3] *Let m be a positive integer, $h = \lfloor \frac{m}{2} \rfloor$ and $n = q^m - 1$.*

- *When m is an odd integer, for any integer $a \le q^{h+1}$, a is the coset leader of $C_n(a)$ if and only if $q \nmid a$.*
- *When m is an even integer, for any integer $a \le 2q^h$, a is the coset leader of $C_n(a)$ if and only if $q \nmid a$.*

Let m and k be two integers such that $m \ge 4$ and $m - 2h \le k \le \lfloor (2m-1)/3 \rfloor - h$. When m is an odd integer, for each integer $i \in [-k+1, k]$, we define $\mathcal{A}_k(i)$ as the set of all integers $a \in [q^{h+k}, q^{h+k+1})$ with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$ that satisfies:

$$a_{h+i} > 0; \tag{3.10}$$

$$(a_{k+i-1}, \dots, a_0) \le (a_{h+k}, \dots, a_{h-i+1}) \text{ and } a_0 > 0; \tag{3.11}$$

$$V(a) = (\mathbf{0}_{h-k}, a_{h+k}, \dots, a_{h+i}, \mathbf{0}_{h-k}, a_{k+i-1}, \dots, a_0). \tag{3.12}$$

When m is an even integer, for each $i \in [-k, k]$, we define $\mathcal{B}_k(i)$ as the set of all integers $a \in [q^{h+k}, q^{h+k+1})$ with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$ that satisfies the condition in (3.10) and the following:

$$(a_{k+i}, \dots, a_0) \le (a_{h+k}, \dots, a_{h-i}) \text{ with } a_0 > 0; \tag{3.13}$$

$$V(a) = (\mathbf{0}_{h-k-1}, a_{h+k}, \dots, a_{h+i}, \mathbf{0}_{h-k-1}, a_{k+i}, \dots, a_0). \tag{3.14}$$

We make the following remarks about the above definitions of $\mathcal{A}_k(i)$ and $\mathcal{B}_k(i)$.

Remark 3.1. *The condition that $k \leq \lfloor (2m-1)/3 \rfloor - h$ implies the following consequences:*

- *When m is odd, $|2i-1| \leq h-k$ for all $i \in [-k+1, k]$.*
- *When m is even, $|2i| \leq h-k-1$ for all $i \in [-k, k]$.*

Remark 3.2. *The condition in (3.10) is satisfied if and only if $q \nmid \sum_{\ell=h+i}^{h+k} a_\ell q^{\ell-(h+i)}$.*

Remark 3.3. *The condition in (3.11) can be equivalently expressed as*

$$\sum_{\ell=0}^{k+i-1} a_\ell q^\ell \leq \sum_{\ell=h-i+1}^{h+k} a_\ell q^{\ell-(h-i+1)} \quad \text{and} \quad a_0 > 0. \tag{3.15}$$

Moreover, the form of $V(a)$ in (3.12) implies that

$$\sum_{\ell=h-i+1}^{h+k} a_\ell q^{\ell-(h-i+1)} = \sum_{\ell=h+i}^{h+k} a_\ell q^{\ell-(h+i)} \cdot q^{2i-1}$$

if $i \in [1, k]$, and

$$\sum_{\ell=h+i}^{h+k} a_\ell q^{\ell-(h+i)} \cdot q^{2i-1} = \sum_{\ell=h-i+1}^{h+k} a_\ell q^{\ell-(h-i+1)} + \sum_{\ell=h+i}^{h-i} a_\ell q^{\ell-(h-i+1)}$$

if $i \in [-k+1, 0]$. Noticing that $0 \leq \sum_{\ell=h+i}^{h-i} a_\ell q^{\ell-(h-i+1)} < 1$ for $i \in [-k+1, 0]$, and the two summations in (3.15) are both integers, we can conclude that (3.15) is equivalent to

$$\sum_{\ell=0}^{k+i-1} a_\ell q^\ell \leq \sum_{\ell=h+i}^{h+k} a_\ell q^{\ell-(h+i)} \cdot q^{2i-1} \quad \text{and} \quad a_0 > 0. \tag{3.16}$$

Similarly, the condition in (3.13) can also be written as

$$\sum_{\ell=0}^{k+i} a_\ell q^\ell \leq \sum_{\ell=h-i}^{h+k} a_\ell q^{\ell-(h-i)} \quad \text{and} \quad a_0 > 0, \tag{3.17}$$

which is further equivalent to

$$\sum_{\ell=0}^{k+i} a_\ell q^\ell \leq \sum_{\ell=h-i}^{h+k} a_\ell q^{\ell-(h+i)} \cdot q^{2i} \quad \text{and} \quad a_0 > 0. \tag{3.18}$$

Remark 3.4. *If $a \in \mathcal{A}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$, then*

$$\sum_{\ell=0}^{h-k} a_\ell q^\ell \leq \sum_{\ell=h-i+1}^{h+k} a_\ell q^{\ell-(h-i+1)}.$$

Similarly, if $a \in \mathcal{B}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$, then

$$\sum_{\ell=0}^{h-k-1} a_\ell q^\ell \leq \sum_{\ell=h-i}^{h+k} a_\ell q^{\ell-(h-i)}.$$

Remark 3.5. *If $a \in \mathcal{A}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$, then i is the smallest integer in $[-k+1, k]$ such that $a_{h+i} > 0$. Consequently, $\mathcal{A}_k(i) \cap \mathcal{A}_k(j) = \varnothing$ for distinct integers $i, j \in [-k+1, k]$.*

Similarly, if $a \in \mathcal{B}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$, then i is the smallest integer in $[-k, k]$ such that $a_{h+i} > 0$. As a result, $\mathcal{B}_k(i) \cap \mathcal{B}_k(j) = \varnothing$ for distinct integers $i, j \in [-k, k]$.

We denote by $\bigsqcup_{i \in I} A_i$ the disjoint union of a family of sets $\{A_i : i \in I\}$, where I is an index set. Recall the definitions of sets $\mathcal{H}$ and $\mathcal{S}$ in (3.6) and (3.9), respectively. Then we have the following Theorem.

Theorem 3.2. *Let m and k be two integers such that $m \geq 4$ and $m - 2h \leq k \leq \lfloor (2m-1)/3 \rfloor - h$.*

- *If m is odd, then*

$$\mathcal{S} \cap [q^{h+k}, q^{h+k+1}) = \bigsqcup_{i=-k+1}^{k} \mathcal{A}_k(i). \tag{3.19}$$

- *If m is even, then*

$$(\mathcal{S} \cup \mathcal{H}) \cap [q^{h+k}, q^{h+k+1}) = \bigsqcup_{i=-k}^{k} \mathcal{B}_k(i). \tag{3.20}$$

Proof. We first consider the case when m is an odd integer. Suppose that $a \in \bigcup_{i=-k+1}^{k} \mathcal{A}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$. By the definition of $\mathcal{A}_k(i)$, we have (3.10) (3.11) and (3.12) for some integer $i \in [-k+1, k]$. It follows that $q \nmid a$ and

$$V(a)Q^{h-i+1} = (\mathbf{0}_{h-k}, a_{k+i-1}, \ldots, a_0, \mathbf{0}_{h-k}, a_{h+k}, \ldots, a_{h+i}). \tag{3.21}$$

If $i \in [-k+1, 0]$, then we can conclude from (3.10) and (3.11) that

$$(a_{k+i-1}, \ldots, a_0, \mathbf{0}_{-2i+1}) < (a_{h+k}, \ldots, a_{h+i}). \tag{3.22}$$

Recalling the fact that $|2i-1| \leq h-k$ in Remark 3.1, it follows from (3.21) and (3.22) that $V(a)Q^{h-i+1} < V(a)$. By the definition of $\mathcal{S}$ and Observation 3.3, we have $a \in \mathcal{S}$. On the other hand, if $i \in [1, k]$, we conclude from $|2i-1| \leq h-k$ and (3.12) that

$$(a_{h+k}, \ldots, a_{h-i+1}) = (a_{h+k}, \ldots, a_{h+i}, \mathbf{0}_{2i-1}).$$

With (3.11), it follows that

$$(a_{k+i-1}, \ldots, a_{2i-1}) < (a_{h+k}, \ldots, a_{h+i}).$$

Consequently, we still have $V(a)Q^{h-i+1} < V(a)$, which implies $a \in \mathcal{S}$. By now, we have already demonstrated that $\bigcup_{i=-k+1}^{k} \mathcal{A}_k(i) \subseteq \mathcal{S} \cap [q^{h+k}, q^{h+k+1})$.

Conversely, let us assume that $a \in \mathcal{S} \cap [q^{h+k}, q^{h+k+1})$ is an integer with q-adic expansion $\sum\limits_{\ell=0}^{h+k} a_\ell q^\ell$. We first have $a_{h+k} > 0$. By the definition of $\mathcal{S}$ and Observation 3.3, we also have $a_0 > 0$ and $V(a)Q^t < V(a)$ for some integer $t \in [1, m-1]$. Noticing that $V(a) = (\mathbf{0}_{h-k}, a_{h+k}, \ldots, a_0)$, it follows that the first $h-k$ entries of $V(a)Q^t$ are all equal to zero. Considering $a_{h+k} > 0$ and $a_0 > 0$, we have $h-k+1 \leq t \leq h+k$. Consequently, we can conclude that

$$V(a)Q^t = (\mathbf{0}_{h-k}, a_{h+k-t}, \ldots, a_0, \mathbf{0}_{h-k}, a_{h+k}, \ldots, a_{m-t})$$

and

$$V(a) = (\mathbf{0}_{h-k}, a_{h+k}, \ldots, a_{m-t}, \mathbf{0}_{h-k}, a_{h+k-t}, \ldots, a_0).$$

Given that $a_{h+k} > 0$, we can chose i to be the smallest integer in $[m-h-t, k]$ such that $a_{h+i} > 0$. Then $V(a)$ has the form specified in (3.12) with $(a_{k+i-1}, \ldots, a_0) = (\mathbf{0}_{h+t+i-m}, a_{h+k-t}, \ldots, a_0)$. Furthermore, the inequality $h-k+1 \leq t \leq h+k$ implies that $i \in [-k+1, k]$.

Additionally, if $i > m-h-t$, we can obtain (3.11) from the fact that $a_{h+k} > 0$ and $a_0 > 0$. On the other hand, if $i = m-h-t$, then we can derive (3.11) from $V(a)Q^t < V(a)$ and $a_0 > 0$. Now we can conclude that $a \in \mathcal{A}_k(i)$ for some integer $i \in [-k+1, k]$. It follows that $\mathcal{S} \cap [q^{h+k}, q^{h+k+1}) \subseteq \bigcup\limits_{i=-k+1}^{k} \mathcal{A}_k(i)$.

We now can conclude from the above argument that $\bigcup\limits_{i=-k+1}^{k} \mathcal{A}_k(i) = \mathcal{S} \cap [q^{h+k}, q^{h+k+1})$. Finally, applying Remark 3.5 directly yields equation (3.19).

If m is an even integer, with Corollary 3.3, we can utilize a similar argument as above to show that

$$\mathcal{S} \cap [q^{h+k}, q^{h+k+1}) = \bigcup_{i=-k}^{k} \mathcal{B}_k(i) \setminus \left[\mathcal{H} \cap [q^{h+k}, q^{h+k+1})\right].$$

It follows that $(\mathcal{S} \cup \mathcal{H}) \cap [q^{h+k}, q^{h+k+1}) = \bigcup_{i=-k}^{k} \mathcal{B}_k(i)$. Then by applying Remark 3.5 again, we have equation (3.20). This completes the proof of Theorem 3.2. $\square$

Chapter 4

Dimension and Bose distance of primitive BCH codes

4.1 Introduction

In this chapter, we investigate the Bose distance and dimension of some primitive BCH codes. Throughout the chapter, we assume that m is a positive integer, let $h = \lfloor m/2 \rfloor$ and $n = q^m - 1$. In this chapter, the notations $\mathcal{C}_{(q,n,\delta,b)}$ and $\mathcal{C}_{(q,n,\delta)}$ denote, respectively, a primitive BCH code and a narrow-sense primitive BCH code, i.e., codes of length $n = q^m - 1$. For a real number a, we define $N(a)$ as the number of integers in the interval $[1, a-1]$ that are not divisible by q, that is, $N(a) = \lfloor a - 1 \rfloor - \lfloor (a-1)/q \rfloor$.

It is well known that the dimension and Bose distance are two crucial parameters of BCH codes. However, determining them in general remains a difficult problem [20, 45]. To date, only limited results are available, most of which concentrate on primitive BCH codes. For narrow-sense primitive BCH codes $\mathcal{C}_{(q,n,\delta)}$, the dimension is fully determined for $m \leq 2$ [35, 45]. For $m \geq 3$, the problem remains largely unsolved. For convenience, we summarize some known results regarding the dimension of narrow-sense primitive BCH codes $\mathcal{C}_{(q,n,\delta)}$ in Table 4.1. For primitive BCH codes $\mathcal{C}_{(q,n,\delta,b)}$ that are not necessarily narrow-sense, there are quite limited results available.

See [39] for the dimensions of some BCH codes that are not narrow-sense. While the dimension captures the number of information symbols a code can carry, the Bose distance provides a lower bound on its error-correction capability. Compared to the dimension, results on the Bose distance are even more scarce. For previous studies on the Bose distance of $\mathcal{C}_{(q,n,\delta)}$, readers are referred to [5, 15, 17, 18, 19, 24].

The reader may also refer to [46, Table 1] and [20] for summaries of the existing results on the parameters of BCH codes.

Table 4.1: Some known results on the dimension of $\mathcal{C}_{(q,n,\delta)}$

m	δ	Year	Reference
$m \geq 1$	$\delta = q^t$	1962	[42]
m is odd	$2 \leq \delta \leq q^{(m+1)/2} + 1$	1996	[58]
m is even	$2 \leq \delta \leq 2q^{m/2} + 1$	1996	[58]
$m \geq 1$	$\delta = (q - l_0)q^{m-l_1-1} - 1$ with $0 \leq l_0 \leq q-2$ and $0 \leq l_1 \leq m-1$	2015	[17]
m is even	$\delta = k(q^{m/2} + 1)$ with $1 \leq k \leq q-1$	2015	[17]
$m \geq 1$	$\delta = q^t - 1$	2015	[17]
$m \geq 1$	$\delta = q^t + b$ with $1 \leq b \leq \lfloor (q^t - 1)/q^{m-t} \rfloor + 1$	2015	[18]
$m \geq 1$	$\delta = (q-1)q^{m-1} - 1 - q^{\lfloor (m-1)/2 \rfloor}$	2017	[19]
$m \geq 4$	$\delta = (q-1)q^{m-1} - 1 - q^{\lfloor (m+1)/2 \rfloor}$	2017	[19]
$m \geq 4$	$2 \leq \delta \leq q^{\lfloor (m+1)/2 \rfloor + 1}$	2017	[39]
$m = 2$	$2 \leq \delta \leq q^m - 2$	2017	[39]
$m > 1$	$\delta = a(q^m - 1)/q - 1$ or $\delta = aq^{m-1} - 1$ with $1 \leq a \leq q-1$	2020	[15]
$m \geq 11$	$\delta = (q-1)q^{m-1} - 1 - q^{\lfloor (m+3)/2 \rfloor}$	2023	[44]
$m > 1$	$\delta = q^t + b$ with $\lceil m/2 \rceil \leq t < m$ and $0 \leq b < q^{m-t} + \sum_{i=1}^{\lfloor t/s \rfloor - 1} q^{m+i(m-t)}$; $\delta = q^t - b$ with $\lceil m/2 \rceil < t < m$ and $0 \leq b < (q-1)\sum_{i=1}^{m-t} q^i$	2024	[24]

As established in Section 2.6 of Chapter 2, the dimension of $\mathcal{C}_{(q,n,\delta)}$ can be determined by identifying all coset leaders modulo n within the interval $[1, \delta - 1]$ and computing the sizes of their corresponding q-cyclotomic cosets. The Bose distance can be derived by finding the smallest coset leader within $[\delta, n-1]$. In general, determining the size of a q-cyclotomic coset modulo $n = q^m - 1$ is relatively straightforward, since it must divide m. However, finding all the coset leaders modulo $n = q^m - 1$ within the interval $[1, \delta - 1]$ in general remains a challenging problem, since the distribution of coset leaders is highly irregular. Only for sufficiently small a, the integer a is a coset leader if and only if q does not divide a. This observation was applied in [58] to determine the dimension of $\mathcal{C}_{(q,n,\delta)}$ for $2 \le \delta \le q^{(m+1)/2} + 1$ when m is odd, and for $2 \le \delta \le 2q^{m/2} + 1$ when m is even. Later, Liu et al. [39] improved this result by giving the dimension of $\mathcal{C}_{(q,n,\delta)}$ for $m \ge 4$ and $2 \le \delta \le q^{\lfloor (m+1)/2 \rfloor + 1}$. Beyond this range, the dimension is determined for a few special cases. For example, Mann [42] established the dimension of $\mathcal{C}_{(q,n,\delta)}$ for $\delta = q^t$. Cherchem et al. [15] gave the dimension and Bose distance of $\mathcal{C}_{(q,n,\delta)}$ for $\delta = \frac{a(q^m-1)}{q-1}$ and $\delta = aq^m - 1$, where $a \in [1, q-1]$ is an integer. By identifying the first few largest coset leaders and the sizes of the corresponding cosets, the parameters of $\mathcal{C}_{(q,n,\delta)}$ for δ as the four largest coset leaders were determined in [19] [36] and [44]. One can also obtain the parameters of some BCH codes by comparing them with those of codes with known parameters. Building on Mann's work [42], Ding et al. determined the dimensions of $\mathcal{C}_{(q,n,q^t-1)}$ [17, Theorem 14], $\mathcal{C}_{(q,n,q^t+b)}$ for $1 \le b \le \lfloor (q^t-1)/q^{m-t} \rfloor + 1$ [18, Theorem 13], and $\mathcal{C}_{(q,n,q^t-2)}$ for $q > 2$ [17, Theorem 15]. Recently, the dimension of $\mathcal{C}_{(q,n,q^t+b)}$ for $\lceil m/2 \rceil \le t < m$ and $0 \le b < q^{m-t} + \sum_{i=1}^{\lfloor t/s \rfloor -1} q^{m+i(m-t)}$, and $\mathcal{C}_{(q,n,q^t-b)}$ for $\lceil m/2 \rceil < t < m$ and $0 \le b < (q-1)\sum_{i=1}^{m-t} q^i$ were provided in [24].

In this chapter, we determine the dimension and Bose distance of narrow-sense primitive $\mathcal{C}_{(q,n,\delta)}$ for $m \ge 4$ and $2 \le \delta \le q^{\lfloor (2m-1)/3 \rfloor + 1}$. We also extend these results to some non-narrow-sense primitive BCH codes. In the existing literature, for $m \ge 4$, the dimension of $\mathcal{C}_{(q,n,\delta)}$ is known only for $\delta \in [2, q^{\lfloor (m+1)/2 \rfloor + 1}]$ and for some special cases. Moreover, it is clear that $q^{\lfloor (2m-1)/3 \rfloor + 1} \ge q^{\lfloor (m+1)/2 \rfloor + 1} \cdot q^{\lfloor (m-4)/6 \rfloor}$. Therefore, our results provide the dimension of $\mathcal{C}_{(q,n,\delta)}$ for δ in a much larger range than previously known.

This chapter is organized as follows. In Section 4.2, we present some auxiliary lemmas. These lemmas together with our findings on q-cyclotomic cosets modulo $q^m - 1$ in Chapter 3 are then utilized to determine the dimension of some primitive BCH codes in Section 4.3. Moreover, we also apply the findings on q-cyclotomic cosets to obtain the Bose distance of some narrow-sense primitive BCH codes in Section 4.4. Furthermore, in Section 4.5, as an illustration of our main results, we present the dimension and Bose distance of narrow-sense primitive BCH codes $\mathcal{C}_{(q,n,\delta)}$ for $\delta = aq^{h+k} + b$, where k, a and b are integers satisfying $m - 2h \leq k \leq \lfloor (2m-1)/3 \rfloor - h]$, $1 \leq a \leq q-1$ and $1 \leq b \leq q^{m-h-k}$ and $q \nmid b$.

4.2 Auxiliary lemmas

Lemma 4.1. *Let m be a positive integer and t be a real number with $t < q^m$. Then*

$$\left| \left\{ (a_{m-1}, \ldots, a_0) \in Z_q^m : \sum_{\ell=0}^{m-1} a_\ell q^\ell \leq t, a_0 > 0 \right\} \right| = N(t+1).$$

Proof. There exists a one-to-one correspondence between the sequences in the above set and the integers in $[1, t]$ that are not divisible by q by mapping $(a_{m-1}, \ldots, a_0)$ to $\sum\limits_{\ell=0}^{m-1} a_\ell q^\ell$. Therefore, the result follows. □

Lemma 4.2. *Let $k \geq 0$ be an integer. Then*

$$\sum_{t=q^k}^{q^{k+1}-1} N(t+1) = \begin{cases} \frac{1}{2}(q^2 - q), & \text{if } k = 0, \\ \frac{1}{2} q^{2k-1}(q-1)^2(q+1), & \text{if } k \geq 1. \end{cases}$$

Proof. By definition, we first have

$$\sum_{t=q^k}^{q^{k+1}-1} N(t+1) = \sum_{t=q^k}^{q^{k+1}-1} t - \sum_{t=q^k}^{q^{k+1}-1} \lfloor t/q \rfloor. \tag{4.1}$$

Through direct computation, we obtain

$$\sum_{t=q^k}^{q^{k+1}-1} t = \begin{cases} \frac{1}{2}(q^2-q), & \text{if } k=0, \\ \frac{1}{2}(q^{2k+2}-q^{2k}-q^{k+1}+q^k), & \text{if } k \geq 1. \end{cases} \tag{4.2}$$

Next, we compute the value of $\sum_{t=q^k}^{q^{k+1}-1} \lfloor t/q \rfloor$. If $k=0$, then $\lfloor t/q \rfloor = 0$ for all $t \in \left[q^k, q^{k+1}-1\right]$, and hence $\sum_{t=q^k}^{q^{k+1}-1} \lfloor t/q \rfloor = 0$. If $k \geq 1$, then $\left[q^k, q^{k+1}-1\right]$ can be partitioned as

$$\left[q^k, q^{k+1}-1\right] = \bigsqcup_{i=0}^{q^{k-1}(q-1)-1} \left[q^k+iq, q^k+(i+1)q-1\right].$$

Moreover, for each integer $i \in \left[0, q^{k-1}(q-1)-1\right]$ and $t \in \left[q^k+iq, q^k+(i+1)q-1\right]$, we have $\lfloor t/q \rfloor = q^{k-1}+i$. Therefore,

$$\begin{aligned} \sum_{t=q^k}^{q^{k+1}-1} \lfloor t/q \rfloor &= \sum_{i=0}^{q^{k-1}(q-1)-1} \sum_{t=q^k+iq}^{q^k+(i+1)q-1} (q^{k-1}+i) \\ &= \frac{1}{2}\left(q^{2k+1}-q^{2k-1}-q^{k+1}+q^k\right) \end{aligned}$$

for $k \geq 1$. Combining (4.1), (4.2) and the value of $\sum_{t=q^k}^{q^{k+1}-1} \lfloor t/q \rfloor$, we obtain the desired equality. $\square$

Lemma 4.3. *Let k and $a \in [1,q]$ be two positive integers, and let i be an integer. Then we have*

$$\sum_{t=q^{k-i}, q\nmid t}^{aq^{k-i}-1} N(tq^{2i-1}+1) = \begin{cases} \frac{1}{2}(a^2-1)(q-1)^2 q^{2k-3}, & \text{if } i \in [-k+2, k-1], \\ \frac{1}{2}a(a-1)(q-1)q^{2k-2}, & \text{if } i = k \text{ or } -k+1, \end{cases} \tag{4.3}$$

and

$$\sum_{t=q^{k-i},q\nmid t}^{aq^{k-i}} N(tq^{2i}+1) = \begin{cases} \frac{1}{2}(a^2-1)(q-1)^2q^{2k-2}, & \textit{if } i \in [-k+1,k-1]\setminus\{0\}, \\ \frac{1}{2}a(a-1)(q-1)q^{2k-1}, & \textit{if } i=k \textit{ or } -k, \\ \begin{pmatrix} \frac{1}{2}(a^2-1)(q-1)^2q^{2k-2} \\ +\frac{1}{2}(a-1)(q-1)q^{k-1} \end{pmatrix}, & \textit{if } i=0. \end{cases} \tag{4.4}$$

Proof. The arguments to obtain the equations (4.3) and (4.4) are similar, so we only demonstrate here that equation (4.3) holds.

If $1 \leq i \leq k$, then we have $N(tq^{2i-1}+1) = tq^{2i-2}(q-1)$. It follows that

$$\sum_{t=q^{k-i},q\nmid t}^{aq^{k-i}-1} N(tq^{2i-1}+1) = \sum_{t=q^{k-i}}^{aq^{k-i}-1} tq^{2i-2}(q-1) - \sum_{t=\mathcal{W}_i}^{aq^{k-i}-1} tq^{2i-2}(q-1),$$

where $\mathcal{W}_i = \left[q^{k-i}, q^{k-i+1}-1\right] \cap \{t \in \mathbb{Z} : q \mid t\}$.

If $i=k$, then $\mathcal{W}_i = \varnothing$. Consequently,

$$\sum_{t\in\mathcal{W}_i} tq^{2i-2}(q-1) = 0 \quad \text{for } i=k.$$

If $1 \leq i \leq k-1$, then

$$\mathcal{W}_i = \{q^{k-i} + \alpha q : \alpha = 0, \ldots, a^{k-i-1}(a-1)-1\}.$$

Thus,

$$\begin{aligned} \sum_{t\in\mathcal{W}_i} tq^{2i-2}(q-1) = & \sum_{\alpha=0}^{q^{k-i-1}(a-1)-1} (q^{k-i}+\alpha q)q^{2i-2}(q-1) \\ = & \frac{1}{2}(a-1)(q-1)\left[(a+1)q^{2k-3} - q^{k+i-2}\right]. \end{aligned}$$

Furthermore, one can easily obtain

$$\sum_{t=q^{k-i}}^{aq^{k-i}-1} tq^{2i-2}(q-1) = \begin{cases} \frac{1}{2}a(a-1)q^{2k-2}(q-1), & \text{if } i=k, \\ \begin{pmatrix} \frac{1}{2}(a^2-1)(q-1)q^{2k-2} \\ -\frac{1}{2}(a-1)(q-1)q^{k+i-2} \end{pmatrix}, & \text{if } 1 \leq i \leq k-1. \end{cases}$$

Then we can conclude from the above four equations that the equality in (4.3) holds for $1 \leq i \leq k$.

If $-k+1 \leq i \leq 0$, then for any integer $t \in \left[q^{k-i}, aq^{k-i}-1\right] \cap \{t \in \mathbb{Z} : q \nmid t\}$ with the q-adic expansion $\sum_{\ell=0}^{k-i} t_\ell q^\ell$, we have the following observations:

- $N(tq^{2i-1}+1) = N(\lfloor tq^{2i-1} \rfloor + 1)$;
- The integer t admits the unique decomposition $t = \lfloor tq^{2i-1} \rfloor \cdot q^{-2i+1} + \sum_{\ell=0}^{-2i} t_\ell q^\ell$;
- As t ranges over integers in $\left[q^{k-i}, aq^{k-i}-1\right]$ not divisible by q, the value of $\lfloor tq^{2i-1} \rfloor$ ranges over integers from q^{k+i-1} to $aq^{k+i-1}-1$;
- For each fixed $\lfloor tq^{2i-1} \rfloor$, the summation $\sum_{\ell=0}^{-2i} t_\ell q^\ell$ ranges from the integers in $[1, q^{-2i+1}-1]$ not devisble by q, yielding exactly $q^{-2i}(q-1)$ distinct integers.

Therefore, for $-k+1 \leq i \leq 0$, we have

$$\sum_{t=q^{k-i}, q \nmid t}^{aq^{k-i}-1} N(tq^{2i-1}+1) = \sum_{\lfloor tq^{2i-1} \rfloor = q^{k+i-1}}^{aq^{k+i-1}-1} q^{-2i}(q-1) N\left(\lfloor tq^{2i-1} \rfloor + 1\right). \tag{4.5}$$

In addition, we can use a similar argument to the proof of Lemma 4.2 to obtain

$$\sum_{\lfloor tq^{2i-1} \rfloor = q^{k+i-1}}^{aq^{k+i-1}-1} N(\lfloor tq^{2i-1} \rfloor + 1) = \begin{cases} \frac{1}{2}(a^2-1)(q-1)q^{2k+2i-3}, & \text{if } -k+2 \leq i \leq 0, \\ \frac{1}{2}a(a-1)q^{2k+2i-2}, & \text{if } i = -k+1. \end{cases}$$

Substituting this into equation (4.5), we can conclude that equation (4.3) holds for $-k+1 \leq i \leq 0$. This completes the proof. □

4.3 Dimension of primitive BCH codes

Let $m \geq 4$ and $\delta \in [2, q^{\lfloor (2m-1)/3 \rfloor + 1}]$ be integers. Let $k_\delta = \lfloor \log_q(\delta - 1) \rfloor - h$. This implies that $q^{h+k_\delta} \leq \delta - 1 < q^{h+k_\delta+1}$. Let $\sum_{\ell=0}^{h+k_\delta} \delta_\ell q^\ell$ be the q-adic expansion of $\delta - 1$. If $k_\delta \geq m - 2h$, let s_δ denote the smallest integer in $[m - 2h - k_\delta, k_\delta]$ such that $\delta_{h+s_\delta} > 0$.

If m is odd, we define the function $f(\delta)$ for integers $\delta \in [2, q^{\lfloor (2m-1)/3 \rfloor + 1}]$ as follows:

$$f(\delta) = \begin{cases} 0, & \delta \leq q^{h+1}, \\ \begin{pmatrix} q^{2k_\delta - 3}(k_\delta - 1)(q-1)^2 \\ + N\left(\mu(\delta) + 1\right) \\ + \displaystyle\sum_{i=-k_\delta+1}^{k_\delta} \sum_{t \in \mathcal{T}_i(\delta)} N(tq^{2i-1} + 1) \end{pmatrix}, & \delta > q^{h+1}, \end{cases} \tag{4.6}$$

where

$$\mathcal{T}_i(\delta) = \left\{ t \in \mathbb{Z} : q^{k_\delta - i} \leq t < \sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^{\ell-h-i}, q \nmid t \right\}$$

and

$$\mu(\delta) = \min \left\{ \sum_{\ell=0}^{h-k_\delta} \delta_\ell q^\ell, \sum_{\ell=h-s_\delta+1}^{h+k_\delta} \delta_\ell q^{\ell-(h-s_\delta+1)} \right\}.$$

If m is even, we define the function $\widetilde{f}(\delta)$ for integers $\delta \in [2, q^{\lfloor (2m-1)/3 \rfloor + 1}]$ as follows:

$$\widetilde{f}(\delta) = \begin{cases} 0, & \delta \leq q^h, \\ \frac{1}{2}(\delta_h - 1)\delta_h + N(\widetilde{\mu}(\delta) + 1), & q^h < \delta \leq q^{h+1}, \\ \begin{pmatrix} (k_\delta - \frac{1}{2})q^{2k_\delta - 2}(q-1)^2 \\ + \frac{1}{2}q^{k_\delta - 1}(q-1) \\ + N(\widetilde{\mu}(\delta) + 1) \\ + \displaystyle\sum_{i=-k_\delta}^{k_\delta} \sum_{t \in \mathcal{T}_i(\delta)} N(tq^{2i} + 1) \end{pmatrix}, & \delta > q^{h+1}, \end{cases} \tag{4.7}$$

where $\widetilde{\mu}(\delta) = \min\left\{\sum_{\ell=0}^{h-k_\delta-1} \delta_\ell q^\ell, \sum_{\ell=h-s_\delta}^{h+k_\delta} \delta_\ell q^{\ell-(h-s_\delta)}\right\}$. We define the function $\tau(\delta)$ for integers $\delta \in (q^h, q^{\lfloor(2m-1)/3\rfloor+1}]$ as follows:

$$\tau(\delta) = \begin{cases} 1, & \text{if } \delta_h > 0 \text{ and } \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} \le \sum_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ 0, & \text{otherwise.} \end{cases}$$

In addition, we define the function $g(\delta)$ for integers $\delta \in [2, q^{\lfloor(2m-1)/3\rfloor+1}]$ as follows:

$$g(\delta) = \begin{cases} 0, & \delta \le q^h, \\ \delta_h - 1 + \tau(\delta), & q^h < \delta \le q^{h+1}, \\ N\left(\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h}\right) + \tau(\delta), & \delta > q^{h+1}. \end{cases} \tag{4.8}$$

Theorem 4.1. *Let $m \ge 4$ and $\delta \in \left[2, q^{\lfloor(2m-1)/3\rfloor+1}\right]$ be integers.*

- *If m is odd, then*

$$\dim(\mathcal{C}_{(q,n,\delta)}) = n - m\left[N(\delta) - f(\delta)\right]. \tag{4.9}$$

- *If m is even, then*

$$\dim(\mathcal{C}_{(q,n,\delta)}) = n - m\left[N(\delta) - \widetilde{f}(\delta)\right] - \frac{m}{2} g(\delta). \tag{4.10}$$

Outline of the proof. The proof is lengthy and involves intricate calculations. To provide clarity for the reader, we briefly outline the main strategy here. The complete argument is established through Assertions 4.1 – 4.4.

As established in equation (2.13), the dimension of $\mathcal{C}_{(q,n,\delta)}$ can be determined if we can identify all the coset leaders modulo n in the interval $[1, \delta - 1]$ and find the sizes of their corresponding q-cyclotomic cosets modulo n.

Our first step is to determine the coset sizes. Theorem 3.1 provides the size of any q-cyclotomic coset $C_n(a)$ for integers a in the range $[1, q^{m-\lfloor m/3\rfloor})$, which, given the condition $\delta \in \left[2, q^{\lfloor (2m-1)/3 \rfloor +1}\right]$, contains our interval of interest $[1, \delta - 1]$. Thus, the size of $C_n(a)$ is known for all $a \in [1, \delta - 1]$. We now consider the cases for odd and even m separately.

Case 1: m is odd. For an odd integer $m \geq 4$, Theorem 3.1 shows that $|C_n(a)| = m$ for all integers $a \in [1, q^{m - \lfloor m/3 \rfloor}]$. Consequently, for any integer $a \in [1, \delta - 1]$, the coset size $|C_n(a)| = m$. The general dimension formula from equation (2.13) therefore simplifies to:

$$\dim(\mathcal{C}_{(q,n,\delta)}) = n - m \cdot |\{a \in [1, \delta - 1] : a \text{ is a coset leader modulo } n\}|. \tag{4.11}$$

By applying Lemma 3.1 and recalling the definition of the set $\mathcal{S}$ from (3.9), the number of coset leaders in $[1, \delta - 1]$ is the count of integers in this range that are neither divisible by q nor belong to $\mathcal{S}$. This leads to:

$$|\{a \in [1, \delta - 1] : a \text{ is a coset leader modulo } n\}| = N(\delta) - |[1, \delta - 1] \cap \mathcal{S}|.$$

The core task is now to compute $|[1, \delta - 1] \cap \mathcal{S}|$. According to Theorem 3.2, this value is the sum of $|[1, \delta - 1] \cap \mathcal{A}_k(i)|$ over the relevant indices k and i. To evaluate this sum, we partition the interval $[1, \delta - 1]$ into several disjoint subintervals, as detailed in Assertions 4.1 – 4.4. Within each subinterval, we explicitly calculate the size of these intersections. Summing these results yields the final value for $|[1, \delta - 1] \cap \mathcal{S}|$, which we will show is precisely $f(\delta)$. Substituting this into equation (4.11) gives the desired dimension formula in (4.9) for odd m.

Case 2: m is even. The argument for an even m is similar but more complex because the coset size $|C_n(a)|$ can be either m or $m/2$. The dimension formula involves separating the leaders based on their coset size:

$$\dim(\mathcal{C}_{(q,n,\delta)}) = n - m \cdot |\mathcal{L}_m^n(1, \delta - 1)| - \frac{m}{2} \cdot |\mathcal{L}_{\frac{m}{2}}^n(1, \delta - 1)|,$$

where $\mathcal{L}_l^n(1, \delta - 1) = \{a \in [1, \delta - 1] : a \text{ is a leader modulo } n \text{ and } |C_n(a)| = l\}$. Recall the definitions of sets $\mathcal{H}$ and $\mathcal{S}$ in (3.6) and (3.9), respectively, where $\mathcal{H}$ precisely identifies the integers a for which $|C_n(a)| = m/2$. Using a similar partitioning strategy as in the odd case, we determine the number of leaders in each category. Specifically, we will show that:

- $|\mathcal{L}^n_{\frac{m}{2}}| = |[1, \delta - 1] \cap \mathcal{H}| = g(\delta)$,
- $|\mathcal{L}^n_m| = N(\delta) - |[1, \delta - 1] \cap (\mathcal{S} \cup \mathcal{H})| = N(\delta) - \widetilde{f}(\delta)$.

Substituting these quantities into the dimension formula yields the result for even m as stated in (4.10).

Our analysis begins with the upper portion of the interval $[1, \delta - 1]$. Specifically, we first focus on the subinterval $[q^{h+k_\delta}, \delta - 1]$ and partition it into two smaller, disjoint pieces based on the q-adic expansion of $\delta - 1$. Assertions 4.1 and 4.2 then compute the required intersection sizes on these two pieces, respectively.

Assertion 4.1. *Suppose that* $q^{m-h} < \delta \leq q^{\lfloor (2m-1)/3 \rfloor + 1}$.

- *If* m *is odd, then*

$$\left| \left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell, \delta - 1 \right] \cap \mathcal{S} \right| = N(\mu(\delta) + 1). \tag{4.12}$$

- *If* m *is even, then*

$$\left| \left[\sum_{\ell=h-k_\delta}^{h+k_\delta} \delta_\ell q^\ell, \delta - 1 \right] \cap (\mathcal{S} \cup \mathcal{H}) \right| = N(\widetilde{\mu}(\delta) + 1) \tag{4.13}$$

  and

$$\left| \left[\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell, \delta - 1 \right] \cap \mathcal{H} \right| = \tau(\delta). \tag{4.14}$$

Proof. If m is odd, our first goal is to show that

$$\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell,\delta-1\right]\cap\mathcal{S}=\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell,\delta-1\right]\cap\mathcal{A}_{k_\delta}(s_\delta). \tag{4.15}$$

Recall that $\sum_{\ell=0}^{h+k_\delta}\delta_\ell q^\ell$ is the q-adic expansion of $\delta-1$. We have

$$V(\delta-1)=(\mathbf{0}_{h-k_\delta},\delta_{h+k_\delta},\ldots,\delta_0)$$

and

$$V\left(\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell\right)=(\mathbf{0}_{h-k_\delta},\delta_{h+k_\delta},\ldots,\delta_{h-k_\delta+1},\mathbf{0}_{h-k_\delta+1}).$$

Suppose that $a\in\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell,\delta-1\right]$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k_\delta}a_\ell q^\ell$.

It follows that $V(\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell)\le V(a)\le V(\delta-1)$. The above two equalities imply that

$$\begin{aligned}V(a)&=(\mathbf{0}_{h-k_\delta},a_{h+k_\delta},\ldots,a_0)\\&=(\mathbf{0}_{h-k_\delta},\delta_{h+k_\delta},\ldots,\delta_{h-k_\delta+1},a_{h-k_\delta},\ldots,a_0).\end{aligned} \tag{4.16}$$

Recalling the definition of s_δ, it follows that s_δ is the smallest integer in $[-k_\delta+1,k_\delta]$ such that $a_{h+s_\delta}>0$. By Remark 3.5, this implies that $a\notin\mathcal{A}_{k_\delta}(i)$ for any integer $i\neq s_\delta$. Therefore, $\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell,\delta-1\right]\cap\mathcal{A}_{k_\delta}(i)=\varnothing$ for any integer $i\neq s_\delta$. Then applying Theorem 3.2, we can conclude that (4.15) holds.

Now, let us count the number of integers in the set $\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell,\delta-1\right]\cap\mathcal{A}_{k_\delta}(s_\delta)$.

By the definition of $\mathcal{A}_{k_\delta}(s_\delta)$ and (4.16), we can conclude that

$$a\in\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell,\delta-1\right]\cap\mathcal{A}_{k_\delta}(s_\delta)$$

if and only if $V(a)$ has the form

$$(\mathbf{0}_{h-k_\delta}, \delta_{h+k_\delta}, \ldots, \delta_{h+s_\delta}, \mathbf{0}_{h-k_\delta}, a_{k_\delta+s_\delta-1}, \ldots, a_0)$$

with $\sum_{\ell=0}^{k_\delta+s_\delta-1} a_\ell q^\ell \leq \mu(\delta)$ and $a_0 > 0$. Consequently, we have

$$\begin{aligned}
&\left| \left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell, \delta - 1 \right] \cap \mathcal{A}_{k_\delta}(s_\delta) \right| \\
= &\left| \left\{ (a_{k_\delta+s_\delta-1}, \ldots, a_0) \in Z_q^{k_\delta+s_\delta} : \sum_{\ell=0}^{k_\delta+s_\delta-1} a_\ell q^\ell \leq \mu(\delta), a_0 > 0 \right\} \right|.
\end{aligned}$$

Noticing that $\mu(\delta) < q^{k_\delta+s_\delta}$, we apply Lemma 4.1 to obtain

$$\left| \left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell, \delta - 1 \right] \cap \mathcal{A}_{k_\delta}(s_\delta) \right| = N(\mu(\delta) + 1).$$

Recalling the equality in (4.15), it follows that equation (4.12) holds.

If m is even, we can apply a similar method as above to derive equation (4.13). Next, we establish equation (4.14). We can employ an analogous argument to that used in deriving (4.16) to conclude that $V(a)$ takes the form

$$(\mathbf{0}_{h-k_\delta-1}, \delta_{h+k_\delta}, \ldots, \delta_h, a_{h-1}, \ldots, a_0)$$

for any integer $a \in \left[\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell, \delta - 1 \right]$. Applying Corollary 3.3, it follows that an integer $a \in \left[\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell, \delta - 1 \right] \cap \mathcal{H}$ if and only if $V(a)$ has the form

$$(\mathbf{0}_{h-k_\delta-1}, \delta_{h+k_\delta}, \ldots, \delta_h, \mathbf{0}_{h-k_\delta-1}, \delta_{h+k_\delta}, \ldots, \delta_h)$$

with $\delta_h > 0$ and $\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} \leq \sum_{\ell=0}^{h-1} \delta_\ell q^\ell$. This implies that equation (4.14) holds. $\square$

Assertion 4.2. *Suppose that* $q^{m-h} < \delta \leq q^{\lfloor (2m-1)/3 \rfloor + 1}$.

- *If* m *is odd, then*

$$\left| \left[q^{h+k_\delta}, \sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{S} \right| = \sum_{i=-k_\delta+1}^{k_\delta} \sum_{t \in \mathcal{T}_i(\delta)} N(tq^{2i-1}+1). \tag{4.17}$$

- *If* m *is even, then*

$$\left| \left[q^{h+k_\delta}, \sum_{\ell=h-k_\delta}^{h+k_\delta} \delta_\ell q^\ell \right) \cap (\mathcal{S} \cup \mathcal{H}) \right| = \sum_{i=-k_\delta}^{k_\delta} \sum_{t \in \mathcal{T}_i(\delta)} N(tq^{2i}+1) \tag{4.18}$$

and

$$\left| \left[q^{h+k_\delta}, \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{H} \right| = N \left(\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} \right) - N \left(q^{k_\delta} \right). \tag{4.19}$$

Proof. If m is odd, we have $k_\delta \geq m - 2h = 1$. By the definition of $\mathcal{A}_{k_\delta}(i)$, we can conclude that an integer $a \in \left[q^{h+k_\delta}, \sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{A}_{k_\delta}(i)$ if and only if

$$V(q^{h+k_\delta}) \leq V(a) < V(\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell), \tag{4.20}$$

and $V(a)$ has form specified in (3.12) with $k = k_\delta$ while satisfying the conditions in (3.10) and (3.11). Notice that

$$V(q^{h+k_\delta}) = (\mathbf{0}_{h-k_\delta}, 1, \mathbf{0}_{h+k_\delta})$$

and

$$V(\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell) = (\mathbf{0}_{h-k_\delta}, \delta_{h+k_\delta}, \ldots, \delta_{h-k_\delta+1}, \mathbf{0}_{h-k_\delta+1}).$$

The form of $V(a)$ in (3.12) and the inequality $a_0 > 0$ in (3.11) imply that the inequality in (4.20) holds if and only if

$$(1, \mathbf{0}_{2k_\delta-1}) \leq (a_{h+k_\delta}, \ldots, a_{h+i}, \mathbf{0}_{k_\delta+i-1})$$
$$< (\delta_{h+k_\delta}, \ldots, \delta_{h-k_\delta+1}).$$

Since s_δ is the smallest integer in $[-k_\delta+1, k_\delta]$ such that $\delta_{h+s_\delta} > 0$, this is further equivalent to

$$q^{k_\delta - i} \leq \sum_{\ell=h+i}^{h+k_\delta} a_\ell q^{\ell-(h+i)} < \sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^{\ell-h-i}.$$

Recall the definition of the set $\mathcal{T}_i(\delta)$ and Remarks 3.2 and 3.3. We can conclude that an integer $a \in \left[q^{h+k_\delta}, \sum\limits_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell\right) \cap \mathcal{A}_{k_\delta}(i)$ if and only if $V(a)$ has the form specified in (3.12) with $k = k_\delta$ and

$$\sum_{\ell=h+i}^{h+k_\delta} a_\ell q^{\ell-(h+i)} \in \mathcal{T}_i(\delta); \tag{4.21}$$

$$\sum_{\ell=0}^{k_\delta+i-1} a_\ell q^\ell \leq \sum_{h+i}^{h+k_\delta} a_\ell q^{\ell-(h+i)} \cdot q^{2i-1} \text{ and } a_0 > 0. \tag{4.22}$$

To enumerate such integers, we have the following observations:

- Each sequence $(a_{h+k_\delta}, \ldots, a_{h+i})$ satisfying (4.21) corresponds to one integer $t = \sum\limits_{\ell=h+i}^{h+k_\delta} a_\ell q^{\ell-(h+i)}$ in the set $\mathcal{T}_i(\delta)$, and vice versa.

- For each fixed $(a_{h+k_\delta}, \ldots, a_{h+i})$, Lemma 4.1 yields that there exist exactly $N(tq^{2i-1}+1)$ sequences $(a_{k_\delta+i-1}, \ldots, a_0)$ meeting the requirement in (4.22), where $t = \sum\limits_{\ell=h+i}^{h+k_\delta} a_\ell q^{\ell-(h+i)}$.

Therefore, we can conclude that for any integer $i \in [-k_\delta + 1, k_\delta]$.

$$\left| \left[q^{h+k_\delta}, \sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{A}_{k_\delta}(i) \right| = \sum_{t \in \mathcal{T}_i(\delta)} N(tq^{2i-1} + 1).$$

Then by Theorem 3.2, we obtain the equality in (4.17).

If m is an even integer, then $k_\delta \geq m - 2h = 0$. The equality in (4.18) can be obtained using a similar argument as presented above. Next, we establish equation (4.19).

By applying Corollary 3.1, we can conclude that an integer

$$a \in \left[q^{h+k_\delta}, \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{H}$$

if and only if

$$V(q^{h+k_\delta}) \leq V(a) < V(\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell) \tag{4.23}$$

and $V(a)$ has the form specified in (3.7) with $k = k_\delta$ and $a_0 > 0$. Noting that $V(q^{h+k_\delta}) = (\mathbf{0}_{h-k_\delta}, 1, \mathbf{0}_{h+k_\delta})$ and $V(\sum\limits_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell) = (\mathbf{0}_{h-k_\delta}, \delta_{h+k_\delta}, \ldots, \delta_h, \mathbf{0}_h)$, it follows that the inequality in (4.23) holds if and only if

$$(1, \mathbf{0}_{k_\delta}) \leq (a_{k_\delta}, \ldots, a_0) < (\delta_{h+k_\delta}, \ldots, \delta_h).$$

This can be equivalently represented as

$$q^{k_\delta} \leq \sum_{\ell=0}^{k_\delta} a_\ell q^\ell < \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h}.$$

Consequently, we have

$$\left| \left[q^{h+k_\delta}, \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{H} \right| = \left| \left\{ (a_{k_\delta}, \ldots, a_0) : q^{k_\delta} \leq \sum_{\ell=0}^{k_\delta} a_\ell q^\ell < \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h}, a_0 > 0. \right\} \right|$$

By Lemma 4.1, it follows that equation (4.19) holds. $\square$

Having analyzed the interval $\left[q^{h+k_\delta}, \delta-1\right]$ in Assertions 4.1 and 4.2, we now turn to the remaining part, $\left[1, q^{h+k_\delta}\right)$. For an odd m, we aim to compute $\left|\left[1, q^{h+k_\delta}\right) \cap \mathcal{S}\right|$. By Lemma 3.3, the intersection over the first part of this interval is zero, i.e., $\left|\left[1, q^{h+1}-1\right] \cap \mathcal{S}\right| = 0$. The remainder is handled by the decomposition

$$\left|\left[q^{h+1}, q^{h+k_\delta}\right) \cap \mathcal{S}\right| = \sum_{k=1}^{k_\delta - 1} \left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{S}\right|.$$

By Theorem 3.2, each term $\left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{S}\right|$ is a sum of $|\mathcal{A}_k(i)|$ over integers $i \in [-k+1, k]$. For an even m, a similar analysis requires the sizes of the sets $\mathcal{B}_k(i)$. The following assertions provide these required sizes.

Assertion 4.3. *Suppose that $k \in [1, \lfloor (2m-1)/3 \rfloor - h]$ is an integer.*

- *If m is odd, then*

$$|\mathcal{A}_k(i)| = \begin{cases} \frac{1}{2} q^{2k-1} (q-1)^2, & \text{if } i = k \text{ or } -k+1, \\ \frac{1}{2} q^{2k-3} (q-1)^3 (q+1), & \text{if } i \in [-k+2, k-1]. \end{cases} \tag{4.24}$$

- *If m is even, then*

$$|\mathcal{B}_k(i)| = \begin{cases} \frac{1}{2} q^{2k} (q-1)^2, & \text{if } i = k \text{ or } -k, \\ \frac{1}{2} q^{2k-2} (q-1)^3 (q+1), & \text{if } i \in [-k+1, k-1] \setminus \{0\}. \end{cases} \tag{4.25}$$

Proof. The arguments to obtain (4.24) and (4.25) are similar, so we here only demonstrate that (4.24) holds if m is odd. We can use the same approach as in the proof of Assertion 4.2 to conclude that an integer $a \in \mathcal{A}_k(i)$ if and only if $V(a)$ has the form specified in (3.12) with

$$\sum_{\ell=h+i}^{h+k} a_\ell q^{l-(h+i)} \in \left[q^{k-i}, q^{k-i+1}-1\right] \cap \{t \in \mathbb{Z} : q \nmid t\}; \tag{4.26}$$

$$\sum_{\ell=0}^{k+i-1} a_\ell q^\ell \leq \sum_{\ell=h+i}^{h+k} a_\ell q^{\ell-(h+i)} \cdot q^{2i-1} \text{ and } a_0 > 0. \tag{4.27}$$

Furthermore, we have the following observations:

- Each sequence $(a_{h+k}, \ldots, a_{h+i})$ satisfying (4.26) corresponds to one integer $t = \sum\limits_{\ell=h+i}^{h+k} a_\ell q^{\ell-(h+i)}$ in the set $[q^{k-i}, q^{k-i+1}-1] \cap \{t \in \mathbb{Z} \mid q \nmid t\}$, and vice versa.
- For each fixed sequence $(a_{h+k}, \ldots, a_{h+i})$, we can utilize Lemma 4.1 to conclude that there exist $N(tq^{2i-1}+1)$ sequences $(a_{k+i-1}, \ldots, a_0) \in Z_q^{k+i}$ satisfying (4.27), where $t = \sum\limits_{\ell=h+i}^{h+k} a_\ell q^{\ell-(h+i)}$.

Consequently, we conclude that

$$|\mathcal{A}_k(i)| = \sum_{t=q^{k-i}, q \nmid t}^{q^{k-i+1}-1} N(tq^{2i-1}+1).$$

Then applying Lemma 4.3 with $a = q$, we derive (4.24). $\square$

Assertion 4.4. *Suppose that m is even and $k \in [0, \lfloor (2m-1)/3 \rfloor - h]$ is an integer. Then*

$$|\mathcal{B}_k(0)| = \begin{cases} \frac{1}{2}q(q-1), & \text{if } k = 0, \\ \frac{1}{2}(q-1)^2(q^{2k} - q^{2k-2} + q^{k-1}), & \text{if } k \geq 1. \end{cases}$$

Proof. By the definition of $\mathcal{B}_k(0)$, we can use a similar argument as in the proof of Assertion 4.2 to derive

$$|\mathcal{B}_k(0)| = \sum_{t=q^k, q \nmid t}^{q^{k+1}-1} N(t+1).$$

If $k \geq 1$, by substituting $i = 0$ and $a = q$ into equation (4.4) in Lemma 4.3, we obtain

$$|\mathcal{B}_k(0)| = \frac{1}{2}(q-1)^2(q^{2k} - q^{2k-2} + q^{k-1}).$$

If $k = 0$, then we have

$$|\mathcal{B}_k(0)| = \sum_{t=1}^{q-1} N(t+1) = \frac{1}{2}q(q-1).$$

This completes the proof of Assertion 4.4. □

Proof of Theorem 4.1. If m is odd, we first aim to show that

$$|[1, \delta - 1] \cap \mathcal{S}| = f(\delta) \quad \text{for } \delta \in \left[2, q^{\lfloor (2m-1)/3 \rfloor + 1}\right]. \tag{4.28}$$

If $2 \leq \delta \leq q^{h+1}$, recalling the definition of $\mathcal{S}$ and applying Lemma 3.3, we can obtain

$$[1, \delta - 1] \cap \mathcal{S}| = 0. \tag{4.29}$$

In particular,

$$\left|\left[1, q^{h+1} - 1\right] \cap \mathcal{S}\right]\right| = 0. \tag{4.30}$$

If $q^{h+1} < \delta \leq q^{\lfloor (2m-1)/3 \rfloor + 1}$, since m is odd, we first have

- $1 \leq k_\delta \leq \lfloor (2m-1)/3 \rfloor - h$;
- $q^{m-h} < \delta \leq q^{\lfloor (2m-1)/3 \rfloor + 1}$.

By applying Theorem 3.2, we can conclude from Assertion 4.3 that for any integer $k \in [1, \lfloor (2m-1)/3 \rfloor - h]$,

$$\begin{aligned} \left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{S}\right| = & \sum_{i=-k+1}^{k} |\mathcal{A}_k(i)| \\ = & (k-1)q^{2k-3}(q-1)^3(q+1) + \ q^{2k-1}(q-1)^2. \end{aligned}$$

Therefore, we have

$$
\begin{aligned}
\left|\left[q^{h+1}, q^{h+k_\delta}\right) \cap \mathcal{S}\right| &= \sum_{k=1}^{k_\delta-1} \left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{S}\right| \\
&= \sum_{k=1}^{k_\delta-1} (k-1)q^{2k-3}(q-1)^3(q+1) + \sum_{k=1}^{k_\delta-1} q^{2k-1}(q-1)^2.
\end{aligned}
$$

It is easy to verify that

$$
\sum_{k=1}^{k_\delta-1} q^{2k-1}(q-1)^2 = \frac{(q^{2k_\delta-1}-q)(q-1)}{q+1}
$$

and

$$
\sum_{k=1}^{k_\delta-1} (k-1)q^{2k-3}(q-1)^3(q+1) = \frac{\left[q-(k_\delta-1)q^{2k_\delta-3}+(k_\delta-2)q^{2k_\delta-1}\right](q-1)}{q+1}.
$$

By adding these two sums together, we have

$$
\left|\left[q^{h+1}, q^{h+k_\delta}\right) \cap \mathcal{S}\right| = (k_\delta-1)q^{2k_\delta-3}(q-1)^2. \tag{4.31}
$$

We can also conclude from Assertions 4.1 and 4.2 that

$$
\begin{aligned}
\left|\left[q^{h+k_\delta}, \delta-1\right] \cap \mathcal{S}\right| &= \left|\left[q^{h+k_\delta}, \sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell\right) \cap \mathcal{S}\right| + \left|\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta q^\ell, \delta-1\right] \cap \mathcal{S}\right| \\
&= \sum_{i=-k_\delta+1}^{k_\delta} \sum_{t\in\mathcal{T}_i(\delta)} N(tq^{2i-1}+1) + N(\mu(\delta)+1).
\end{aligned}
$$

It follows from (4.30), (4.31) and (4.32) that

$$
\begin{aligned}
|[1,\delta-1]\cap\mathcal{S}| &= \left|\left[1, q^{h+1}-1\right] \cap \mathcal{S}\right| + \left|\left[q^{h+1}, q^{h+k_\delta}\right) \cap \mathcal{S}\right| + \left|\left[q^{h+k_\delta}, \delta-1\right] \cap \mathcal{S}\right| \\
&= (k_\delta-1)q^{2k_\delta-3}(q-1)^2 + N(\mu(\delta)+1) + \sum_{i=k_\delta+1}^{k_\delta} \sum_{t\in\mathcal{T}_i(\delta)} N(tq^{2i-1}+1).
\end{aligned}
$$

By the definition of the function $f(\delta)$, we now can conclude from (4.29) and (4.32) that equation (4.28) holds. Recalling the fact that an integer cannot be a coset leader if $q \mid a$, and the definition of $\mathcal{S}$, it follows that

$$|\mathcal{L}^n(1, \delta - 1)| = N(\delta) - f(\delta) \tag{4.31}$$

for any integer $\delta \in \left[2, q^{\lfloor (2m-1)/3 \rfloor + 1}\right]$. In addition, it is easy to verify that

$$\lfloor (2m-1)/3 \rfloor + 1 \leq m - \lfloor m/3 \rfloor.$$

This implies that $\delta - 1 < q^{\lfloor (2m-1)/3 \rfloor + 1} \leq q^{m - \lfloor m/3 \rfloor}$. Then applying Theorem 3.1, we have

$$|C_n(a)| = m \quad \text{for any integer } a \in [1, \delta - 1]. \tag{4.32}$$

Recalling equation (2.13), we obtain (4.9) from (4.31) and (4.32).

If m is even, our first goal is to to establish

$$|[1, \delta - 1] \cap (\mathcal{S} \cup \mathcal{H})| = \widetilde{f}(\delta) \tag{4.33}$$

and

$$|[1, \delta - 1] \cap \mathcal{H}| = g(\delta) \tag{4.34}$$

for any integer $\delta \in \left[2, q^{\lfloor (2m-1)/3 \rfloor + 1}\right]$.

If $2 \leq \delta \leq q^h$, we can apply Lemma 3.3 to conclude that

$$|[1, \delta - 1] \cap \mathcal{S}| = 0.$$

In addition, by applying Corollary 3.2, we obtain

$$|[1, \delta - 1] \cap \mathcal{H}| = 0.$$

In particular, we have

$$|[1, q^h - 1] \cap (\mathcal{S} \cup \mathcal{H})| = 0 \tag{4.35}$$

and

$$|[1, q^h - 1] \cap \mathcal{H}| = 0. \tag{4.36}$$

If $q^h < \delta \leq q^{h+1}$, since m is even, we first have

- $k_\delta = 0$;
- $\mathcal{T}_0(\delta) = \{t \in \mathbb{Z} : 1 \leq t \leq \delta_h - 1\}$;
- $q^{m-h} < \delta \leq q^{\lfloor (2m-1)/3 \rfloor + 1}$.

Therefore, by substituting $k_\delta = 0$ into (4.13) and (4.18), we obtain

$$\left|\left[\delta_h q^h, \delta - 1\right] \cap (\mathcal{S} \cup \mathcal{H})\right| = N(\widetilde{\mu}(\delta) + 1)$$

and

$$\left|\left[q^h, \delta_h q^h\right) \cap (\mathcal{S} \cup \mathcal{H})\right| = \sum_{t \in \mathcal{T}_0(\delta)} N(t+1) = \frac{1}{2}(\delta_h - 1)\delta_h.$$

With (4.35), it follows that

$$|[1, \delta - 1] \cap (\mathcal{S} \cup \mathcal{H})| = \frac{1}{2}(\delta_h - 1)\delta_h + N(\widetilde{\mu}(\delta) + 1). \tag{4.37}$$

Additionally, by substituting $k_\delta = 0$ into (4.14) and (4.19), we obtain

$$\left|\left[\delta_h q^h, \delta - 1\right] \cap \mathcal{H}\right| = \tau(\delta)$$

and

$$\left|\left[q^h, \delta_h q^h\right) \cap \mathcal{H}\right| = \delta_h - 1.$$

Combing these two equalities with (4.36), we obtain

$$|[1, \delta - 1] \cap \mathcal{H}| = \delta_h - 1 + \tau(\delta). \tag{4.38}$$

By now we have already demonstrated that both (4.33) and (4.34) hold for $2 \leq \delta \leq q^{h+1}$.

Notice that $q^{h+1}-1=\sum\limits_{\ell=0}^{h}(q-1)q^{\ell}$. Therefore, for $\delta=q^{h+1}$, we have $\tau(\delta)=1$ and $\widetilde{\mu}(\delta)=q-1$. Consequently, we can conclude from (4.37) and (4.38) that

$$\big|\big[1,q^{h+1}-1\big]\cap(\mathcal{S}\cup\mathcal{H})\big|=\frac{1}{2}q(q-1) \tag{4.39}$$

and

$$\big|\big[1,q^{h+1}-1\big]\cap\mathcal{H}\big|=q-1. \tag{4.40}$$

If $q^{h+1}<\delta\leq q^{\lfloor(2m-1)/3\rfloor+1}$, since m is even, we have

- $1\leq k_{\delta}\leq\lfloor(2m-1)/3\rfloor-h$;
- $q^{m-h}<\delta\leq q^{\lfloor(2m-1)/3\rfloor+1}$

By applying Theorem 3.2, we can conclude from Assertions 4.3 and 4.4 to conclude that for $k\in[1,\lfloor(2m-1)/3\rfloor-h]$,

$$\begin{aligned}\big|\big[q^{h+k},q^{h+k+1}\big)\cap(\mathcal{S}\cup\mathcal{H})\big|=&\sum_{i=-k}^{k}|\mathcal{B}_k(i)|\\ =&(k-\frac{1}{2})q^{2k-2}(q-1)^3(q+1)+\ (q-1)^2(\frac{1}{2}q^{k-1}+q^{2k}).\end{aligned}$$

It follows that

$$\begin{aligned}\big|\big[q^{h+1},q^{h+k_{\delta}}\big)\cap(\mathcal{S}\cup\mathcal{H})\big|=&\sum_{k=1}^{k_{\delta}-1}\big|\big[q^{h+k},q^{h+k+1}\big)\cap(\mathcal{S}\cup\mathcal{H})\big|\\ =&(k_{\delta}-\frac{1}{2})q^{2k_{\delta}-2}(q-1)^2+\frac{1}{2}(q-1)(q^{k_{\delta}-1}-q).\end{aligned}$$

We can also conclude from Assertions 4.1 and 4.2 that

$$\big|\big[q^{h+k_{\delta}},\delta-1\big]\cap(\mathcal{S}\cup\mathcal{H})\big|=\sum_{i=-k_{\delta}}^{k_{\delta}}\sum_{t\in\mathcal{T}_i(\delta)}N(tq^{2i}+1)+\ N(\widetilde{\mu}(\delta)+1). \tag{4.41}$$

Combining (4.39), (4.41) and (4.41), we obtain

$$\begin{aligned}
&|[1,\delta-1]\cap(\mathcal{S}\cup\mathcal{H})| \\
=&\left|\left[1,q^{h+1}\right)\cap(\mathcal{S}\cup\mathcal{H})\right| + \left|\left[q^{h+1},q^{h+k_\delta}\right)\cap(\mathcal{S}\cup\mathcal{H})\right| + \left|\left[q^{h+k_\delta},\delta-1\right]\cap(\mathcal{S}\cup\mathcal{H})\right| \\
=&(k_\delta-\frac{1}{2})q^{2k_\delta-2}(q-1)^2+\frac{1}{2}q^{k_\delta-1}(q-1)+N(\widetilde{\mu}(\delta)+1)+\sum_{i=-k_\delta}^{k_\delta}\sum_{t\in\mathcal{T}_i(\delta)}N(tq^{2i}+1)
\end{aligned}$$

for $q^{h+1}<\delta\leq q^{\lfloor(2m-1)/3\rfloor+1}$.

In addition, by applying Corollary 3.4, we have

$$\begin{aligned}
\left|\left[q^{h+1},q^{h+k_\delta}\right)\cap\mathcal{H}\right| &= \sum_{k=1}^{k_\delta-1}|[q^{h+k},q^{h+k+1})\cap\mathcal{H}| \\
&= (q^{k_\delta-1}-1)(q-1).
\end{aligned}$$

With (4.40), it follows that

$$\left|\left[1,q^{h+k_\delta}\right)\cap\mathcal{H}\right| = q^{k_\delta-1}(q-1). \tag{4.42}$$

Noting that $N(q^{k_\delta})=q^{k_\delta-1}(q-1)$ for $k_\delta\geq 1$, we can combine (4.14), (4.19) and (4.42) to obtain

$$\begin{aligned}
|[1,\delta-1]\cap\mathcal{H}| &= |[1,q^{h+k_\delta})\cap\mathcal{H}|+\left|\left[q^{h+k_\delta},\sum_{\ell=h}^{h+k_\delta}\delta_\ell q^\ell\right)\cap\mathcal{H}\right|+\left|\left[\sum_{\ell=h}^{h+k_\delta}\delta_\ell q^\ell,\delta-1\right]\cap\mathcal{H}\right| \\
&= N\left(\sum_{\ell=h}^{h+k_\delta}\delta_\ell q^{\ell-h}\right)+\tau(\delta).
\end{aligned}$$

We now have showed that (4.33) and (4.34) also hold for $q^{h+1}<\delta\leq q^{\lfloor(2m-1)/3\rfloor+1}$.

Next, we establish equation (4.10). Note that $\delta\leq q^{\lfloor(2m-1)/3\rfloor+1}\leq q^{m-\lfloor m/4\rfloor}$ for even m. Thus, by Theorem 3.1, we have $|C_a|=m$ or $|C_a|=m/2$ for any integer $a\in[1,\delta-1]$. Recall the definitions of $\mathcal{S}$ and $\mathcal{H}$. We can conclude from (4.33) and (4.34) that

$$|\mathcal{L}_m^n(1,\delta-1)| = N(\delta)-\widetilde{f}(\delta) \quad \text{and} \quad |\mathcal{L}_{\frac{m}{2}}^n(1,\delta-1)| = g(\delta). \tag{4.43}$$

Consequently, we conclude that the equality in (4.10) holds. This completes the proof of Theorem 4.1. $\square$

As examples of Theorem 4.1, we present the following two corollaries, which give explicit formulas to compute the dimension of $\mathcal{C}_{(q,n,\delta)}$ for $\delta \in \left[2, q^{\lceil \frac{m}{2} \rceil+1}\right]$. It can be verified that these two corollaries are equivalent to Theorem 17 and Theorem 18 in [39], respectively.

Corollary 4.1. *Let $m \geq 4$ be an even integer and $\delta \in [2, q^{h+1}]$ be an integer. Then*

$$\dim(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} n - mN(\delta), & \text{if } \delta \leq q^h, \\ n - m\left(N(\delta) - \frac{1}{2}\delta_h^2\right), & \text{if } \delta > q^h \text{ and } \delta_h \leq \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ n - m\left[N(\delta) - \frac{1}{2}(\delta_h - 1)^2 - \delta_0\right], & \text{if } \delta > q^h \text{ and } \delta_h > \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell. \end{cases}$$

Proof. We consider the following cases:

Case 1. If $\delta \leq q^h$, we immediately have $\widetilde{f}(\delta) = 0$ and $g(\delta) = 0$ by definition.

Case 2. If $\delta > q^h$, we can observe that $\delta_h > 0$ and $s_\delta = k_\delta = 0$. Then we distinguish the following two subcases:

Subcase 1. If $\delta_h \leq \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell$, then $\tau(\delta) = 1$ and $\widetilde{\mu}(\delta) = \delta_h$, which implies that

$$\widetilde{f}(\delta) = \frac{1}{2}(\delta_h - 1)\delta_h + \delta_h \quad \text{and} \quad g(\delta) = \delta_h.$$

Subcase 2. If $\delta_h > \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell$, then $\tau(\delta) = 0$ and $\widetilde{\mu}(\delta) = \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell = \delta_0$, which implies that

$$\widetilde{f}(\delta) = \frac{1}{2}(\delta_h - 1)\delta_h + \delta_0 \quad \text{and} \quad g(\delta) = \delta_h - 1.$$

By substituting the values of $\widetilde{f}(\delta)$ and $g(\delta)$ into equation (4.10) for each corresponding case, we obtain the desired equality. $\square$

Corollary 4.2. *Let $m \geq 5$ be an odd integer and $\delta \in [2, q^{h+2}]$ be an integer. Then*

$$\dim(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} n - mN(\delta), \ \ \textit{if } \delta \leq q^{h+1}, \\ n - m\left[N(\delta) - (q-1)\delta_{h+1}^2 - (\delta_h - 1)\delta_{h+1} - \delta_0\right], \\ \quad \textit{if } \delta > q^{h+1}, \delta_h > 0 \textit{ and } \delta_{h+1} > \sum_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ n - m\left[N(\delta) - (q-1)\delta_{h+1}^2 - \delta_h\delta_{h+1}\right], \\ \quad \textit{if } \delta > q^{h+1}, \delta_h > 0 \textit{ and } \delta_{h+1} \leq \sum_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ n - m\left[N(\delta) - (q-1)(\delta_{h+1}^2 - \delta_{h+1} + \delta_1) - \delta_0\right], \\ \quad \textit{if } \delta > q^{h+1}, \delta_h = 0 \textit{ and } \delta_{h+1}q > \sum_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ n - m\left[N(\delta) - (q-1)\delta_{h+1}^2\right], \\ \quad \textit{if } \delta > q^{h+1}, \delta_h = 0 \textit{ and } \delta_{h+1}q \leq \sum_{\ell=0}^{h-1} \delta_\ell q^\ell. \end{cases}$$

Proof. We consider the following cases:

Case 1. If $\delta \leq q^{h+1}$, we can directly have $f(\delta) = 0$ by definition.

Case 2. If $\delta > q^{h+1}$, we have $k_\delta = 1$, then we distinguish the following subcases:

Subcase 1. If $\delta_h > 0$, then $s_\delta = 0$, which leads to

- $\mathcal{T}_0(\delta) = [q, \delta_{h+1}q + \delta_h - 1] \cap \{t \in \mathbb{Z} : q \nmid t\}$;
- $\mathcal{T}_1(\delta) = [1, \delta_{h+1}]$;
- $\mu(\delta) = \min\left\{\delta_{h+1}, \sum_{\ell=0}^{h-1} \delta_\ell q^\ell\right\}$.

Noticing that $\mu(\delta) = \sum_{\ell=0}^{h-1} \delta_\ell q^\ell = \delta_0$ if $\delta_{h+1} > \sum_{\ell=0}^{h-1} \delta_\ell q^\ell$, we can substitute these terms into equation (4.6) to obtain

$$f(\delta) = \begin{cases} (q-1)\delta_{h+1}^2 + (\delta_h - 1)\delta_{h+1} + \delta_0, & \text{if } \delta_h > 0 \text{ and } \delta_{h+1} > \sum_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ (q-1)\delta_{h+1}^2 + \delta_h\delta_{h+1}, & \text{if } \delta_h > 0 \text{ and } \delta_{h+1} \leq \sum_{\ell=0}^{h-1} \delta_\ell q^\ell. \end{cases}$$

Subcase 2. If $\delta_h = 0$, then $s_\delta = 1$, which leads to

- $\mathcal{T}_0(\delta) = [q, \delta_{h+1}q - 1] \cap \{t \in \mathbb{Z} : q \nmid t\}$;

- $\mathcal{T}_1(\delta) = [1, \delta_{h+1} - 1]$;

- $\mu(\delta) = \min\left\{\delta_{h+1}q, \sum_{\ell=0}^{h-1} \delta_\ell q^\ell\right\}$.

Noting that $\mu(\delta) = \sum_{\ell=0}^{h-1} \delta_\ell q^\ell = \delta_1 q + \delta_0$ if $\delta_{h+1}q > \sum_{\ell=0}^{h-1} \delta_\ell q^\ell$, we can substitute these terms into equation (4.6) to derive

$$f(\delta) = \begin{cases} (q-1)\delta_{h+1}^2, & \text{if } \delta_h = 0 \text{ and } \delta_{h+1}q \le \sum_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ (q-1)(\delta_{h+1}^2 - \delta_{h+1} + \delta_1) + \delta_0, & \text{if } \delta_h = 0 \text{ and } \delta_{h+1}q > \sum_{\ell=0}^{h-1} \delta_\ell q^\ell. \end{cases}$$

Finally, substituting the value of $f(\delta)$ into equation (4.9) for each corresponding case yields the result. $\square$

Based on the proof of Theorem 4.1, we can easily generalize the results in Theorem 4.1 to some primitive BCH codes that are not necessarily narrow-sense as follows.

Theorem 4.2. *Let $m \ge 4$ be an integer, and let b and δ be two positive integers such that $b \ge 2$ and $b(q-1) + 1 \le \delta \le q^{\lfloor (2m-1)/3 \rfloor + 1} + 1 - b$.*

- *If m is odd, then*

$$\dim(\mathcal{C}_{(q,n,\delta,b)}) = n - m\left[N(b+\delta-1) - f(b+\delta-1)\right].$$

- *If m is even, then*

$$\dim(\mathcal{C}_{(q,n,\delta,b)}) = n - m\left[N(b+\delta-1) - \widetilde{f}(b+\delta-1)\right] - \frac{m}{2} g(b+\delta-1).$$

Proof. Since $\delta \ge b(q-1)+1$, for each integer $x \in [1, b-1]$, there exists i such that $b \le xq^i \le bq - 1 \le b + \delta - 2$. Therefore,

$$C_x \subseteq \bigcup_{a=b}^{b+\delta-2} C_a \quad \text{for all } x \in [1, b-1].$$

It follows that

$$\bigcup_{a=1}^{b+\delta-2} C_a = \bigcup_{a=b}^{b+\delta-2} C_a,$$

which is equivalent to $\mathcal{C}_{(q,n,\delta,b)} = \mathcal{C}_{(q,n,b+\delta-1)}$. Noticing that $b+\delta-1 \leq q^{\lfloor (2m-1)/3 \rfloor+1}$, we can apply Theorem 3 to obtain the result. □

4.4 Bose distance of primitive BCH codes

When $\delta = q^{\lfloor (2m-1)/3 \rfloor+1}$, the Bose distance of $C_{(q,n,\delta)}$ was given by [18, Theorem 13]. In this section, we determine the dimension of $C_{(q,n,\delta)}$ for $\delta \in [2, q^{\lfloor (2m-1)/3 \rfloor+1})$.

We can first apply Lemma 3.3 to determine the Bose distance of $\mathcal{C}_{(q,n,\delta)}$ for $\delta \in [2, q^{m-h})$ as follows.

Theorem 4.3. *Let $\delta \in [2, q^{m-h})$ be an integer. Then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } q \nmid \delta, \\ \delta+1, & \text{if } q \mid \delta. \end{cases}$$

Proof. Note that $m-h=h$ when m is odd, and $m-h=h+1$ when m is even. We can apply Lemma 3.3 to conclude that δ is the smallest coset leader in $[\delta, n]$ if $q \nmid \delta$, and $\delta+1$ is the smallest coset leader in $[\delta, n]$ if $q \mid \delta$. Then the result follows. □

Next, we determine the the Bose distance of $\mathcal{C}_{(q,n,\delta)}$ for $\delta \in [q^{m-h}, q^{\lfloor (2m-1)/3 \rfloor+1})$ and $m \geq 4$ by giving the following Theorem 4.4 and Theorem 4.5.

Theorem 4.4. *Suppose that $m \geq 5$ is an odd integer and $\delta \in \left[q^{h+1}, q^{\lfloor (2m-1)/3 \rfloor+1}\right)$ is an integer. Let j_δ be the integer such that $q^{h+j_\delta} \leq \delta < q^{h+j_\delta+1}$. Let $\sum_{\ell=0}^{h+j_\delta} \delta_\ell q^\ell$ denote the q-adic expansion of δ, and let r_δ be the smallest integer in $[-j_\delta+1, j_\delta]$ such that $\delta_{h+r_\delta} > 0$. Define $\hat{\delta} = \sum_{\ell=h+r_\delta}^{h+j_\delta} \delta_\ell q^\ell + \sum_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}$.*

- *If $q \nmid \delta$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell > \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}, \\ \hat{\delta}+1, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell \leq \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)} \\ & \text{and } \delta_{h-r_\delta+1} \neq q-1, \\ \hat{\delta}+2, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell \leq \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)} \\ & \text{and } \delta_{h-r_\delta+1} = q-1. \end{cases} \tag{4.44}$$

- *If $q \mid \delta$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta+1, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell \geq \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}, \\ \hat{\delta}+1, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell < \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)} \\ & \text{and } \delta_{h-r_\delta+1} \neq q-1, \\ \hat{\delta}+2, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell < \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)} \\ & \text{and } \delta_{h-r_\delta+1} = q-1. \end{cases} \tag{4.45}$$

Proof. We will show that equation (4.44) holds if $q \nmid \delta$ through the following cases.

Case 1. Suppose that $\sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell > \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}$. By Remark 3.4, we first have $\delta \notin \mathcal{A}_{j_\delta}(r_\delta)$. Furthermore, recalling the definition of r_δ and applying Remark 3.5, we can also conclude that $\delta \notin \mathcal{A}_{j_\delta}(i)$ for any $i \neq r_\delta$. By applying Theorem 3.2, it follows that $\delta \notin \mathcal{S}$, which implies that δ is a coset leader. It follows that $d_B(\mathcal{C}_{(q,n,\delta)}) = \delta$.

Case 2. Suppose that $\sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell \leq \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}$. We first aim to show that any integer $\delta' \in \left[\delta, \hat{\delta}\right]$ is not a coset leader. Noticing $\sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)} < q^{j_\delta+r_\delta}$, we have $\sum_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell < q^{j_\delta+r_\delta}$. This implies that

$$\delta_\ell = 0 \quad \text{for } \ell = j_\delta + r_\delta, \ldots, h - j_\delta.$$

Recalling the definition of r_δ, it follows that

$$V(\delta) = (\mathbf{0}_{h-j_\delta}, \delta_{h+j_\delta}, \ldots, \delta_{h+r_\delta}, \mathbf{0}_{h-j_\delta}, \delta_{j_\delta+r_\delta-1}, \ldots, \delta_0).$$

It is clear that

$$V(\hat{\delta}) = (\mathbf{0}_{h-j_\delta}, \delta_{h+j_\delta}, \ldots, \delta_{h+r_\delta}, \mathbf{0}_{h-j_\delta}, \delta_{h+j_\delta}, \ldots, \delta_{h-r_\delta+1}).$$

Consequently, for any integer $\delta' \in \left[\delta, \hat{\delta}\right]$ with q-adic expansion $\sum_{\ell=0}^{h+j_\delta} \delta'_\ell q^\ell$, we have

$$\begin{aligned} V(\delta') &= (\mathbf{0}_{h-j_\delta}, \delta'_{h+j_\delta}, \ldots . \delta'_0) \\ &= (\mathbf{0}_{h-j_\delta}, \delta_{h+j_\delta}, \ldots, \delta_{h+r_\delta}, \mathbf{0}_{h-j_\delta}, \delta'_{j_\delta+r_\delta-1}, \ldots . \delta'_0) \end{aligned} \tag{4.46}$$

and

$$\begin{aligned} (\delta'_{j_\delta+r_\delta-1}, \ldots, \delta'_0) &\leq (\delta_{h+j_\delta}, \ldots, \delta_{h-r_\delta+1}) \\ &= (\delta'_{h+j_\delta}, \ldots, \delta'_{h-r_\delta+1}). \end{aligned} \tag{4.47}$$

If $\delta'_0 = 0$, then $q \mid \delta'$, indicating that δ' is not a coset leader. If $\delta'_0 \neq 0$, then we can conclude from (4.46) and (4.47) that $\delta' \in \mathcal{A}_{j_\delta}(r_\delta)$. Thus, by applying Theorem 3.2, we can still can conclude that δ' is not a coset leader.

In addition, we can use a similar argument in Case 1 to conclude that

- If $\delta_{h-r_\delta+1} \neq q-1$, then $\hat{\delta}+1$ is a coset leader.
- If $\delta_{h-r_\delta+1} = q-1$, then $\hat{\delta}+2$ is a coset leader.

Furthermore, since $q \mid \hat{\delta}+1$ when $\delta_{h-r_\delta+1} = q-1$, we can also conclude that $\hat{\delta}+1$ is not a coset leader in this case. Consequently, we conclude that $d_B(\mathcal{C}_{(q,n,\delta)}) = \hat{\delta}+1$ if

$\delta_{h-r_\delta+1} \neq q-1$, and $d_B(\mathcal{C}_{(q,n,\delta)}) = \hat{\delta}+2$ if $\delta_{h-r_\delta+1} = q-1$. We now have demonstrated that equation (4.44) holds if $q \nmid \delta$.

If $q \mid \delta$, then δ is not a coset leader. It follows that $d_B(\mathcal{C}_{(q,n,\delta)}) = d_B(\mathcal{C}_{(q,m,\delta+1)})$. Notably $q \mid \delta$ implies that $q \nmid \delta + 1$. Therefore, we can obtain (4.45) by substituting $\delta + 1$ into equation (4.44). $\square$

Theorem 4.5. *Suppose that $m \geq 4$ is an even integer, and $\delta \in [q^h, q^{\lfloor (2m-1)/3 \rfloor + 1})$ is an integer. Let j_δ be the integer such that $q^{h+j_\delta} \leq \delta < q^{h+j_\delta+1}$. Let $\sum_{\ell=0}^{h+j_\delta} \delta_\ell q^\ell$ denote the q-adic expansion of δ, and let r_δ be the smallest integer in $[-j_\delta, j_\delta]$ such that $\delta_{h+r_\delta} > 0$. Define $\hat{\delta} = \sum_{\ell=h+r_\delta}^{h+j_\delta} \delta_\ell q^\ell + \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)}$.*

- *If $r_\delta \neq 0$ and $q \nmid \delta$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell > \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)}, \\ \hat{\delta}+1, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell \leq \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)} \\ & \text{and } \delta_{h-r_\delta} \neq q-1, \\ \hat{\delta}+2, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell \leq \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)} \\ & \text{and } \delta_{h-r_\delta} = q-1. \end{cases} \tag{4.48}$$

- *If $r_\delta \neq 0$ and $q \mid \delta$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta+1, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell \geq \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)}, \\ \hat{\delta}+1, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell < \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)} \\ & \text{and } \delta_{h-r_\delta} \neq q-1, \\ \hat{\delta}+2, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell < \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)} \\ & \text{and } \delta_{h-r_\delta} = q-1. \end{cases} \tag{4.49}$$

- *If $r_\delta = 0$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell > \sum\limits_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h} \text{ and } q \nmid \delta, \\ \delta+1, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell > \sum\limits_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h} \text{ and } q \mid \delta, \\ \hat{\delta}, & \text{if } \sum\limits_{\ell=0}^{h-j_\delta-1} \delta_\ell q^{\ell-h} \leq \sum\limits_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}. \end{cases} \tag{4.50}$$

Proof. First, by an argument similar to that in the proof of Theorem 4.4, we conclude that (4.48) holds if $r_\delta \neq 0$ and $q \nmid \delta$, and that (4.49) holds if $r_\delta \neq 0$ and $q \mid \delta$. Next, we will show that (4.50) holds if $r_\delta = 0$ by considering the following cases.

Case 1. Suppose that $\sum\limits_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell > \sum\limits_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}$ and $q \nmid \delta$. Then by applying Remarks 3.4 and 3.5, we see that $\delta \notin \mathcal{B}_{j_\delta}(i)$ for any $i \in [-j_\delta, j_\delta]$. Hence $a \notin \mathcal{S} \cup \mathcal{H}$. Therefore, we can conclude δ is a coset leader. Consequently, we have $d_B(\mathcal{C}_{(q,n,\delta)}) = \delta$ in this case.

Case 2. Suppose that $\sum\limits_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell > \sum\limits_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}$ and $q \mid \delta$. Then the assumption that $q \mid \delta$ implies that δ is not a coset leader. Furthermore, by an argument similar to that in Case 1, we conclude that $\delta+1$ is a coset leader. Therefore, $d_B(\mathcal{C}_{(q,n,\delta)}) = \delta+1$.

Case 3. Suppose that $\sum\limits_{\ell=0}^{h-j_\delta-1} \delta_\ell q^{\ell-h} \leq \sum\limits_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}$. Then we distinguish the following two subcases:

Subcase 1. If $\sum\limits_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell = \sum\limits_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}$, then we have

$$\delta_\ell = 0 \quad \text{for } \ell = j_\delta+1, \ldots, h-j_\delta-1$$

and

$$\delta_\ell = \delta_{\ell+h} \quad \text{for } \ell = 0, \ldots, j_\delta.$$

It follows that $\hat{\delta} = \delta$, and $V(\delta)$ has the form

$$(\mathbf{0}_{h-j_\delta-1}, \delta_{j_\delta}, \ldots, \delta_0, \mathbf{0}_{h-j_\delta-1}, \delta_{j_\delta}, \ldots, \delta_0)$$

with $\delta_0 > 0$ and $\delta_{j_\delta} > 0$. By applying Corollary 3.3, we can conclude that $\delta \in \mathcal{H}$, which implies that δ is a coset leader. Therefore, we have $d_B(\delta) = \delta = \hat{\delta}$.

Subcase 2. If $\sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^{\ell-h} < \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}$. By an argument similar to that in Case 1 of the proof of Theorem 4.4, we first conclude that any integer $\delta' \in \left[\delta, \hat{\delta}\right)$ is not a coset leader. Note that $\delta_h > 0$ and $\hat{\delta} = \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^\ell + \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}$ when $r_\delta = 0$. Applying Corollary 3.3, one can easily verify that $\hat{\delta} \in \mathcal{H}$. This implies that $\hat{\delta}$ is a coset leader. Consequently, we have $d_B(\mathcal{C}_{(q,n,\delta)}) = \hat{\delta}$. □

An $[n, k, d]$ code over $\mathbb{F}_q$ is called *optimal* if there is no $[n, k', d]$ linear code with $k' > k$, or $[n, k, d']$ linear code with $d' > d$ over $\mathbb{F}_q$. We provide examples of narrow-sense BCH codes discussed in this chapter in Tables 4.2 and 4.3. The dimensions k and Bose distances d_B of the BCH codes presented in these tables are calculated using the formulas from Theorems 4.1, 4.3, 4.4, and 4.5, with all parameters verified using Magma. We compare these codes with the Database and find that they are either optimal or match the parameters of the best-known linear codes. We also utilized Magma to calculate the minimum distance of the codes. For codes whose minimum distance could not be determined by Magma within a reasonable time, we denote this with "–". Notably, the Bose distance and minimum distance of these codes are equal.

Table 4.2: Examples of binary narrow-sense primitive BCH codes

q	m	δ	n	k	d_B	d	Optimality
2	4	2 – 3	15	11	3	3	Optimal
2	4	4 – 5	15	7	5	5	Optimal
2	4	6 –7	15	5	7	7	Optimal
2	5	2 – 3	31	26	3	3	Optimal
2	5	4 – 5	31	21	5	5	Optimal
2	5	6 –7	31	16	7	7	Optimal
2	5	8 – 11	31	11	11	11	Optimal
2	5	12 – 15	31	6	15	15	Optimal
2	6	2 – 3	63	57	3	3	Optimal
2	6	4 – 5	63	51	5	5	Optimal
2	6	8 – 9	63	39	9	9	Best Known
2	6	10 – 11	63	36	11	11	Best Known
2	6	12 – 13	63	30	13	13	Best Known
2	7	2 – 3	127	120	3	3	Optimal
2	7	4 – 5	127	113	5	5	Optimal
2	7	6 – 7	127	106	7	7	Best Known
2	7	8 – 9	127	99	9	9	Best Known
2	7	10 – 11	127	92	11	11	Best Known
2	7	12 – 13	127	85	13	13	Best Known
2	7	14 – 15	127	78	15	15	Best Known
2	7	16 – 19	127	71	19	19	Best Known
2	7	20 – 21	127	64	21	21	Best Known
2	7	24 – 27	127	50	27	27	Best Known
2	8	2 – 3	254	247	3	3	Optimal
2	8	5	254	239	5	5	Optimal
2	8	6 – 7	254	231	7	7	Best Known
2	8	8 – 9	254	223	9	9	Best Known
2	8	10 – 11	254	215	11	11	Best Known
2	8	12 – 13	254	207	13	13	Best Known
2	8	14 – 15	254	199	15	15	Best Known
2	8	16 – 17	254	191	17	17	Best Known
2	8	18 – 19	254	187	19	19	Best Known
2	8	20 – 21	254	179	21	21	Best Known
2	8	22 – 23	254	171	23	23	Best Known
2	8	24 – 25	254	163	25	25	Best Known
2	8	26 – 27	254	155	27	27	Best Known
2	8	28 – 29	254	147	29	29	Best Known
2	8	30 – 31	254	139	31	31	Best Known
2	8	32 – 37	254	131	37	37	Best Known
2	8	38 – 39	254	123	39	39	Best Known
2	8	40 – 43	254	115	43	43	Best Known
2	8	44 – 45	254	107	45	45	Best Known
2	8	46 – 47	254	99	47	47	Best Known
2	8	48 – 51	254	91	51	51	Best Known
2	8	52 – 53	254	87	53	53	Best Known

Table 4.3: Examples of nonbinary narrow-sense primitive BCH codes

q	m	δ	n	k	d_B	d	Optimality
3	4	2	80	76	2	2	Optimal
3	4	3 – 4	80	72	4	4	Best Known
3	4	8	80	60	8	8	Best Known
3	4	9 – 10	80	56	10	10	Best Known
3	4	11	80	54	11	11	Best Known
3	4	12 – 13	80	50	13	13	Best Known
3	4	14	80	46	14	14	Best Known
3	5	2	242	237	2	2	Optimal
3	5	3 – 4	242	232	4	4	Optimal
3	5	5	242	227	5	5	Best Known
3	5	6 – 7	242	222	7	7	Best Known
3	5	8	242	217	8	8	Best Known
3	5	9 – 10	242	212	10	10	Best Known
3	5	11	242	207	11	11	Best Known
3	5	12 – 13	242	202	13	13	Best Known
3	5	14	242	197	14	14	Best Known
3	5	15 – 16	242	192	16	16	Best Known
3	5	17	242	187	17	17	Best Known
3	5	18 – 19	242	182	19	–	Best Known
3	5	20	242	177	20	–	Best Known
3	5	21 – 22	242	172	22	–	Best Known
3	5	23	242	167	23	–	Best Known
3	5	24 – 25	242	162	25	–	Best Known
3	5	26	242	157	26	–	Best Known
3	5	27 – 31	242	152	31	–	Best Known
3	5	32	242	147	32	–	Best Known
3	5	33 – 34	242	142	34	–	Best Known
3	5	35	242	137	35	–	Best Known
3	5	36 – 38	242	132	38	–	Best Known
3	5	39 – 40	242	127	40	–	Best Known
3	5	41	242	122	41	–	Best Known
3	5	42 – 43	242	117	43	–	Best Known
4	4	2	255	251	2	2	Best Known
4	4	4 – 5	255	243	5	5	Best Known
4	4	6	255	239	6	6	Best Known
4	4	8 – 9	255	231	9	9	Best Known
4	4	10	255	227	10	10	Best Known
4	4	11	255	223	11	11	Best Known
4	4	12 – 13	255	219	13	13	Best Known
4	4	14	255	215	14	14	Best Known
4	4	15	255	211	15	15	Best Known
4	4	16 – 17	255	207	17	17	Best Known
4	4	18	255	205	18	–	Best Known
4	4	19	255	201	19	–	Best Known
4	4	20 – 21	255	197	21	–	Best Known
4	4	22	255	193	22	–	Best Known
4	4	23	255	189	23	–	Best Known
4	4	24 – 25	255	185	25	–	Best Known
4	4	25	255	185	25	–	Best Known
4	4	26	255	181	26	–	Best Known
4	4	27	255	177	27	–	Best Known
4	4	28 – 29	255	173	29	–	Best Known
4	4	30	255	169	30	–	Best Known
4	4	32 – 34	255	161	34	–	Best Known
4	4	35	255	159	35	–	Best Known
4	4	36 – 37	255	155	37	–	Best Known

4.5 Narrow-sense primitive BCH codes with designed distance $\delta = aq^{h+k} + b$

As a special case of our main results on primitive BCH codes in the above sections, in the following corollaries, we give the dimension and Bose distance of $\mathcal{C}_{(q,n,\delta)}$ for $m \geq 4$ and $\delta = aq^{h+k} + b$, where k, a and b are integer satisfying $m - 2h \leq k \leq \lfloor (2m-1)/3 \rfloor - h$, $1 \leq a \leq q-1$ and $1 \leq b \leq q^{m-h-k}$.

Corollary 4.3. *Let $m \geq 5$ be an odd integer and $k \in [1, \lfloor (2m-1)/3 \rfloor - h]$ be an integer. If $\delta = aq^{h+k} + b$ for some integers $a \in [1, q-1]$ and $b \in [1, q^{h-k+1}]$ with $q \nmid b$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } b > aq^{2k-1}, \\ aq^{h+k} + aq^{2k-1} + 1, & \text{if } b \leq aq^{2k-1}, \end{cases} \tag{4.51}$$

and

$$\dim(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \begin{pmatrix} n - mN(\delta) \\ \quad + ma^2(q-1)q^{2k-3}\left[(q-1)k+1\right] \end{pmatrix}, & \text{if } b > aq^{2k-1}, \\ \begin{pmatrix} n - maq^{h+k-1}(q-1) \\ \quad - ma(q-1)q^{2k-2} \\ \quad + ma^2(q-1)q^{2k-3}\left[(q-1)k+1\right] \end{pmatrix}, & \text{if } b \leq aq^{2k-1}. \end{cases} \tag{4.52}$$

Proof. By applying Theorem 4.4, we can directly derive equation (4.51). Therefore, we only demonstrate that (4.52) holds. It is clear that $V(\delta-1)$ has the form

$$(\mathbf{0}_{h-k}, a, \mathbf{0}_{2k-1}, \delta_{h-k}, \ldots, \delta_0)$$

with $\sum_{\ell=0}^{h-k} \delta_\ell q^\ell = b - 1$. By definition, it follows that

- $s_\delta = k_\delta = k$;
- $\mu(\delta) = \min\left\{b-1, aq^{2k-1}\right\}$;
- $\mathcal{T}_i(\delta) = \left[q^{k-i}, aq^{k-i} - 1\right] \cap \{t \in \mathbb{Z} : q \nmid t\}$ for each integer $i \in [-k+1, k]$.

Then applying Lemma 4.3, we can obtain

$$\sum_{t\in\mathcal{T}_i(\delta)} N(tq^{2i-1}+1) = \begin{cases} \frac{1}{2}(a^2-1)(q-1)^2q^{2k-3}, & \text{if } i\in[-k+2,k-1], \\ \frac{1}{2}a(a-1)(q-1)q^{2k-2}, & \text{if } i=k \text{ or } -k+1. \end{cases}$$

It follows that

$$\begin{aligned} \sum_{i=-k_\delta+1}^{k_\delta}\sum_{t\in\mathcal{T}_i(\delta)} N(tq^{2i-1}+1) = & \sum_{i=-k+1}^{k}\sum_{t\in\mathcal{T}_i(\delta)} N(tq^{2i-1}+1) \\ = & a(a-1)(q-1)q^{2k-2}+(a^2-1)(k-1)(q-1)^2q^{2k-3}. \end{aligned}$$

By substituting the values of k_δ, $\mu(\delta)$ and the above expression into (4.6), we obtain

$$f(\delta) = \begin{cases} a^2(q-1)q^{2k-3}\left[k(q-1)+1\right], & \text{if } b>aq^{2k-1}, \\ a(q-1)q^{2k-3}\left[ak(q-1)+a-q\right]+N(b), & \text{if } b\le aq^{2k-1}. \end{cases}$$

Finally, noticing that $N(\delta)-N(b)=aq^{h+k-1}(q-1)$, we can apply Theorem 4.1 to derive the result. $\square$

Corollary 4.4. *Let $m\ge 4$ be an even intger and $0\le k\le\lfloor(2m-1)/3\rfloor-h$ be an integer. If $\delta=aq^{h+k}+b$ for some integers $a\in[1,q-1]$ and $b\in[1,q^{h-k}]$ with $q\nmid b$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} aq^h+a, & \textit{if } k=0, b\le a, \\ \delta, & \textit{if } k=0, b>a, \\ \delta, & \textit{if } k\ge 1, b>aq^{2k}, \\ aq^{h+k}+aq^{2k}+1, & \textit{if } k\ge 1, b\le aq^{2k}. \end{cases} \tag{4.53}$$

and

$$\dim(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} n-maq^{h-1}(q-1)+\frac{1}{2}m(a-1)^2, & \textit{if } k=0, b\le a, \\ n-mN(\delta)+\frac{1}{2}ma^2, & \textit{if } k=0, b>a, \\ \begin{pmatrix} ma^2(q-1)^2q^{2k-2}\left(k-\frac{1}{2}\right) \\ +ma^2(q-1)q^{2k-1} \\ +n-mN(\delta) \end{pmatrix}, & \textit{if } k\ge 1, b>aq^{2k} \\ \begin{pmatrix} ma^2(q-1)^2q^{2k-2}\left(k-\frac{1}{2}\right) \\ +ma(a-1)(q-1)q^{2k-1} \\ +n-maq^{h+k-1}(q-1) \end{pmatrix}, & \textit{if } k\ge 1, b\le aq^{2k}. \end{cases} \tag{4.54}$$

Proof. By applying Theorem 4.5, it is easy to derive equation (4.53). Therefore, we only need to demonstrate that (4.54) holds. If $k = 0$, then we have $\delta - 1 = aq^h + b - 1$ with $0 \leq b - 1 < q^{h-1}$. It follows that $q^h < \delta \leq q^{h+1}$ and $\delta_h = a$. Consequently, we have $s_\delta = k_\delta = 0$, which implies

- $\widetilde{\mu}(\delta) = \min\{b-1, a\}$;
- $\tau(\delta) = 1$ if $a \leq b-1$, and $\tau(\delta) = 0$ if otherwise.

Thus, by substituting $\delta_h = a$, and the values of $\tau(\delta)$ and $\widetilde{\mu}(\delta)$ for the corresponding case into equations (4.7) and (4.8), we derive

$$\widetilde{f}(\delta) = \begin{cases} \frac{1}{2}a(a-1) + N(b), & \text{if } k = 0 \text{ and } b \leq a, \\ \frac{1}{2}a(a-1) + N(a+1), & \text{if } k = 0 \text{ and } b > a, \end{cases}$$

and

$$g(\delta) = \begin{cases} a-1, & \text{if } k = 0 \text{ and } b \leq a, \\ a, & \text{if } k = 0 \text{ and } b > a. \end{cases}$$

If $k \geq 1$, then we have $k_\delta = k$ and $V(\delta - 1)$ has the form

$$(\mathbf{0}_{h-k-1}, a, \mathbf{0}_{2k}, \delta_{h-k-1}, \ldots, \delta_0)$$

with $\sum_{\ell=0}^{h-k} \delta_\ell q^\ell = b - 1$. By definition, it follows that

- $s_\delta = k_\delta = k$;
- $\tau(\delta) = 0$;
- $\widetilde{\mu}(\delta) = \min\left\{b-1, aq^{2k}\right\}$;
- $\mathcal{T}_i(\delta) = \left[q^{k-i}, aq^{k-i} - 1\right] \cap \{t \in \mathbb{Z} : q \nmid t\}$ for each integer $i \in [-k, k]$.

Applying Lemma 4.3, we obtain

$$\sum_{t\in\mathcal{T}_i(\delta)} N(tq^{2i}+1) = \begin{cases} \frac{1}{2}(a^2-1)(q-1)^2q^{2k-2}, & \text{if } i \in [-k+1,,k-1]\setminus\{0\}, \\ \frac{1}{2}a(a-1)(q-1)q^{2k-1}, & \text{if } i = k \text{ or } -k, \\ \begin{pmatrix} \frac{1}{2}(a^2-1)(q-1)^2q^{2k-2} \\ +\frac{1}{2}(a-1)(q-1)q^{k-1} \end{pmatrix}, & \text{if } i = 0. \end{cases}$$

It follows that

$$\sum_{i=-k_\delta}^{k_\delta}\sum_{t\in\mathcal{T}_i(\delta)} N(tq^{2i}+1) = \sum_{i=-k}^{k}\sum_{t\in\mathcal{T}_i(\delta)} N(tq^{2i}+1)$$

$$=(a^2-1)(q-1)^2(k-\frac{1}{2})q^{2k-2} + a(a-1)(q-1)q^{2k-1} + \frac{1}{2}(a-1)q^{k-1}(q-1).$$

By substituting the values of k_δ, $\widetilde{\mu}(\delta)$ and the above expression into (4.7) and (4.8), we obtain

$$\widetilde{f}(\delta) = \begin{cases} \begin{pmatrix} a^2(q-1)^2q^{2k-2}\left(k-\frac{1}{2}\right) \\ +a^2(q-1)q^{2k-1} \\ +\frac{1}{2}aq^{k-1}(q-1) \end{pmatrix}, & \text{if } k\geq 1, b > aq^{2k}, \\ \begin{pmatrix} a^2(q-1)^2q^{2k-2}(k-\frac{1}{2}) \\ +a(a-1)(q-1)q^{2k-1} \\ +\frac{1}{2}aq^{k-1}(q-1)+N(b) \end{pmatrix}, & \text{if } k\geq 1, b\leq aq^{2k}, \end{cases}$$

and

$$g(\delta) = aq^{k-1}(q-1) \quad \text{for } k\geq 1.$$

Finally, by applying Theorem 4.1, we obtain the result. □

Chapter 5

Dimension and Bose distance of BCH codes of length $\frac{q^m-1}{\lambda}$

5.1 Introduction

In this chapter, we study the dimension and Bose distance of some BCH codes of length $(q^m-1)/\lambda$, where λ is a positive divisor of $q-1$. This class notably includes primitive BCH codes when $\lambda = 1$. Throughout this chapter, let m be a positive integer, λ be a positive divisor of $q-1$, $h = \lfloor m/2 \rfloor$, and $n = (q^m-1)/\lambda$. The notation $\mathcal{C}_{(q,n,\delta,b)}$ always denotes a BCH code of length $(q^m-1)/\lambda$, while $\mathcal{C}_{(q,n,\delta)}$ denotes the corresponding narrow-sense BCH code. For any real number a, we define $N(a)$ as the number of integers in the interval $[1, a-1]$ that are not divisible by q, i.e., $N(a) = \lfloor a-1 \rfloor - \lfloor (a-1)/q \rfloor$.

While our understanding of primitive BCH codes is already limited, as discussed in previous chapters, the BCH codes of length $(q^m-1)/\lambda$ with $\lambda \neq 1$ are understood to an even lesser extent. Even for specific cases, such as $\lambda = 2$ [38, 53] and $\lambda = q-1$ [34, 39], the dimension and Bose distance are known only for a restricted range of designed distances. For positive general divisors λ of $q-1$, Zhu et al. [60] determined the dimension of narrow-sense BCH codes $\mathcal{C}_{(q,n,\delta)}$ for designed distances $2 \leq \delta \leq \frac{q^{\lceil (m+1)/2 \rceil}-1}{\lambda} + 1$. More recently, Sun [51] provided results on the dimension and minimum distance of $\mathcal{C}_{(q,n,\delta)}$ for other specific designed distances.

As established in Section 2.6 of Chapter 2, a thorough understanding of q-cyclotomic cosets, particularly their sizes and coset leaders, is fundamental for characterizing the dimension and Bose distance of BCH codes. Building upon our prior analysis of q-cyclotomic cosets modulo q^m-1, presented in Chapter 3, we previously determined the Bose distance and dimension of some primitive BCH codes in Chapter 4.

To extend this analysis to BCH codes of length $(q^m-1)/\lambda$, we need investigate q-cyclotomic cosets modulo $(q^m-1)/\lambda$. A key insight, provided by Lemma 3.2 and its corollary, establishes a direct correspondence: an integer a is a coset leader modulo $(q^m-1)/\lambda$ if and only if λa is a coset leader modulo q^m-1. Furthermore, the size of the q-cyclotomic coset of a modulo $(q^m-1)/\lambda$ equals the size of the q-cyclotomic coset of λa modulo q^m-1. This reduces the determination of coset leaders and sizes of q-cyclotomic cosets modulo $(q^m-1)/\lambda$ to identifying integers that are both divisible by λ and coset leaders modulo q^m-1, as well as computing the sizes of their corresponding cosets.

Leveraging this observation and our prior analysis of q-cyclotomic cosets modulo q^m-1, we determine, for any positive divisor λ of $q-1$ and any integer $m\geq 4$:

- the dimension of $\mathcal{C}_{(q,n,\delta)}$ for $2\leq\delta\leq\frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}+1$;
- the Bose distance of $\mathcal{C}_{(q,n,\delta)}$ for $2\leq\delta\leq\frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}$.

This significantly extends the current state of knowledge for such codes. Existing results for the dimension of narrow-sense BCH codes of length $(q^m-1)/\lambda$ are limited to designed distances $2\leq\delta\leq\frac{q^{\lceil(m+1)/2\rceil}-1}{\lambda}+1$ and a few specific cases. Our work substantially broadens this range, as evidenced by the inequality:

$$\frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}\geq\frac{q^{\lceil(m+1)/2\rceil}-1}{\lambda}\cdot q^{\lceil(m-4)/6\rceil}.$$

Additionally, we extend these results to some non-narrow-sense BCH codes of length $\frac{q^m-1}{\lambda}$.

This chapter is organized as follows. In Section 5.2, we present several auxiliary lemmas that will be employed in subsequent sections. Based on these theoretical foundations, we then determine the dimension of BCH codes $\mathcal{C}_{(q,n,\delta)}$ for $2 \leq \delta \leq \frac{q^{\lfloor (2m-1)/3 \rfloor+1}-1}{\lambda} + 1$ in Section 5.3 and the Bose distance of $\mathcal{C}_{(q,n,\delta)}$ for $2 \leq \delta \leq \frac{q^{\lfloor (2m-1)/3 \rfloor+1}-1}{\lambda}$ in Section 5.4, both by providing explicit formulas. Furthermore, in Section 5.5, as an illustration of our main results, we provide explicit formulas for determining the dimension and Bose distance of $\mathcal{C}_{(q,n,\delta)}$ when $\lambda\delta = aq^{h+k} + b$, where k, a, b are integers satisfying $m - 2h \leq k \leq \lfloor (2m-1)/3 \rfloor - h$, $1 \leq a \leq q-1$, $\lambda \leq b \leq q^{m-h-k}$, and $q \nmid b$. Following this, Section 5.6 extends our analysis to determine the dimension and Bose distance of certain non-narrow-sense BCH codes.

5.2 Auxiliary Lemmas

The reader may recall from Chapter 4 that determining the dimension of primitive BCH codes involves extensive calculations. These computations primarily consist of counting integers in specific intervals that are not divisible by q and evaluating related summations. The task of determining the dimension of BCH codes of length $n = (q^m - 1)/\lambda$ is considerably more intricate. This is because it requires counting integers within specific intervals that are divisible by λ, and more challengingly, those that are simultaneously divisible by λ but not by q, as well as handling a series of complex summations involving these counts.

In this section, we provide a series of lemmas designed to tackle these specific counting and summation problems. These lemmas are utilized in obtain our formulas for the dimension of BCH codes of length $(q^m - 1)/\lambda$ in subsequent sections.

The first two lemmas, Lemma 5.1 and Lemma 5.2, , both concern counting integers that are divisible by λ but not by q.

Lemma 5.1. *Suppose that x and y are two positive integers. Then*

$$|\{\alpha \in [1,x] : q \nmid \alpha \text{ and } \lambda \mid \alpha + y\}| = \left\lfloor \frac{x+y}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor x/q \rfloor + y}{\lambda} \right\rfloor .$$

Proof. It is clear that

$$\begin{aligned} &\{a \in [1,x] : q \nmid a \text{ and } \lambda \mid a+y\} \\ =&\{a \in [1,x] : \lambda \mid a+y\} - \{a \in [1,x] : q \mid a \text{ and } \lambda \mid a+y\}. \end{aligned} \tag{5.1}$$

Next, we show that

$$|\{a \in [1,x] : q \mid a \text{ and } \lambda \mid a+y\}| = |\{a \in [1, \lfloor x/q \rfloor] : \lambda \mid a+y\}| . \tag{5.2}$$

Notice that there exists a bijective $a \mapsto a/q$ between the integers in $[1,x]$ that are divisible by q and the integers in $[1, \lfloor x/q \rfloor]$. Furthermore, for any integer a such that $q \mid a$, we have

$$a + y = \frac{a}{q}(q-1) + \frac{a}{q} + y.$$

Since $\lambda \mid q-1$, it follows that $\lambda \mid a+y$ if and only if $\lambda \mid \frac{a}{q} + y$ for any integer a such that $q \mid a$. Therefore, we can conclude that there exists a one-to-one correspondence between the two sets in (5.2) by mapping a to a/q, and hence the equality in (5.2) holds. With (5.1), it follows that

$$\begin{aligned} |\{a \in [1,x] : q \nmid a \text{ and } \lambda \mid a+y\}| &= |\{a \in [\lfloor x/q \rfloor + 1, x] : \lambda \mid a+y\}| \\ &= \left\lfloor \frac{x+y}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor x/q \rfloor + y}{\lambda} \right\rfloor . \end{aligned}$$

This completes the proof. $\square$

Lemma 5.2. *Suppose that x and y are two integers such that $x \le y$. Then we have*

$$|\{\alpha \in [x,y] : \lambda \mid 2\alpha \text{ and } q \nmid \alpha\}| = \begin{cases} \left\lfloor \frac{y}{\lambda} \right\rfloor - \left\lfloor \frac{x-1}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor y/q \rfloor}{\lambda} \right\rfloor + \left\lfloor \frac{\lceil x/q \rceil - 1}{\lambda} \right\rfloor, & \text{if } \lambda \text{ is odd,} \\ \left\lfloor \frac{2y}{\lambda} \right\rfloor - \left\lfloor \frac{2x-2}{\lambda} \right\rfloor - \left\lfloor \frac{2\lfloor y/q \rfloor}{\lambda} \right\rfloor + \left\lfloor \frac{2\lceil x/q \rceil - 2}{\lambda} \right\rfloor, & \text{if } \lambda \text{ is even.} \end{cases}$$

Proof. First, we can apply a similar argument as utilized in the proof of Lemma 5.1 to conclude that

$$|\{\alpha \in [x, y] : \lambda \mid 2\alpha \text{ and } q \mid \alpha\}| = \left|\left\{\alpha \in \left[\lceil x/q \rceil, \lfloor y/q \rfloor\right] : \lambda \mid 2\alpha\right\}\right|.$$

It follows that

$$\begin{aligned} &|\{\alpha \in [x, y] : \lambda \mid 2\alpha \text{ and } q \nmid \alpha\}| \\ =&|\{\alpha \in [x, y] : \lambda \mid 2\alpha\}| - \left|\left\{\alpha \in \left[\lceil x/q \rceil, \lfloor y/q \rfloor\right] : \lambda \mid 2\alpha\right\}\right| \end{aligned} \tag{5.3}$$

Then we distinguish the following two cases:

Case 1. Suppose that λ is odd. Then $\lambda \mid 2\alpha$ holds if and only if $\lambda \mid \alpha$. Therefore,

$$|\{\alpha \in [x, y] : \lambda \mid 2\alpha\}| = |\{\alpha \in [x, y] : \lambda \mid \alpha\}| = \left\lfloor \frac{y}{\lambda} \right\rfloor - \left\lfloor \frac{x-1}{\lambda} \right\rfloor.$$

Similarly, we also have

$$|\{\alpha \in [\lceil x/q \rceil, \lfloor y/q \rfloor] : \lambda \mid 2\alpha\}| = \left\lfloor \frac{\lfloor y/q \rfloor}{\lambda} \right\rfloor - \left\lfloor \frac{\lceil x/q \rceil - 1}{\lambda} \right\rfloor.$$

Case 2. Suppose that λ is even. Then $\lambda \mid 2\alpha$ holds if and only if $\frac{\lambda}{2} \mid \alpha$. Consequently,

$$|\{\alpha \in [x, y] : \lambda \mid 2\alpha\}| = \left|\left\{\alpha \in [x, y] : \frac{\lambda}{2} \mid \alpha\right\}\right| = \left\lfloor \frac{2y}{\lambda} \right\rfloor - \left\lfloor \frac{2x-2}{\lambda} \right\rfloor.$$

Similarly, we also have

$$\left|\left\{\alpha \in \left[\lceil x/q \rceil, \lfloor y/q \rfloor\right] : \lambda \mid 2\alpha\right\}\right| = \left\lfloor \frac{2\lfloor y/q \rfloor}{\lambda} \right\rfloor - \left\lfloor \frac{2\lceil x/q \rceil - 2}{\lambda} \right\rfloor.$$

We now can derive the desired equation from equation (5.3) and the discussion for the above two cases. This completes the proof. $\square$

The next two lemmas, Lemma 5.3 and Lemma 5.4, are dedicated to evaluating summations where each term represents a count of integers divisible by λ within a dynamically defined interval. Specifically, Lemma 5.3 sums terms counting integers in $(t+y, t+x]$ divisible by λ, while Lemma 5.4 sums terms counting integers in $(t+x, 2t+x]$ divisible by λ.

Lemma 5.3. *Suppose that x and y are two integers. Then*

$$\sum_{t=1}^{q-1}\left[\left\lfloor\frac{t+x}{\lambda}\right\rfloor-\left\lfloor\frac{t+y}{\lambda}\right\rfloor\right]=\frac{(q-1)(x-y)}{\lambda}.$$

Proof. For simplicity, we set $\beta_1 = x-\lambda\cdot\left\lfloor\frac{x}{\lambda}\right\rfloor$ and $\beta_2 = y-\lambda\cdot\left\lfloor\frac{y}{\lambda}\right\rfloor$. Then

$$\sum_{t=1}^{q-1}\left[\left\lfloor\frac{t+x}{\lambda}\right\rfloor-\left\lfloor\frac{t+y}{\lambda}\right\rfloor\right]=\sum_{t=1}^{q-1}\left[\left\lfloor\frac{x}{\lambda}\right\rfloor-\left\lfloor\frac{y}{\lambda}\right\rfloor+\left\lfloor\frac{t+\beta_1}{\lambda}\right\rfloor-\left\lfloor\frac{t+\beta_2}{\lambda}\right\rfloor\right]. \tag{5.4}$$

It is straightforward to verify that

$$\left\lfloor\frac{t+\beta_1}{\lambda}\right\rfloor=\begin{cases}0, & \text{for } t\in[1,\lambda-\beta_1-1],\\ i, & \text{for } t\in[i\lambda-\beta_1,(i+1)\lambda-1-\beta_1],\\ \frac{q-1}{\lambda}, & \text{for } t\in[q-1-\beta_1,q-1],\end{cases}$$

where i can be any integer in $[1,\frac{q-1}{\lambda}-1]$. Therefore, we can obtain

$$\sum_{t=1}^{q-1}\left\lfloor\frac{t+\beta_1}{\lambda}\right\rfloor=\frac{(q-1)(\beta_1+1)}{\lambda}+\sum_{i=1}^{\frac{q-1}{\lambda}-1} i\lambda.$$

Similarly, we can also derive

$$\sum_{t=1}^{q-1}\left\lfloor\frac{t+\beta_2}{\lambda}\right\rfloor=\frac{(q-1)(\beta_2+1)}{\lambda}+\sum_{i=1}^{\frac{q-1}{\lambda}-1} i\lambda.$$

Combining the above two equalities, we obtain

$$\sum_{t=1}^{q-1}\left[\left\lfloor\frac{t+\beta_1}{\lambda}\right\rfloor-\left\lfloor\frac{t+\beta_2}{\lambda}\right\rfloor\right]=\frac{(q-1)(\beta_1-\beta_2)}{\lambda}.$$

With the equality in (5.4), it follows

$$\sum_{t=1}^{q-1}\left[\left\lfloor\frac{t+x}{\lambda}\right\rfloor-\left\lfloor\frac{t+y}{\lambda}\right\rfloor\right]=\frac{q-1}{\lambda}\left(\lambda\cdot\left\lfloor\frac{x}{\lambda}\right\rfloor+\beta_1\right)-\frac{q-1}{\lambda}\left(\lambda\cdot\left\lfloor\frac{y}{\lambda}\right\rfloor+\beta_2\right)$$
$$=\frac{(q-1)(x-y)}{\lambda}.$$

This completes the proof. □

Lemma 5.4. *Suppose that x is an even integer. Then*

$$\sum_{t=1}^{q-1}\left[\left\lfloor\frac{2t+x}{\lambda}\right\rfloor-\left\lfloor\frac{t+x}{\lambda}\right\rfloor\right]=\begin{cases}\frac{q(q-1)}{2\lambda}, & \text{if } \lambda \text{ is odd},\\ \frac{(q-1)(q+1)}{2\lambda}, & \text{if } \lambda \text{ is even}.\end{cases}$$

Proof. Notice that each integer $t\in[0,q-2]$ admits a uniquely unique decomposition

$$t=i\lambda+j \quad \text{with } i\in\left[0,\frac{q-1}{\lambda}-1\right] \text{ and } j\in[0,\lambda-1].$$

Therefore, we have

$$\sum_{t=1}^{q-1}\left[\left\lfloor\frac{2t+x}{\lambda}\right\rfloor-\left\lfloor\frac{t+x}{\lambda}\right\rfloor\right]$$
$$=\sum_{t=0}^{q-1}\left[\left\lfloor\frac{2t+x}{\lambda}\right\rfloor-\left\lfloor\frac{t+x}{\lambda}\right\rfloor\right]$$
$$=\sum_{i=0}^{\frac{q-1}{\lambda}-1}\sum_{j=0}^{\lambda-1}\left[\left\lfloor\frac{2i\lambda+2j+x}{\lambda}\right\rfloor-\left\lfloor\frac{i\lambda+j+x}{\lambda}\right\rfloor\right]+\left\lfloor\frac{2(q-1)+x}{\lambda}\right\rfloor-\left\lfloor\frac{q-1+x}{\lambda}\right\rfloor$$
$$=\sum_{i=0}^{\frac{q-1}{\lambda}-1}\sum_{j=0}^{\lambda-1}\left[i+\left\lfloor\frac{2j+x}{\lambda}\right\rfloor-\left\lfloor\frac{j+x}{\lambda}\right\rfloor\right]+\frac{q-1}{\lambda}$$
$$=\frac{(q-1)(q+1)}{2\lambda}-\frac{q-1}{2}+\frac{q-1}{\lambda}\sum_{j=0}^{\lambda-1}\left[\left\lfloor\frac{2j+x}{\lambda}\right\rfloor-\left\lfloor\frac{j+x}{\lambda}\right\rfloor\right]. \tag{5.5}$$

Let $y = x - \lambda \cdot \lfloor \frac{x}{\lambda} \rfloor$. Then we have $0 \le y \le \lambda - 1$ and

$$\left\lfloor \frac{2j+x}{\lambda} \right\rfloor - \left\lfloor \frac{j+x}{\lambda} \right\rfloor = \left\lfloor \frac{2j+y}{\lambda} \right\rfloor - \left\lfloor \frac{j+y}{\lambda} \right\rfloor. \tag{5.6}$$

Noting that $\lfloor \frac{j+y}{\lambda} \rfloor = 0$ for each integer $j \in [0, \lambda - y - 1]$, and $\lfloor \frac{j+y}{\lambda} \rfloor = 1$ for each integer $j \in [\lambda - y, \lambda - 1]$, we can derive

$$\sum_{j=0}^{\lambda-1} \left\lfloor \frac{j+y}{\lambda} \right\rfloor = y. \tag{5.7}$$

Next, we determine the value of $\sum\limits_{j=0}^{\lambda-1} \lfloor \frac{2j+y}{\lambda} \rfloor$ through the following two cases:

Case 1. Suppose that λ is even. Since x is even, it follows that y is also even. We can obtain

$$\left\lfloor \frac{2j+y}{\lambda} \right\rfloor = \begin{cases} 0, & \text{if } 0 \le j \le \frac{\lambda-y}{2} - 1, \\ 1, & \text{if } \frac{\lambda-y}{2} \le j \le \frac{2\lambda-y}{2} - 1, \\ 2, & \text{if } \frac{2\lambda-y}{2} \le j \le \lambda - 1. \end{cases}$$

It follows that

$$\sum_{j=0}^{\lambda-1} \left\lfloor \frac{2j+y}{\lambda} \right\rfloor = \left(\frac{2\lambda - y}{2} - \frac{\lambda - y}{2} \right) + 2 \left(\lambda - \frac{2\lambda - y}{2} \right) = \frac{\lambda}{2} + y.$$

Case 2. Suppose that λ is odd. Then we can obtain

$$\left\lfloor \frac{2j+y}{\lambda} \right\rfloor = \begin{cases} 0, & \text{if } 0 \le j \le \frac{\lambda-y}{2} - 1, \\ 1, & \text{if } \frac{\lambda+1}{2} - \lfloor \frac{y+1}{2} \rfloor \le j \le \lambda - \lceil \frac{y+1}{2} \rceil, \\ 2, & \text{if } \lambda - \lceil \frac{y+1}{2} \rceil + 1 \le j \le \lambda - 1. \end{cases}$$

Consequently, we have

$$\begin{aligned} \sum_{j=0}^{\lambda-1} \left\lfloor \frac{2j+y}{\lambda} \right\rfloor &= \left(\lambda - \lceil \frac{y+1}{2} \rceil - \frac{\lambda+1}{2} + \left\lfloor \frac{y+1}{2} \right\rfloor + 1 \right) + 2 \left(\lceil \frac{y+1}{2} \rceil - 1 \right) \\ &= \frac{\lambda-1}{2} - 1 + \lceil \frac{y+1}{2} \rceil + \left\lfloor \frac{y+1}{2} \right\rfloor + 1 \\ &= \frac{\lambda-1}{2} + y. \end{aligned}$$

From equations (5.6) and (5.7), and the discussion for the above two cases, we can conclude that

$$\sum_{j=0}^{\lambda-1}\left[\left\lfloor\frac{2j+x}{\lambda}\right\rfloor-\left\lfloor\frac{j+x}{\lambda}\right\rfloor\right]=\begin{cases}\frac{\lambda}{2}, & \text{if } \lambda \text{ is even,}\\ \frac{\lambda-1}{2}, & \text{if } \lambda \text{ is odd.}\end{cases}$$

Then by applying (5.5), we obtain the desired equation. This completes the proof.

□

The following lemma is a generalization of Lemma 4.2 from Chapter 4 and will be used in the proof of Lemma 5.6 below.

Lemma 5.5. *Let k and $a \in [1, q]$ be two integers. Then*

$$\sum_{t=q^k}^{aq^k-1} N(t+1)=\begin{cases}\frac{1}{2}a(a-1), & \text{if } k=0,\\ \frac{1}{2}(a^2-1)(q-1)q^{2k-1}, & \text{if } k\geq 1.\end{cases}$$

Proof. By definition, we first have

$$\sum_{t=q^k}^{aq^k-1} N(t+1)=\sum_{t=q^k}^{aq^k-1} t-\sum_{t=q^k}^{aq^k-1}\lfloor t/q\rfloor. \tag{5.8}$$

Through direct computation, we obtain

$$\sum_{t=q^k}^{aq^k-1} t=\begin{cases}\frac{1}{2}a(a-1), & \text{if } k=0,\\ \frac{1}{2}(a^2-1)q^{2k}-\frac{1}{2}(a-1)q^k, & \text{if } k\geq 1.\end{cases} \tag{5.9}$$

To determine the value of $\sum_{t=q^k}^{aq^k-1}\lfloor t/q\rfloor$, first note $\lfloor t/q\rfloor=0$ for all $t\in\left[q^k, aq^k-1\right]$ when $k=0$. This implies that $\sum_{t=q^k}^{aq^k-1}\lfloor t/q\rfloor=0$ if $k=0$. While when $k\geq 1$, the interval $\left[q^k, q^{k+1}-1\right]$ can be partitioned as

$$\left[q^k, q^{k+1}-1\right]=\bigsqcup_{i=0}^{q^{k-1}(a-1)-1}\left[q^k+iq, q^k+(i+1)q-1\right].$$

Moreover, for each integer $i \in \big[0, q^{k-1}(a-1)-1\big]$ and $t \in \big[q^k+iq, q^k+(i+1)q-1\big]$, we have $\lfloor t/q \rfloor = q^{k-1} + i$. Therefore,

$$\begin{aligned}\sum_{t=q^k}^{aq^k-1} \lfloor t/q \rfloor &= \sum_{i=0}^{q^{k-1}(a-1)-1} \sum_{t=q^k+iq}^{q^k+(i+1)q-1} (q^{k-1}+i) \\ &= \frac{1}{2}(a^2-1)q^{2k} - \frac{1}{2}(a-1)q^k.\end{aligned}$$

if $k \geq 1$. Combining (5.8), (5.9) and the value of $\sum\limits_{t=q^k}^{q^{k+1}-1} \lfloor t/q \rfloor$ as above, we obtain the desired equality. □

Lemma 5.6. *Let k and $a \in [1, q]$ be two positive integers. Then*

$$\begin{aligned}&\sum_{t=q^{k-i}, q\nmid t}^{aq^{k-i}-1} \left[\left\lfloor \frac{\lfloor tq^{2i-1} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-2} \rfloor + t}{\lambda} \right\rfloor \right] \\ &= \begin{cases} \frac{1}{2\lambda}(a^2-1)(q-1)^2 q^{2k-3}, & \text{if } i \in [-k+2, k-1], \\ \frac{1}{2\lambda} a(a-1)(q-1)q^{2k-2}, & \text{if } i = k \text{ or } -k+1 \end{cases}\end{aligned} \tag{5.10}$$

and

$$\begin{aligned}&\sum_{t=q^{k-i}, q\nmid t}^{aq^{k-i}-1} \left[\left\lfloor \frac{\lfloor tq^{2i} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-1} \rfloor + t}{\lambda} \right\rfloor \right] \\ &= \begin{cases} \frac{1}{2\lambda}(a^2-1)(q-1)^2 q^{2k-2}, & \text{if } i \in [-k+1, 0) \cup (0, k-1], \\ \frac{1}{2\lambda} a(a-1)(q-1)q^{2k-1}, & \text{if } i = k \text{ or } -k. \end{cases}\end{aligned} \tag{5.11}$$

The summations in the lemma above are the most challenging to evaluate in our analysis. Before presenting the detailed proof, we use the identity in (5.10) as an example to introduce the combinatorial meaning of these summations. Note that Lemma 5.1 implies that the summation term in (5.10) is exactly the count of integers in the set $\{\alpha \in [1, \lfloor tq^{2i-1} \rfloor] : q \nmid \alpha \text{ and } \lambda \mid \alpha + t\}$. Thus, the summation in (5.10) is exactly

$$\sum_{t=q^{k-i}, q\nmid t}^{aq^{k-i}-1} \left|\left\{\alpha \in \left[1, \left\lfloor tq^{2i-1}\right\rfloor\right] : q \nmid \alpha \text{ and } \lambda \mid \alpha + t\right\}\right|.$$

This value is needed in the determination of the dimension of $\mathcal{C}_{(q,n,\delta)}$ in Sections 5.3 and 5.5. Therefore, we present the lemma above. We now give the detailed proof as follows.

Proof. The arguments used to derive (5.10) and (5.11) are analogues, so we only demonstrate equation (5.10) holds through the following two cases.

Case 1. Suppose that $1 \le i \le k$. In this case, we first have

$$\left\lfloor \frac{\lfloor tq^{2i-1}\rfloor + t}{\lambda}\right\rfloor = \frac{t(q^{2i-1}-1)}{\lambda} + \left\lfloor \frac{2t}{\lambda}\right\rfloor \text{ and } \left\lfloor \frac{\lfloor tq^{2i-2}\rfloor + t}{\lambda}\right\rfloor = \frac{t(q^{2i-2}-1)}{\lambda} + \left\lfloor \frac{2t}{\lambda}\right\rfloor.$$

It follows that

$$\left\lfloor \frac{\lfloor tq^{2i-1}\rfloor + t}{\lambda}\right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-2}\rfloor + t}{\lambda}\right\rfloor = \frac{tq^{2i-2}(q-1)}{\lambda}.$$

This leads to

$$\begin{aligned} &\sum_{t=q^{k-i}, q\nmid t}^{aq^{k-i}-1} \left[\left\lfloor \frac{\lfloor tq^{2i-1}\rfloor + t}{\lambda}\right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-2}\rfloor + t}{\lambda}\right\rfloor\right] \\ =& \sum_{t=q^{k-i}}^{aq^{k-i}-1} \frac{tq^{2i-2}(q-1)}{\lambda} - \sum_{t\in\mathcal{W}_i} \frac{tq^{2i-2}(q-1)}{\lambda} \end{aligned} \tag{5.12}$$

with $\mathcal{W}_i = \left[q^{k-i}, aq^{k-i}-1\right] \cap \{t \in \mathbb{Z} : q \mid t\}$.

Note that $\mathcal{W}_i = \varnothing$ if $i = k$. Thus,

$$\sum_{t\in\mathcal{W}_i} \frac{tq^{2i-2}(q-1)}{\lambda} = 0 \quad \text{if } i = k. \tag{5.13}$$

On the other hand, it can be easily verified that

$$\mathcal{W}_i = \{q^{k-i} + jq \mid j = 0, \ldots, q^{k-i-1}(a-1) - 1\}$$

if $1 \le i \le k-1$. Therefore,

$$\begin{aligned} \sum_{t\in\mathcal{W}_i} \frac{tq^{2i-2}(q-1)}{\lambda} &= \sum_{j=0}^{q^{k-i-1}(a-1)-1} \frac{(q^{k-i}+qj)q^{2i-2}(q-1)}{\lambda} \\ &= \frac{1}{2\lambda}(q-1)(a-1)\left[(a+1)q^{2k-3} + q^{k+i-2}\right] \qquad (5.14) \end{aligned}$$

if $1 \le i \le k-1$. Additionally, by straightforward computation, we can obtain

$$\sum_{t=q^{k-i}}^{aq^{k-i}-1} \frac{tq^{2i-2}(q-1)}{\lambda} = \begin{cases} \frac{1}{2\lambda}a(a-1)(q-1)^2q^{2k-2}, \text{ if } i=k, \\ \frac{1}{2\lambda}(q-1)(a-1)\left[(a+1)q^{2k-2} - q^{k+i-2}\right], \\ \quad \text{if } 1 \le i \le k-1. \end{cases} \qquad (5.15)$$

By substituting equations (5.13)-(5.15) into equation (5.12), we conclude that equation (5.10) holds for $1 \le i \le k$.

Case 2. Suppose that $-k+1 \le i \le 0$. Then for any integer $t \in \left[q^{k-i}, aq^{k-i}-1\right] \cap \{t \in \mathbb{Z} : q \nmid t\}$ with q-adic expansion $\sum_{\ell=0}^{k-i} t_\ell q^\ell$, we have

$$\left\lfloor tq^{2i-1} \right\rfloor = \left\lfloor tq^{2i-2} \right\rfloor \cdot q + t_{-2i+1}. \qquad (5.16)$$

This leads to

$$\left\lfloor \frac{t + \lfloor tq^{2i-1} \rfloor}{\lambda} \right\rfloor = \frac{\sum_{\ell=0}^{k-i} t_\ell(q^\ell - 1)}{\lambda} + \frac{\lfloor tq^{2i-2} \rfloor (q-1)}{\lambda} + \left\lfloor \frac{\sum_{\ell=0}^{k-i} t_\ell + \lfloor tq^{2i-2} \rfloor + t_{-2i+1}}{\lambda} \right\rfloor.$$

We also have

$$\left\lfloor \frac{t + \lfloor tq^{2i-2} \rfloor}{\lambda} \right\rfloor = \frac{\sum_{\ell=0}^{k-i} t_\ell(q^\ell - 1)}{\lambda} + \left\lfloor \frac{\sum_{\ell=0}^{k-i} t_\ell + \lfloor tq^{2i-2} \rfloor}{\lambda} \right\rfloor.$$

Combining the above two equalities, we can obtain

$$\left\lfloor \frac{t+\lfloor tq^{2i-1}\rfloor}{\lambda} \right\rfloor - \left\lfloor \frac{t+\lfloor tq^{2i-2}\rfloor}{\lambda} \right\rfloor$$

$$= \left\lfloor \frac{\sum_{\ell=0}^{k-i} t_\ell + \lfloor tq^{2i-2}\rfloor + t_{-2i+1}}{\lambda} \right\rfloor - \left\lfloor \frac{\sum_{\ell=0}^{k-i} t_\ell + \lfloor tq^{2i-2}\rfloor}{\lambda} \right\rfloor + \frac{\lfloor tq^{2i-2}\rfloor (q-1)}{\lambda}.$$

By applying Lemma 5.3 with $x = \sum_{\ell=1}^{k-i} t_\ell + \lfloor tq^{2i-2}\rfloor + t_{-2i+1}$ and $y = \sum_{\ell=1}^{k-i} t_\ell + \lfloor tq^{2i-2}\rfloor$, we have

$$\sum_{t_0=1}^{q-1} \left[\left\lfloor \frac{\sum_{\ell=0}^{k-i} t_\ell + \lfloor tq^{2i-2}\rfloor + t_{-2i+1}}{\lambda} \right\rfloor - \left\lfloor \frac{\sum_{\ell=0}^{k-i} t_\ell + \lfloor tq^{2i-2}\rfloor}{\lambda} \right\rfloor \right] = \frac{(q-1)t_{-2i+1}}{\lambda}.$$

Noticing that the value of $\lfloor tq^{2i-2}\rfloor$ is independent of t_0, we get

$$\sum_{t_0=1}^{q-1} \frac{\lfloor tq^{2i-2}\rfloor (q-1)}{\lambda} = \frac{\lfloor tq^{2i-2}\rfloor (q-1)^2}{\lambda}.$$

Noting that $\lfloor tq^{2i-2}\rfloor = \left\lfloor \frac{\lfloor tq^{2i-1}\rfloor}{q} \right\rfloor$ and recalling equation (5.16), we can add the above two sums to obtain

$$\begin{aligned} \sum_{t_0=1}^{q-1} \left[\left\lfloor \frac{t+\lfloor tq^{2i-1}\rfloor}{\lambda} \right\rfloor - \left\lfloor \frac{t+\lfloor tq^{2i-2}\rfloor}{\lambda} \right\rfloor \right] &= \frac{\lfloor tq^{2i-2}\rfloor (q-1)^2}{\lambda} + \frac{(q-1)t_{-2i+1}}{\lambda} \\ &= \frac{q-1}{\lambda} N\left(\left\lfloor tq^{2i-1}\right\rfloor + 1\right). \end{aligned} \tag{5.17}$$

In addition, each integer $t \in \left[q^{k-i}, aq^{k-i+1}-1\right] \cap \{t \in \mathbb{Z} : q \nmid t\}$ with q-adic expansion $\sum_{\ell=0}^{k-i} t_\ell q^\ell$ can be uniquely decomposed as

$$t = \left\lfloor tq^{2i-1}\right\rfloor \cdot q^{-2i+1} + \sum_{\ell=1}^{-2i} t_\ell q^\ell + t_0.$$

Furthermore, as t ranges over integers from q^{k-i} to $q^{k-i+1}-1$ that are not divisible by q, the value of $\lfloor tq^{2i-1} \rfloor$ ranges from q^{k+i-1} to $aq^{k+i-1}-1$. Additionally, for each fixed value of $\lfloor tq^{2i-1} \rfloor$, the sum $\sum_{\ell=1}^{-2i} t_\ell q^\ell$ ranges over integers from 0 to $q^{-2i}-1$, while t_0 varies from 1 to $q-1$. Therefore, we can conclude that

$$\begin{aligned}
&\sum_{t=q^{k-i}, q\nmid t}^{q^{k-i+1}-1} \left[\left\lfloor \frac{\lfloor tq^{2i-1} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-2} \rfloor + t}{\lambda} \right\rfloor \right] \\
=& \sum_{\lfloor tq^{2i-1} \rfloor = q^{k+i-1}}^{aq^{k+i-1}-1} \sum_{\sum_{\ell=1}^{-2i} t_\ell q^\ell = 0}^{q^{-2i}-1} \sum_{t_0=1}^{q-1} \left[\left\lfloor \frac{t + \lfloor tq^{2i-1} \rfloor}{\lambda} \right\rfloor - \left\lfloor \frac{t + \lfloor tq^{2i-2} \rfloor}{\lambda} \right\rfloor \right] \\
=& \sum_{\lfloor tq^{2i-1} \rfloor = q^{k+i-1}}^{aq^{k+i-1}-1} \frac{q^{-2i}(q-1)}{\lambda} N(\lfloor tq^{2i-1} \rfloor + 1),
\end{aligned}$$

where the second equality follows from equation (5.17). We can now apply Lemma 5.5 to conclude that (5.10) holds for $-k+1 \leq i \leq 0$. $\square$

Lemma 5.7. *Let k and $a \in [1, q]$ be two positive integers. Then*

$$\sum_{t=q^k, q\nmid t}^{aq^k-1} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{-1} \rfloor + t}{\lambda} \right\rfloor \right] = \frac{1}{2\lambda}(a^2-1)(q-1)^2 q^{2k-2} + \frac{(3+(-1)^\lambda)}{4\lambda}(a-1)(q-1)q^{k-1}.$$

Proof. Note that each integer $t \in [q^k, aq^k]$ such that $q \nmid t$ can be uniquely decomposed as

$$t = iq + j \quad \text{with } i \in [q^{k-1}, aq^{k-1}-1] \text{ and } j \in [1, q-1].$$

Therefore, by replacing t with $iq+j$, we obtain

$$\sum_{t=q^k, q\nmid t}^{aq^k-1} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{-1} \rfloor + t}{\lambda} \right\rfloor \right]$$

$$= \sum_{i=q^{k-1}}^{aq^{k-1}-1} \sum_{j=1}^{q-1} \left[\left\lfloor \frac{2iq+2j}{\lambda} \right\rfloor - \left\lfloor \frac{i+iq+j}{\lambda} \right\rfloor \right]$$

$$= \sum_{i=q^{k-1}}^{aq^{k-1}-1} \sum_{j=1}^{q-1} \left[\frac{i(q-1)}{\lambda} + \left\lfloor \frac{2j+2i}{\lambda} \right\rfloor - \left\lfloor \frac{j+2i}{\lambda} \right\rfloor \right]$$

$$= \sum_{i=q^{k-1}}^{aq^{k-1}-1} \frac{i(q-1)^2}{\lambda} + \sum_{i=q^{k-1}}^{aq^{k-1}-1} \sum_{j=1}^{q-1} \left[\left\lfloor \frac{2j+2i}{\lambda} \right\rfloor - \left\lfloor \frac{j+2i}{\lambda} \right\rfloor \right].$$

It is straightforward to obtain

$$\sum_{i=q^{k-1}}^{aq^{k-1}-1} \frac{i(q-1)^2}{\lambda} = \frac{q^{k-1}(q-1)^2(aq^{k-1}+q^{k-1}-1)}{2\lambda}.$$

In addition, by applying Lemma 5.4, we have

$$\sum_{i=q^{k-1}}^{aq^{k-1}-1} \sum_{j=1}^{q-1} \left[\left\lfloor \frac{2j+2i}{\lambda} \right\rfloor - \left\lfloor \frac{j+2i}{\lambda} \right\rfloor \right] = \begin{cases} \frac{q^k(q-1)(a-1)}{2\lambda}, & \text{if } \lambda \text{ is odd,} \\ \frac{q^{k-1}(q-1)(q+1)(a-1)}{2\lambda}, & \text{if } \lambda \text{ is even.} \end{cases}$$

Combining the above three equalities, we obtain the desired equation. This completes the proof. □

In addition to establishing the above lemmas, we also need to make some remarks regarding the sets of $\mathcal{A}_k(i)$ and $\mathcal{B}_k(i)$, which are defined in section 3.3 of Chapter 3

For each integer $a \in \mathcal{A}_k(i)$, we define $t(a) = \sum_{\ell=h+i}^{h+k} a_\ell q^{\ell-h-i}$ and $\alpha(a) = \sum_{\ell=0}^{k+i-1} a_\ell q^\ell$;

For each integer $a \in \mathcal{B}_k(i)$, we define $t(a) = \sum_{\ell=h+i}^{h+k} a_\ell q^{\ell-h-i}$ and $\alpha(a) = \sum_{\ell=0}^{k+i} a_\ell q^\ell$. Then we have the following remarks.

Remark 5.1. *The condition in (3.10) can be equivalently represented as* $q \nmid t(a)$.

Remark 5.2. *The condition in (3.12) implies that each integer* $a \in \mathcal{A}_k(i)$ *can be uniquely decomposed as*

$$a = t(a)q^{h+i} + \alpha(a).$$

Since $\lambda \mid q-1$, *it follows that for any integer* $a \in \mathcal{A}_k(i)$,

$$\lambda \mid a \quad \text{if and only if} \quad \lambda \mid t(a) + \alpha(a).$$

Similarly, each integer $a \in \mathcal{B}_k(i)$ *can be uniquely decomposed as*

$$a = t(a)q^{h+i} + \alpha(a),$$

and

$$\lambda \mid a \quad \text{if and only if} \quad \lambda \mid t(a) + \alpha(a).$$

Remark 5.3. *The condition in (3.11) can be equivalently expressed as*

$$1 \le \alpha(a) \le \sum_{\ell=h-i+1}^{h+k} a_\ell q^{\ell-(h-i+1)} \quad \text{and} \quad q \nmid \alpha(a). \tag{5.18}$$

Moreover, the form of $V(a)$ *in (3.12) implies that*

$$\sum_{\ell=h-i+1}^{h+k} a_\ell q^{\ell-(h-i+1)} = t(a) \cdot q^{2i-1} \quad \text{for } i \in [1,k],$$

and

$$\sum_{\ell=h-i+1}^{h+k} a_\ell q^{\ell-(h-i+1)} + \sum_{\ell=h+i}^{h-i} a_\ell q^{\ell-(h-i+1)} \quad = \quad t(a) \cdot q^{2i-1} \quad \text{for } i \in [-k+1,0].$$

Noticing that $0 \le \sum_{\ell=h+i}^{h-i} a_\ell q^{\ell-(h-i+1)} < 1$ *for* $i \in [-k+1,0]$, *we can conclude that (5.18) is equivalent to*

$$1 \le \alpha(a) \le \lfloor t(a) \cdot q^{2i-1} \rfloor \quad \text{and} \quad q \nmid \alpha(a). \tag{5.19}$$

Similarly, the condition in (3.13) can also be written as

$$1 \le \alpha(a) \le \sum_{\ell=h-i}^{h+k} a_\ell q^{\ell-(h-i)} \quad \text{and} \quad q \nmid \alpha(a), \tag{5.20}$$

which is further equivalent to

$$1 \le \alpha(a) \le \left\lfloor t(a) \cdot q^{2i} \right\rfloor \quad \text{and} \quad q \nmid \alpha(a). \tag{5.21}$$

Remark 5.4. *If $a \in \mathcal{A}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$, then*

$$\sum_{\ell=0}^{h-k} a_\ell q^\ell \le \sum_{\ell=h-i+1}^{h+k} a_\ell q^{\ell-(h-i+1)}.$$

Similarly, if $a \in \mathcal{B}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$, then

$$\sum_{\ell=0}^{h-k-1} a_\ell q^\ell \le \sum_{\ell=h-i}^{h+k} a_\ell q^{\ell-(h-i)}.$$

Remark 5.5. *If $a \in \mathcal{A}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$, then i is the smallest integer in $[-k+1, k]$ such that $a_{h+i} > 0$. Consequently, $\mathcal{A}_k(i) \cap \mathcal{A}_k(j) = \varnothing$ for distinct integers $i, j \in [-k+1, k]$.*

Similarly, if $a \in \mathcal{B}_k(i)$ is an integer with q-adic expansion $\sum_{\ell=0}^{h+k} a_\ell q^\ell$, then i is the smallest integer in $[-k, k]$ such that $a_{h+i} > 0$. As a result, $\mathcal{B}_k(i) \cap \mathcal{B}_k(j) = \varnothing$ for distinct integers $i, j \in [-k, k]$.

5.3 Dimension of BCH codes of length $\frac{q^m-1}{\lambda}$

Let $m \ge 4$ and $\delta \in [2, \frac{q^{\lfloor (2m-1)/3 \rfloor + 1} - 1}{\lambda} + 1]$ be an integer. Let k_δ be the integer such that $q^{h+k_\delta} \le \lambda(\delta - 1) < q^{h+k_\delta+1}$. Let $\sum_{\ell=0}^{h+k_\delta} \delta_\ell q^\ell$ denote the q-adic expansion of

$\lambda(\delta-1)$. If $k_\delta \geq m-2h$, let s_δ denote the smallest integer in $[m-2h-k_\delta, k_\delta]$ such that $\delta_{h+s_\delta} > 0$ and define $w_\delta = \sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^\ell$.

If m is odd, for each integer $\delta \in [2, \frac{q^{\lfloor (2m-1)/3 \rfloor+1}-1}{\lambda}+1]$, we define the function $f(\delta)$ by

$$f(\delta) = \begin{cases} 0, & \text{if } \delta \leq \frac{q^{h+1}-1}{\lambda}+1, \\ \left(\begin{array}{l} \frac{(q-1)^2}{\lambda}(k_\delta-1)q^{2k_\delta-3} + \left\lfloor \frac{\mu(\delta)+w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \mu(\delta)/q \rfloor + w_\delta}{\lambda} \right\rfloor \\ + \sum_{i=-k_\delta+1}^{k_\delta} \sum_{t \in \mathcal{T}_i(\delta)} \left[\left\lfloor \frac{\lfloor tq^{2i-1} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-2} \rfloor + t}{\lambda} \right\rfloor \right] \end{array} \right), & \\ & \text{if } \delta > \frac{q^{h+1}-1}{\lambda}+1, \end{cases} \tag{5.22}$$

where

$$\mu(\delta) = \min \left\{ \sum_{\ell=0}^{h-k_\delta} \delta_\ell q^\ell, \sum_{\ell=h-s_\delta+1}^{h+k_\delta} \delta_\ell q^{\ell-(h-s_\delta+1)} \right\}$$

and

$$\mathcal{T}_i(\delta) = \left\{ t \in \mathbb{Z} : q^{k_\delta - i} \leq t < \sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^{\ell-h-i} \text{ and } q \nmid t \right\}.$$

If m is even, for each integer $\delta \in [2, \frac{q^{\lfloor (2m-1)/3 \rfloor+1}-1}{\lambda}+1]$, we define the function $\widetilde{f}(\delta)$ by

$$\widetilde{f}(\delta) = \begin{cases} 0, & \text{if } \delta \leq \frac{q^{h}-1}{\lambda}+1, \\ \left\lfloor \frac{\widetilde{\mu}(\delta)+w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \widetilde{\mu}(\delta)/q \rfloor + w_\delta}{\lambda} \right\rfloor + \sum_{t=1}^{\delta_h-1} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor \right], & \\ & \text{if } \frac{q^h-1}{\lambda}+1 < \delta \leq \frac{q^{h+1}-1}{\lambda}+1, \\ \left(\begin{array}{l} q^{2k_\delta-2}\left(k_\delta - \frac{1}{2}\right)\frac{(q-1)^2}{\lambda} + \frac{q-1}{2\lambda}\left(q^{k_\delta-1} + \frac{1+(-1)^\lambda}{2}\right) \\ + \left\lfloor \frac{\widetilde{\mu}(\delta)+w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \widetilde{\mu}(\delta)/q \rfloor + w_\delta}{\lambda} \right\rfloor \\ + \sum_{i=-k_\delta}^{k_\delta} \sum_{t \in \mathcal{T}_i(\delta)} \left[\left\lfloor \frac{\lfloor tq^{2i} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-1} \rfloor + t}{\lambda} \right\rfloor \right] \end{array} \right), & \\ & \text{if } \delta > \frac{q^{h+1}-1}{\lambda}+1 \end{cases} \tag{5.23}$$

where $\widetilde{\mu}(\delta) = \min\left\{\sum_{\ell=0}^{h-k_\delta-1} \delta_\ell q^\ell, \sum_{\ell=h-s_\delta}^{h+k_\delta} \delta_\ell q^{\ell-(h-s_\delta)}\right\}$. We define the function $\tau(\delta)$ for each integer $\delta \in [2, \frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}+1]$ by

$$\tau(\delta) = \begin{cases} 1, & \text{if } \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} \le \sum_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ & \delta_h > 0 \text{ and } \lambda \mid 2\sum_{\ell=h}^{h+k_\delta} \delta_\ell, \\ 0, & \text{otherwise.} \end{cases} \tag{5.24}$$

Additionally, we define the function $g(\delta)$ for integers $\delta \in [2, \frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}+1]$ by

$$g(\delta) = \begin{cases} 0, & \text{if } \delta \le \frac{q^h-1}{\lambda}+1, \\ \left\lfloor \frac{(\delta_h-1)\left(3+(-1)^\lambda\right)}{2\lambda} \right\rfloor + \tau(\delta) & \\ & \text{if } \frac{q^h-1}{\lambda}+1 < \delta \le \frac{q^{h+1}-1}{\lambda}+1, \\ \left\lfloor \frac{\phi(\delta)\left(3+(-1)^\lambda\right)}{2\lambda} \right\rfloor - \left\lfloor \frac{\lfloor\phi(\delta)/q\rfloor\left(3+(-1)^\lambda\right)}{2\lambda} \right\rfloor + \tau(\delta), & \\ & \text{if } \frac{q^{h+1}-1}{\lambda}+1 < \delta, \end{cases} \tag{5.25}$$

where $\phi(\delta) = \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} - 1$.

Theorem 5.1. *Let $m \ge 4$ and $\delta \in \left[2, \frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}+1\right]$ be two integers.*

- *If m is odd, then*

$$\dim(\mathcal{C}_{(q,n,\delta)}) = n - m\left[N(\delta) - f(\delta)\right]. \tag{5.26}$$

- *If m is even, then*

$$\dim(\mathcal{C}_{(q,n,\delta)}) = n - m\left[N(\delta) - \widetilde{f}(\delta)\right] - \frac{m}{2}g(\delta). \tag{5.27}$$

Outline of the proof. The proof of Theorem 5.1 proceeds via Assertions 5.1–5.5. The overall strategy is analogous to the proof of Theorem 4.1 for primitive BCH codes. We determine the dimension by identifying the coset leaders in $[1, \delta-1]$ and their corresponding coset sizes.

The key distinction in this setting is the code length, which is $n = (q^m-1)/\lambda$ for some divisor λ of $q-1$. Consequently, we should work with q-cyclotomic cosets modulo $(q^m-1)/\lambda$, not q^m-1. Fortunately, Lemma 3.2 and its corollary provide a crucial bridge between q-cyclotomic cosets modulo $(q^m-1)/\lambda$ and q-cyclotomic cosets modulo q^m-1. We now outline the argument for odd and even m separately.

Case 1: m is odd. For an odd $m \geq 4$, applying Lemma 3.2 allows us to relate the coset sizes and coset leaders back to the primitive setting. First, the coset size for any integer $a \in [1, \delta-1]$ is $|C_n(a)| = |C_{\lambda n}(\lambda a)| = m$. Second, the set of coset leaders modulo $n = (q^m-1)/\lambda$ in the interval $[1, \delta-1]$ corresponds to coset leaders modulo q^m-1 in the expanded range $[1, \lambda(\delta-1)]$ that are divisible by λ. Formally,

$$\begin{aligned}
&\{a \in [1, \delta-1] : a \text{ is a leader modulo } n\} \\
=&\{a \in [1, \lambda(\delta-1)] : a \text{ is a leader modulo } q^m-1 \text{ and } \lambda \mid a\}.
\end{aligned}$$

This leads to

$$\dim(\mathcal{C}_{(q,n,\delta)}) = n - m \cdot |\{a \in [1, \lambda(\delta-1)] : a \text{ is a coset leader modulo } q^m-1 \text{ and } \lambda \mid a\}|.$$

Recall the definition of the set $\mathcal{S}$ in (3.9). Note that coset leaders modulo q^m-1 are integers not divisible by q and not in the set $\mathcal{S}$. Thus, the number of such coset leaders is:

$$\begin{aligned}
&|\{a \in [1, \lambda(\delta-1)] : a \text{ is a coset leader modulo } q^m-1 \text{ and } \lambda \mid a\}| \\
=&|\{a \in [1, \lambda(\delta-1)] : q \nmid a \text{ and } \lambda \mid a\}| - |[1, \lambda(\delta-1)] \cap \mathcal{S} \cap \mathcal{D}_\lambda| \\
=&N(\delta) - |[1, \lambda(\delta-1)] \cap \mathcal{S} \cap \mathcal{D}_\lambda|,
\end{aligned}$$

where $\mathcal{D}_\lambda = \{a \in \mathbb{Z} : \lambda \mid a\}$. The problem is now reduced to computing the size of the intersection with $\mathcal{S} \cap \mathcal{D}_\lambda$.

Case 2: m is even. The argument is similar but more complex, as the coset sizes $|C_n(a)|$, which equal $|C_{\lambda n}(\lambda a)|$, can be either m or $m/2$. We must therefore count the coset leaders in each category separately. Recall the definitions of the sets $\mathcal{H}$ and $\mathcal{S}$ in (3.6) and (3.9). Using the same correspondence from Lemma 3.2, we can show that this task is equivalent to counting coset leaders modulo $q^m - 1$ that are divisible by λ, while also keeping track of whether they belong to the set $\mathcal{H}$. This leads to determining the quantities:

- $|[1, \lambda(\delta - 1)] \cap \mathcal{H} \cap \mathcal{D}_\lambda|$;
- $|[1, \lambda(\delta - 1)] \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda|$.

To compute these intersection sizes, we adopt the same partitioning strategy as in the proof of Theorem 4.1. We divide the interval $[1, \lambda(\delta - 1)]$ into disjoint subintervals and, for each piece, count the number of integers belonging to $\mathcal{S} \cap \mathcal{D}_\lambda$ for odd m or $(\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda$ and $\mathcal{H} \cap \mathcal{D}_\lambda$ for even m. This task is accomplished by applying Theorem 3.2, which allows us to break down these intersections into a sum of disjoint intersections with the families $\mathcal{A}_k(i)$ and $\mathcal{B}_k(i)$.

Assertions 5.1 and 5.2 provide the counts for the upper interval range $[q^{h+k_\delta}, \lambda(\delta - 1)]$. To do this, the interval is divided into two parts, with Assertion 5.1 analyzing the first part and Assertion 5.2 the second.

Assertion 5.1. *Suppose that* $\frac{q^{m-h}-1}{\lambda} + 1 < \delta \leq \frac{q^{\lfloor (2m-1)/3 \rfloor + 1}-1}{\lambda} + 1$.

- *If m is odd, then*

$$\left| \left[\sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^\ell, \lambda(\delta - 1) \right] \cap \mathcal{S} \cap \mathcal{D}_\lambda \right| = \left\lfloor \frac{\mu(\delta) + w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \mu(\delta)/q \rfloor + w_\delta}{\lambda} \right\rfloor. \tag{5.28}$$

- *If m is even, then*

$$\left| \left[\sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^\ell, \lambda(\delta - 1) \right] \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda \right| = \left\lfloor \frac{\widetilde{\mu}(\delta) + w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \widetilde{\mu}(\delta)/q \rfloor + w_\delta}{\lambda} \right\rfloor \tag{5.29}$$

and

$$\left|\left[\sum_{\ell=h}^{h+k_\delta}\delta_\ell q^\ell,\lambda(\delta-1)\right]\cap\mathcal{H}\cap\mathcal{D}_\lambda\right|=\tau(\delta). \tag{5.30}$$

Proof. Suppose that m is odd. We first aim to show that

$$\left[\sum_{\ell=h+s_\delta}^{h+k_\delta}\delta_\ell q^\ell,\lambda(\delta-1)\right]\cap\mathcal{S}\cap\mathcal{D}_\lambda=\left[\sum_{\ell=h+s_\delta}^{h+k_\delta}\delta_\ell q^\ell,\lambda(\delta-1)\right]\cap\mathcal{A}_{k_\delta}(s_\delta)\cap\mathcal{D}_\lambda. \tag{5.31}$$

For any integer $a\in\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell,\lambda(\delta-1)\right]$ with q-adic expansion $\sum_{\ell=0}^{h+k_\delta}a_\ell q^\ell$, we have

$$V(\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell)\le V(a)\le V(\lambda(\delta-1)).$$

Noting that

$$V(\lambda(\delta-1))=(\mathbf{0}_{h-k_\delta},\delta_{h+k_\delta},\dots,\delta_0)$$

and

$$V(\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell)=(\mathbf{0}_{h-k_\delta},\delta_{h+k_\delta},\dots,\delta_{h-k_\delta+1},\mathbf{0}_{h-k_\delta+1}),$$

it follows that

$$V(a)=(\mathbf{0}_{h-k_\delta},a_{h+k_\delta},\dots,a_0)=(\mathbf{0}_{h-k_\delta},\delta_{h+k_\delta},\dots,\delta_{h-k_\delta+1},a_{h-k_\delta},\dots,a_0). \tag{5.32}$$

Recalling the definition of s_δ, it follows that s_δ is the smallest integer in $[-k_\delta+1,k_\delta]$ such that $a_{h+s_\delta}>0$. By Remark 5.5, this implies $a\notin\mathcal{A}_{k_\delta}(i)$ for any integer $i\neq s_\delta$. Therefore, $\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta}\delta_\ell q^\ell,\delta-1\right]\cap\mathcal{A}_{k_\delta}(i)=\varnothing$ for any integer $i\neq s_\delta$. Then applying Theorem 3.2, we can conclude that (5.31) holds.

Now, let us count the number of integers in the set

$$\left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell, \delta-1\right] \cap \mathcal{A}_{k_\delta}(s_\delta) \cap \mathcal{D}_\lambda.$$

Recall

$$w_\delta = \sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^\ell, \alpha(a) = \sum_{\ell=0}^{k_\delta+s_\delta-1} a_\ell q^\ell \text{ and } \mu(\delta) = \min\left\{\sum_{\ell=0}^{h-k_\delta} \delta_\ell q^\ell, \sum_{\ell=h-s_\delta+1}^{h+k_\delta} \delta_\ell q^{\ell-(h-s_\delta+1)}\right\}.$$

for each integer $a \in \mathcal{A}_{k_\delta}(s_\delta)$ with q-adic expansion $\sum_{\ell=0}^{h+k_\delta} a_\ell q^\ell$. We conclude from equation (5.32) and the definition of $\mathcal{A}_{k_\delta}(s_\delta)$ that an integer

$$a \in \left[\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell, \delta-1\right] \cap \mathcal{A}_{k_\delta}(s_\delta) \cap \mathcal{D}_\lambda$$

if and only if a admits the decomposition

$$a = w_\delta + \alpha(a)$$

with $\alpha(a) \in \{\alpha \in [1, \mu(\delta)] : q \nmid \alpha \text{ and } \lambda \mid \alpha + w_\delta\}$. Consequently, we have

$$\left|\left[\sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^\ell, \lambda(\delta-1)\right] \cap \mathcal{A}_{k_\delta} \cap \mathcal{D}_\lambda\right| = \left|\{\alpha \in [1, \mu(\delta)] : q \nmid \alpha \text{ and } \lambda \mid \alpha + w_\delta\}\right|.$$

Then by applying Lemma 5.1, equation (5.28) follows.

Suppose that m is even. The equality in (5.29) can be obtained by emplying a similar argument as above. It remains to establish equation (5.30). By applying Lemma 3.3, we can conclude that $a \in \left[\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell, \lambda(\delta-1)\right] \cap \mathcal{H} \cap \mathcal{D}_\lambda$ if and only if $V(a)$ has the form

$$(\mathbf{0}_{h-k_\delta-1}, \delta_{h+k_\delta}, \ldots, \delta_h, \mathbf{0}_{h-k_\delta-1}, \delta_{h+k_\delta}, \ldots, \delta_h)$$

with $\delta_h > 0$, $\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} \leq \sum_{\ell=0}^{h-1} \delta_\ell q^\ell$ and $\lambda \mid \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} + \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell$. Since $\lambda \mid q-1$, the condition $\lambda \mid \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} + \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell$ is equivalent $\lambda \mid 2\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell$. Therefore, an integer satisfying the above condition exists and is unique if and only if $\delta_h > 0$, $\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} \leq \sum_{\ell=0}^{h-1} \delta_\ell q^\ell$ and $\lambda \mid 2\sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell$. It follows that equation (5.30) holds. $\square$

Assertion 5.2. *Suppose that* $\frac{q^{m-h}-1}{\lambda} + 1 < \delta \leq \frac{q^{\lfloor (2m-1)/3 \rfloor + 1}-1}{\lambda} + 1$.

- *If m is odd, then*

$$\begin{aligned} &\left| \left[q^{h+k_\delta}, \sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{S} \cap \mathcal{D}_\lambda \right| \\ &= \sum_{i=-k_\delta+1}^{k_\delta} \sum_{t \in \mathcal{T}_i(\delta)} \left[\left\lfloor \frac{\lfloor t q^{2i-1} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor t q^{2i-2} \rfloor + t}{\lambda} \right\rfloor \right]. \end{aligned} \tag{5.33}$$

- *If m is even, then*

$$\begin{aligned} &\left| \left[q^{h+k_\delta}, \sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^\ell \right) \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda \right| \\ &= \sum_{i=-k_\delta}^{k_\delta} \sum_{t \in \mathcal{T}_i(\delta)} \left[\left\lfloor \frac{\lfloor t q^{2i} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor t q^{2i-1} \rfloor + t}{\lambda} \right\rfloor \right] \end{aligned} \tag{5.34}$$

  and

$$\begin{aligned} &\left| \left[q^{h+k_\delta}, \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{H} \cap \mathcal{D}_\lambda \right| \\ &= \begin{cases} \left\lfloor \frac{(\delta_h - 1)\left(3+(-1)^\lambda\right)}{2\lambda} \right\rfloor, & \textit{if } k_\delta = 0, \\ \left\lfloor \frac{\phi(\delta)\left(3+(-1)^\lambda\right)}{2\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \phi(\delta)/q \rfloor \left(3+(-1)^\lambda\right)}{2\lambda} \right\rfloor - \frac{q^{k_\delta - 1}(q-1)\left(3+(-1)^\lambda\right)}{2\lambda}, \\ \qquad \textit{if } k_\delta \geq 1, \end{cases} \end{aligned} \tag{5.35}$$

where $\phi(\delta) = \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} - 1.$

Proof. Suppose that m is odd. By definition, an integer

$$a \in \left[q^{h+k_\delta}, \sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell\right) \cap \mathcal{A}_{k_\delta}(i)$$

if and only if the following conditions are satisfied:

(i) $V(a)$ is of the form given in (3.12) and satisfies (3.10) and (3.11) for $k = k_\delta$;

(ii) $V(q^{h+k_\delta}) \leq V(a) < V\left(\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell\right)$.

Notice that

$$V(q^{h+k_\delta}) = (\mathbf{0}_{h-k_\delta}, 1, \mathbf{0}_{h+k_\delta})$$

and

$$V\left(\sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell\right) = (\mathbf{0}_{h-k_\delta}, \delta_{h+k_\delta}, \ldots, \delta_{h-k_\delta+1}, \mathbf{0}_{h-k_\delta+1}).$$

Therefore, the form of $V(a)$ in (3.12) together with the inequality $a_0 > 0$ in (3.11) imply that condition (ii) is satisfied if and only if

$$(1, \mathbf{0}_{2k_\delta-1}) \leq (a_{h+k_\delta}, \ldots, a_{h+i}, \mathbf{0}_{k_\delta+i-1}) < (\delta_{h+k_\delta}, \ldots, \delta_{h-k_\delta+1}).$$

Since s_δ is the smallest integer in $[-k_\delta+1, k_\delta]$ such that $\delta_{h+s_\delta} > 0$, this is further equivalent to

$$q^{k_\delta - i} \leq \sum_{\ell=h+i}^{h+k_\delta} a_\ell q^{\ell-h-i} < \sum_{\ell=h+s_\delta}^{h+k_\delta} \delta_\ell q^{\ell-h-i}.$$

Recall the definition of the set $\mathcal{T}_i(\delta)$ and Remarks 5.1 – 5.3. We now can conclude that for each integer $i \in [-k_\delta+1, k_\delta]$, an integer

$$a \in \left[q^{h+k_\delta}, \sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell\right) \cap \mathcal{A}_{k_\delta}(i) \cap \mathcal{D}_\lambda$$

if and only if a admits the decomposition

$$a = t(a) \cdot q^{h+i} + \alpha(a)$$

with

$$\begin{cases} \lambda \mid t(a) + \alpha(a), \\ t(a) \in \mathcal{T}_i(\delta), \\ 1 \le \alpha(a) \le \lfloor t(a) \cdot q^{2i-1} \rfloor \text{ and } q \nmid \alpha(a). \end{cases}$$

Consequently, we can apply Lemma 5.1 to conclude that

$$\begin{aligned} &\left| \left[q^{h+k_\delta}, \sum_{\ell=h-k_\delta+1}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{A}_{k_\delta}(i) \cap \mathcal{D}_\lambda \right| \\ &= \sum_{t \in \mathcal{T}_i(\delta)} \left| \left\{ \alpha \in [1, \lfloor tq^{2i-1} \rfloor] : q \nmid \alpha \text{ and } \lambda \mid \alpha + t \right\} \right| \\ &= \sum_{t \in \mathcal{T}_i(\delta)} \left[\left\lfloor \frac{\lfloor tq^{2i-1} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-2} \rfloor + t}{\lambda} \right\rfloor \right]. \end{aligned}$$

Then applying Theorem 3.2, it follows that (5.33) holds.

Suppose that m is even. We can first utilize a similar argument as above to obtain (5.34). Next, we demonstrate that equation (5.35) holds. By applying Lemma 3.3, we can conclude that an integer $a \in \left[q^{h+k_\delta}, \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell \right) \cap \mathcal{H} \cap \mathcal{D}_\lambda$ if and only if a can be decomposed as decomposition

$$a = \sum_{\ell=0}^{k_\delta} a_\ell q^\ell \cdot q^h + \sum_{\ell=0}^{k_\delta} a_\ell q^\ell \tag{5.36}$$

with $q \nmid \sum_{\ell=0}^{k_\delta} a_\ell q^\ell$, $q^{h+k_\delta} \le a < \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell$ and $\lambda \mid a$. It is easy to see that $q^{h+k_\delta} \le a < \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell$ holds if and only if $q^{k_\delta} \le \sum_{\ell=0}^{k_\delta} a_\ell q^\ell \le \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} - 1$. Furthermore, since $\lambda \mid q-1$, the condition $\lambda \mid a$ is satisfied if and only if $\lambda \mid 2\sum_{\ell=0}^{k_\delta} a_\ell q^\ell$. Therefore, an integer $a \in \left[q^{h+k_\delta}, \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell\right) \cap \mathcal{H} \cap \mathcal{D}_\lambda$ if and only if a admits the decomposition given in (5.36) with

$$\begin{cases} q^{k_\delta} \le \sum_{\ell=0}^{k_\delta} a_\ell q^\ell \le \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} - 1; \\ q \nmid \sum_{\ell=0}^{k_\delta} a_\ell q^\ell; \\ \lambda \mid 2 \sum_{\ell=0}^{k_\delta} a_\ell q^\ell. \end{cases}$$

Consequently,

$$\begin{aligned} &\left| \left[q^{h+k_\delta}, \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^\ell\right) \cap \mathcal{H} \cap \mathcal{D}_\lambda \right| \\ =& \left| \left\{ \alpha \in \left[q^{k_\delta}, \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} - 1\right] : \lambda \mid 2\alpha \text{ and } q \nmid \alpha \right\} \right|. \end{aligned}$$

By applying Lemma 5.2, it follows that equation (5.35) holds. □

Having addressed the interval $\left[q^{h+k_\delta}, \lambda(\delta-1)\right]$ in Assertions 5.1 and 5.2, we proceed to analyze the remaining segment, $\left[1, q^{h+k_\delta}\right)$. First, consider the case where m is odd. The quantity to be determined is $\left|\left[1, q^{h+k_\delta}\right) \cap \mathcal{S} \cap \mathcal{D}_\lambda\right|$. We begin by applying Lemma 3.3, which establishes that $\left|\left[1, q^{h+1}-1\right] \cap \mathcal{S} \cap \mathcal{D}_\lambda\right| = 0$. The analysis of the non-trivial portion is then facilitated by the following summation:

$$\left|\left[q^{h+1}, q^{h+k_\delta}\right) \cap \mathcal{S} \cap \mathcal{D}_\lambda\right| = \sum_{k=1}^{k_\delta - 1} \left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{S} \cap \mathcal{D}_\lambda\right|.$$

Theorem 3.2 provides the mechanism for computing each term in this sum, expressing $\left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{S} \cap \mathcal{D}_\lambda\right|$ as a summation over the quantities $|\mathcal{A}_k(i) \cap \mathcal{D}_\lambda|$ for $i \in [-k+1, k]$. Similarly, for even m, the calculation depends on the sizes of both $\mathcal{B}_k(i) \cap \mathcal{D}_\lambda$ and the intersection size $\left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{H} \cap \mathcal{D}_\lambda\right|$. The required formulas for the terms involving $\mathcal{A}_k(i)$ and $\mathcal{B}_k(i)$ are given in Assertions 5.3 and 5.4, while the value for the $\mathcal{H}$ intersection is given in Assertion 5.5.

Assertion 5.3. *Suppose that $k \in [1, \lfloor (2m-1)/3 \rfloor - h]$ is an integer.*

- *If m is odd, then*

$$|\mathcal{A}_k(i) \cap \mathcal{D}_\lambda| = \begin{cases} \frac{1}{2\lambda}(q-1)^3(q+1)q^{2k-3}, & \textit{if } i \in [-k+2, k-1], \\ \frac{1}{2\lambda}(q-1)^2 q^{2k-1}, & \textit{if } i = -k+1 \textit{ or } k. \end{cases} \tag{5.37}$$

- *If m is even, then*

$$|\mathcal{B}_k(i) \cap \mathcal{D}_\lambda| = \begin{cases} \frac{1}{2\lambda}(q-1)^3(q+1)q^{2k-2}, & \textit{if } [-k+1, 0) \cup (0, k-1], \\ \frac{1}{2\lambda}(q-1)^2 q^{2k}, & \textit{if } i = -k \textit{ or } k. \end{cases} \tag{5.38}$$

Proof. The arguments used to establish (5.37) and (5.38) are analogous. Therefore, we only demonstrate that (5.37) holds when m is odd. Using reasoning similar to that in the proof of Assertion 2, we can conclude that an integer $a \in \mathcal{A}_{k_\delta}(i) \cap \mathcal{D}_\lambda$ if and only if a admits the decomposition

$$a = t(a) \cdot q^{h+i} + \alpha(a)$$

with

$$\begin{cases} \lambda \mid t(a) + \alpha(a); \\ t(a) \in \left[q^{k-i}, \, q^{k-i+1} - 1\right] \cap \{t \in \mathbb{Z} : q \nmid t\}; \\ 1 \le \alpha(a) \le \lfloor t(a) \cdot q^{2i-1} \rfloor \ \text{ and } q \nmid \alpha(a). \end{cases}$$

Consequently, by applying Lemma 5.1, we derive

$$\begin{aligned} |\mathcal{A}_{k_\delta}(i) \cap \mathcal{D}_\lambda| &= \sum_{t=q^{k-i}, q\nmid t}^{q^{k-i+1}-1} \left| \left\{ \alpha \in \left[1, \left\lfloor t q^{2i-1} \right\rfloor\right] : q \nmid \alpha \text{ and } \lambda \mid \alpha + t \right\} \right| \\ &= \sum_{t=q^{k-i}, q\nmid t}^{q^{k-i+1}-1} \left[\left\lfloor \frac{\lfloor t q^{2i-1} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor t q^{2i-2} \rfloor + t}{\lambda} \right\rfloor \right]. \end{aligned}$$

Then applying Lemma 5.6, we obtain equation (5.37). $\square$

Assertion 5.4. *Suppose that m is even and $k \in [0, \lfloor (2m-1)/3 \rfloor - h]$ is an integer.*

- *If λ is odd, then*

$$|B_k(0) \cap \mathcal{D}_\lambda| = \begin{cases} \frac{q(q-1)}{2\lambda}, & \text{if } k = 0, \\ \frac{(q-1)^2}{2\lambda}(q^{2k} - q^{2k-2} + q^{k-1}) & \text{if } k \geq 1. \end{cases}$$

- *If λ is even, then*

$$|B_k(0) \cap \mathcal{D}_\lambda| = \begin{cases} \frac{(q+1)(q-1)}{2\lambda}, & \text{if } k = 0, \\ \frac{(q-1)^2}{2\lambda}(q^{2k} - q^{2k-2} + 2q^{k-1}) & \text{if } k \geq 1. \end{cases}$$

Proof. Following a similar approach to the proof of Assertion 5.3, we can obtain

$$|B_k(0) \cap \mathcal{D}_\lambda| = \sum_{t=q^k, q \nmid t}^{q^{k+1}-1} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{-1} \rfloor + t}{\lambda} \right\rfloor \right].$$

Then applying Lemmas 5.4 and 5.7, the assertion follows. $\square$

Assertion 5.5. *Suppose that $m \geq 4$ is an even integer, and $k \in [0, \lfloor (2m-1)/3 \rfloor - h]$ is an integer.*

- *If λ is odd, then*

$$\left| \left[q^{h+k}, q^{h+k+1} \right) \cap \mathcal{H} \cap \mathcal{D}_\lambda \right| = \begin{cases} \frac{q-1}{\lambda}, & \text{for } k = 0, \\ \frac{(q-1)^2 q^{k-1}}{\lambda}, & \text{for } k \geq 1. \end{cases} \tag{5.39}$$

- *If λ is even, then*

$$\left| \left[q^{h+k}, q^{h+k+1} \right) \cap \mathcal{H} \cap \mathcal{D}_\lambda \right| = \begin{cases} \frac{2(q-1)}{\lambda}, & \text{for } k = 0, \\ \frac{2(q-1)^2 q^{k-1}}{\lambda}, & \text{for } k \geq 1. \end{cases} \tag{5.40}$$

Proof. By applying Lemma 3.3, we can conclude that an integer

$$a \in \mathcal{H} \cap [q^{h+k}, q^{h+k+1}) \cap \mathcal{D}_\lambda$$

if and only if a adimits the decomposition

$$a = \sum_{\ell=0}^{k} a_\ell q^\ell \cdot q^h + \sum_{\ell=0}^{k} a_\ell q^\ell. \tag{5.41}$$

with $a_0 > 0$, $a_k > 0$, and $\lambda \mid a$. Since $\lambda \mid q-1$, it follows that $\lambda \mid a$ is equivalent to $\lambda \mid 2\sum\limits_{\ell=0}^{k} a_\ell q^\ell$. In addition, it is straightforward to verify that the conditions $a_0 > 0$ and $a_k > 0$ are satisfied if and only if $q^k \le \sum\limits_{\ell=0}^{k} a_\ell q^\ell \le q^{k+1}-1$ and $q \nmid \sum\limits_{\ell=0}^{k} a_\ell q^\ell$. Therefore, an integer $a \in \mathcal{H} \cap [q^{h+k}, q^{h+k+1}) \cap \mathcal{D}_\lambda$ if and only if a has the decomposition as given in (5.41) with

$$\begin{cases} q \nmid \sum\limits_{\ell=0}^{k} a_\ell q^\ell; \\ q^k \le \sum\limits_{\ell=0}^{k} a_\ell q^\ell \le q^{k+1} - 1; \\ \lambda \mid 2\sum\limits_{\ell=0}^{k} a_\ell q^\ell. \end{cases}$$

Consequently,

$$\left|\mathcal{H} \cap \left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{D}_\lambda\right| = \left|\left\{\alpha \in \left[q^k, q^{k+1}-1\right] : \lambda \mid 2\alpha \text{ and } q \nmid \alpha\right\}\right|.$$

Then by applying Lemma 5.2, the assertion follows. $\square$

Having established the above assertions, we now prove Theorem 5.1.

Proof of Theorem 5.1. Suppose that m is odd. We first aim to show that

$$|[1, \lambda(\delta-1)] \cap \mathcal{S} \cap \mathcal{D}_\lambda| = f(\delta) \quad \text{for } \delta \in \left[2, \frac{q^{\lfloor (2m-1)/3 \rfloor + 1} - 1}{\lambda} + 1\right]. \tag{5.42}$$

If $2 \le \delta \le \frac{q^{h+1}-1}{\lambda} + 1$, then $\lambda \le \lambda(\delta-1) \le q^{h+1}-1$. By applying Lemma 3.3, we can obtain

$$[1, \lambda(\delta-1)] \cap \mathcal{S} \cap \mathcal{D}_\lambda = 0.$$

In particular,

$$\left|\left[1, q^{h+1}-1\right] \cap \mathcal{S} \cap \mathcal{D}_\lambda\right| = 0. \tag{5.43}$$

If $\frac{q^{h+1}-1}{\lambda}+1 < \delta \le \frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}+1$, then $q^{h+1} \le \lambda(\delta-1) < q^{\lfloor(2m-1)/3\rfloor+1}$. This implies $1 \le k_\delta \le \lfloor(2m-1)/3\rfloor - h$. By applying Theorem 3.2, we can conclude from Assertion 5.3 that for any integer $k \in [1, \lfloor(2m-1)/3\rfloor - h]$,

$$\begin{aligned}
\left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{S} \cap \mathcal{D}_\lambda\right| &= \sum_{i=-k+1}^{k} |\mathcal{A}_k(i) \cap \mathcal{D}_\lambda| \\
&= \frac{1}{\lambda}\left[(k-1)q^{2k-3}(q-1)^3(q+1) + q^{2k-1}(q-1)^2\right].
\end{aligned}$$

Therefore,

$$\begin{aligned}
&\left|\left[q^{h+1}, q^{h+k_\delta}\right) \cap \mathcal{S} \cap \mathcal{D}_\lambda\right| \\
=& \sum_{k=1}^{k_\delta-1} \left|\left[q^{h+k}, q^{h+k+1}\right) \cap \mathcal{S} \cap \mathcal{D}_\lambda\right| \\
=& \sum_{k=1}^{k_\delta-1} \frac{(q-1)^3}{\lambda}(q+1)(k-1)q^{2k-3} + \sum_{k=1}^{k_\delta-1} \frac{q^{2k-1}(q-1)^2}{\lambda}.
\end{aligned}$$

It is straightforward to verify that

$$\sum_{k=1}^{k_\delta-1} \frac{q^{2k-1}(q-1)^2}{\lambda} = \frac{(q^{2k_\delta-1}-q)(q-1)}{\lambda(q+1)}$$

and

$$\sum_{k=1}^{k_\delta-1} \frac{(q-1)^3}{\lambda}(q+1)(k-1)q^{2k-3} = \frac{\left[q-(k_\delta-1)q^{2k_\delta-3}+(k_\delta-2)q^{2k_\delta-1}\right](q-1)}{\lambda(q+1)}.$$

By adding these two sums, we can obtain

$$\left|\left[q^{h+1}, q^{h+k_\delta}\right) \cap \mathcal{S} \cap \mathcal{D}_\lambda\right| = \frac{(q-1)^2}{\lambda}(k_\delta-1)q^{2k_\delta-3}. \tag{5.44}$$

Combining equations (5.28), (5.33), (5.43) and (5.44) we obtain

$$\begin{aligned}
&|[1,\lambda(\delta-1)]\cap\mathcal{S}\cap\mathcal{D}_\lambda|\\
=&\frac{(q-1)^2}{\lambda}(k_\delta-1)q^{2k_\delta-3}+\left\lfloor\frac{\mu(\delta)+w_\delta}{\lambda}\right\rfloor-\left\lfloor\frac{\lfloor\mu(\delta)/q\rfloor+w_\delta}{\lambda}\right\rfloor\\
&+\sum_{i=-k_\delta+1}^{k_\delta}\sum_{t\in\mathcal{T}_i(\delta)}\left[\left\lfloor\frac{\lfloor tq^{2i-1}\rfloor+t}{\lambda}\right\rfloor-\left\lfloor\frac{\lfloor tq^{2i-2}\rfloor+t}{\lambda}\right\rfloor\right].
\end{aligned}$$

Recalling the definition of $f(\delta)$, we can now claim that equation (5.42) holds.

Next, we establish equation (5.26). Noticing that $\lfloor(2m-1)/3\rfloor+1\le m-\lfloor m/3\rfloor$, we have $\lambda(\delta-1)<q^{m-\lfloor m/3\rfloor}$. Therefore, we can apply Theorem 3.1 and Lemma 3.2 to obtain

$$|C_n(a)|=|C_{\lambda n}(\lambda a)|=m\quad\text{for all } a\in[1,\delta-1]\tag{5.44}$$

and

$$\mathcal{L}_m^{\lambda n}(1,\lambda(\delta-1))=\mathcal{L}^{\lambda n}(1,\lambda(\delta-1)).$$

Recalling the definition of $\mathcal{S}$ and noting that an integer a cannot be the coset leader of $C_n(a)$ if $q\mid a$, it follows that

$$\begin{aligned}
&\left|\mathcal{L}_m^{\lambda n}(1,\lambda(\delta-1))\cap\mathcal{D}_\lambda\right|\\
=&\left|\mathcal{L}^{\lambda n}(1,\lambda(\delta-1))\cap\mathcal{D}_\lambda\right|\\
=&\left|\{a\in[1,\lambda(\delta-1)]:q\nmid a\}\cap\mathcal{D}_\lambda\right|-\left|[1,\lambda(\delta-1)]\cap\mathcal{S}\cap\mathcal{D}_\lambda\right|.
\end{aligned}$$

It can be easily verified that

$$|\{a\in[1,\lambda(\delta-1)]:q\nmid a\}\cap\mathcal{D}_\lambda|=N(\delta).$$

Utilizing Corollary 3.1 and equation (5.42), we have

$$|\mathcal{L}_m^n(1,\delta-1)|=\left|\mathcal{L}_m^{\lambda n}(1,\lambda(\delta-1))\cap\mathcal{D}_\lambda\right|=N(\delta)-f(\delta).\tag{5.45}$$

Recalling the equality in (2.13), we can now conclude from (5.44) and (5.45) that (5.26) holds.

Suppose that m is even. Our first goal is to show that

$$|[1, \lambda(\delta - 1)] \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda| = \widetilde{f}(\delta) \tag{5.46}$$

and

$$|[1, \lambda(\delta - 1)] \cap \mathcal{H} \cap \mathcal{D}_\lambda| = g(\delta) \tag{5.47}$$

for $\delta \in [2, \frac{q^{\lfloor (2m-1)/3 \rfloor + 1} - 1}{\lambda} + 1]$.

If $2 \leq \delta \leq \frac{q^h - 1}{\lambda} + 1$, then we have $2\lambda \leq \lambda(\delta - 1) \leq q^h - 1$. By applying Lemma 3.3, we can conclude that

$$|[1, \lambda(\delta - 1)] \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda| = 0$$

and

$$|[1, \lambda(\delta - 1)] \cap \mathcal{H} \cap \mathcal{D}_\lambda| = 0.$$

In particular, we have

$$\left|\left[1, q^h - 1\right] \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda\right| = 0 \tag{5.48}$$

and

$$\left|\left[1, q^h - 1\right] \cap \mathcal{H} \cap \mathcal{D}_\lambda\right| = 0. \tag{5.49}$$

If $\frac{q^h - 1}{\lambda} + 1 < \delta \leq \frac{q^{h+1} - 1}{\lambda} + 1$, then we have $q^h \leq \lambda(\delta - 1) \leq q^{h+1} - 1$. Since m is even, we have

- $k_\delta = 0$;
- $\mathcal{T}_0(\delta) = \{t \in \mathbb{Z} : 1 \leq t \leq \delta_h - 1\}$;

By substituting k_δ and $\mathcal{T}_0(\delta)$ as above into equations (5.29) and (5.34), we obtain

$$\left|\left[\delta_h q^h, \lambda(\delta - 1)\right] \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda\right| = \left\lfloor \frac{\widetilde{\mu}(\delta) + w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \widetilde{\mu}(\delta)/q \rfloor + w_\delta}{\lambda} \right\rfloor$$

and

$$\left|\left[q^h, \delta_h q^h\right) \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda\right| = \sum_{t=1}^{\delta_h - 1} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor\right].$$

Combining the above two equalities with (5.48), we obtain

$$\begin{aligned} &|[1, \lambda(\delta-1)] \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda| \\ =& \left\lfloor \frac{\widetilde{\mu}(\delta) + w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \widetilde{\mu}(\delta)/q \rfloor + w_\delta}{\lambda} \right\rfloor + \sum_{t=1}^{\delta_h - 1} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor\right]. \end{aligned} \tag{5.50}$$

Additionally, by substituting $k_\delta = 0$ into (5.30) and (5.35), we have

$$\left|\left[\delta_h q^h, \lambda(\delta - 1)\right] \cap \mathcal{H} \cap \mathcal{D}_\lambda\right| = \tau(\delta)$$

and

$$\left|\left[q^h, \delta_h q^h\right) \cap \mathcal{H} \cap \mathcal{D}_\lambda\right| = \left\lfloor \frac{\left(3 + (-1)^\lambda\right)(\delta_h - 1)}{2\lambda} \right\rfloor.$$

Combining these two equalities with (5.49), we obtain

$$|[1, \lambda(\delta - 1)] \cap \mathcal{H} \cap \mathcal{D}_\lambda| = \left\lfloor \frac{\left(3 + (-1)^\lambda\right)(\delta_h - 1)}{2\lambda} \right\rfloor + \tau(\delta). \tag{5.51}$$

Notice that $\lambda(\delta - 1) = q^{h+1} - 1 = \sum\limits_{\ell=0}^{h} (q-1) q^\ell$ when $\delta = \frac{q^{h+1}-1}{\lambda} + 1$. Therefore, for $\delta = \frac{q^{h+1}-1}{\lambda} + 1$, we have

$$\widetilde{\mu}(\delta) = q - 1, w_\delta = (q-1)q^h \text{ and } \delta_h = q - 1.$$

Consequently, by substituting $\delta = \frac{q^{h+1}-1}{\lambda} + 1$ into equation (5.50) and applying Lemma 5.4, we obtain

$$\begin{aligned} &\left|\left[1, q^{h+1} - 1\right] \cap (\mathcal{S} \cup \mathcal{H}) \cap \mathcal{D}_\lambda\right| \\ =& \left\lfloor \frac{(q-1)(q^h + 1)}{\lambda} \right\rfloor - \left\lfloor \frac{(q-1)q^h}{\lambda} \right\rfloor + \sum_{t=1}^{q-2} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor\right] \\ =& \frac{q-1}{2\lambda}\left(q + \frac{1 + (-1)^\lambda}{2}\right). \end{aligned} \tag{5.52}$$

If $\frac{q^{h+1}-1}{\lambda}+1<\delta\leq\frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}+1$, then we have $q^{h+1}\leq\lambda(\delta-1)<q^{\lfloor(2m-1)/3\rfloor+1}$. This implies that $1\leq k_\delta\leq\lfloor(2m-1)/3\rfloor-h$. By applying Theorem 3.2, we can conclude from Assertions 5.3 and 5.4 that

$$\begin{aligned}\left|\left[q^{h+k},q^{h+k+1}\right)\cap(\mathcal{S}\cup\mathcal{H})\cap\mathcal{D}_\lambda\right| &= \sum_{i=-k}^{k}|\mathcal{B}_k(i)| \\ &= \frac{(q-1)^3}{\lambda}(k-\frac{1}{2})q^{2k-2}(q+1)+)\frac{(q-1)^2}{\lambda}(\frac{1}{2}q^{k-1}+q^{2k}) \qquad (5.53)\end{aligned}$$

for each integer $k\in[1,\lfloor(2m-1)/3\rfloor-h]$. It follows that

$$\begin{aligned}\left|\left[q^{h+1},q^{h+k_\delta}\right)\cap(\mathcal{S}\cup\mathcal{H})\right| &= \sum_{k=1}^{k_\delta-1}\left|\left[q^{h+k},q^{h+k+1}\right)\cap(\mathcal{S}\cup\mathcal{H})\right| \qquad (5.54)\\ &= \frac{(q-1)^2}{\lambda}(k_\delta-\frac{1}{2})q^{2k_\delta-2}+\frac{q-1}{2\lambda}(q^{k_\delta-1}-q).\end{aligned}$$

Combing (5.29), (5.34), (5.52) and (5.54), we derive

$$\begin{aligned}&|[1,\lambda(\delta-1)]\cap(\mathcal{S}\cup\mathcal{H})\cap\mathcal{D}_\lambda|\\ =&\frac{q-1}{2\lambda}\left(q^{k_\delta-1}+\frac{1+(-1)^\lambda}{2}\right)+\left\lfloor\frac{\widetilde{\mu}(\delta)+w_\delta}{\lambda}\right\rfloor-\left\lfloor\frac{\lfloor\widetilde{\mu}(\delta)/q\rfloor+w_\delta}{\lambda}\right\rfloor\\ &+\frac{(q-1)^2}{\lambda}(k_\delta-\frac{1}{2})q^{2k_\delta-2}+\sum_{i=-k_\delta}^{k_\delta}\sum_{t\in\mathcal{T}_i(\delta)}\left[\left\lfloor\frac{\lfloor tq^{2i}\rfloor+t}{\lambda}\right\rfloor-\left\lfloor\frac{\lfloor tq^{2i-1}\rfloor+t}{\lambda}\right\rfloor\right]\end{aligned}$$

On the other hand, we conclude from Assertion 5.5 that

$$\begin{aligned}\left|\left[q^{h},q^{h+k_\delta}\right)\cap\mathcal{H}\cap\mathcal{D}_\lambda\right| &= \sum_{k=0}^{k_\delta-1}\left|\left[q^{h+k},q^{h+k+1}\right)\cap\mathcal{H}\cap\mathcal{D}_\lambda\right|\\ &=\frac{(3+(-1)^\lambda)(q-1)q^{k_\delta-1}}{2\lambda}.\end{aligned}$$

With (5.30) and (5.35), it follows that

$$|[1,\lambda(\delta-1))\cap\mathcal{H}\cap\mathcal{D}_\lambda|=\left\lfloor\frac{\phi(\delta)\left(3+(-1)^\lambda\right)}{\lambda}\right\rfloor-\left\lfloor\frac{\lfloor\phi(\delta)/q\rfloor\left(3+(-1)^\lambda\right)}{2\lambda}\right\rfloor+\tau(\delta),$$

where $\phi(\delta) = \sum_{\ell=h}^{h+k_\delta} \delta_\ell q^{\ell-h} - 1$.

By now, we have already demonstrated that both (5.46) and (5.47) hold for $\delta \in [2, \frac{q^{\lfloor (2m-1)/3 \rfloor + 1} - 1}{\lambda} + 1]$. Next, we show that equation (5.27) holds. Notice that $\lambda(\delta - 1) < q^{m - \lfloor m/4 \rfloor}$. We can apply Theorem 3.1 and Lemma 3.2 to obtain

$$|C_n(a)| = |C_{\lambda n}(\lambda a)| = m \text{ or } \frac{m}{2} \quad \text{for } a \in [1, \delta - 1]. \tag{5.55}$$

By applying Corollary 3.1, we can derive from (5.46) and (5.47) that

$$|\mathcal{L}_m^n(1, \delta - 1)| = \left|\mathcal{L}_m^{\lambda n}(1, \lambda(\delta - 1)) \cap \mathcal{D}_\lambda\right| = N(\delta) - \widetilde{f}(\delta) \tag{5.56}$$

and

$$\left|\mathcal{L}_{\frac{m}{2}}^n(1, \delta - 1)\right| = \left|\mathcal{L}_{\frac{m}{2}}^{\lambda n}(1, \lambda(\delta - 1)) \cap \mathcal{D}_\lambda\right| = g(\delta). \tag{5.57}$$

Recalling the equality in (2.13), we can now conclude from (5.55), (5.56) and (5.57) that (5.27) holds. This completes the proof. □

As examples of Theorem 5.1, we present the following two corollaries, Corollary 5.1 and Corollary 5.2, that determine the dimension of $\mathcal{C}_{(q,n,\delta)}$ for designed distances in the range $2 \le \delta \le \frac{q^{\lceil m/2 \rceil + 1} - 1}{\lambda} + 1$.

We compare the formulas in the these two corollaries with those given by Zhu et al. in [60], which determined the dimension for designed distances $2 \le \delta \le \frac{q^{\lceil (m+1)/2 \rceil} - 1}{\lambda} + 1$. Note that $\lceil \frac{m}{2} \rceil + 1 > \lceil \frac{m+1}{2} \rceil$ when m is odd, and $\lceil \frac{m}{2} \rceil + 1 = \lceil \frac{m+1}{2} \rceil$ when m is even. Consequently, Corollary 5.2 extends the known range of designed distances for odd m. For even m, Corollary 5.1 covers the same range as Zhu's result but provides a more concise formula for the dimension.

Corollary 5.1. *Let $m \ge 4$ be an even integer and $\delta \in \left[2, \frac{q^{h+1} - 1}{\lambda} + 1\right]$ be an integer.*

Then

$$\dim(\mathcal{C}_{(q,n,\delta)})$$

$$= \begin{cases} n - mN(\delta), \\ \qquad \textit{if } \delta \leq \frac{q^h-1}{\lambda} + 1, \\ n - mN(\delta) + m \sum\limits_{t=1}^{\delta_h} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor \right] - \frac{m}{2} \left\lfloor \frac{\left(3+(-1)^{\lambda}\right)(\delta_h-1)}{2\lambda} \right\rfloor - \frac{m}{2}, \\ \qquad \textit{if } \delta > \frac{q^h-1}{\lambda} + 1, \delta_h \leq \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell \ \textit{and } \lambda \mid 2\delta_h, \\ n - mN(\delta) + m \sum\limits_{t=1}^{\delta_h} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor \right] - \frac{m}{2} \left\lfloor \frac{\left(3+(-1)^{\lambda}\right)(\delta_h-1)}{2\lambda} \right\rfloor, \\ \qquad \textit{if } \delta > \frac{q^h-1}{\lambda} + 1, \delta_h \leq \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell \ \textit{and } \lambda \nmid 2\delta_h, \\ n - mN(\delta) + m \left[\sum\limits_{t=1}^{\delta_h} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor \right] + \left\lfloor \frac{\delta_0+\delta_h}{\lambda} \right\rfloor - \left\lfloor \frac{2\delta_h}{\lambda} \right\rfloor \right] - \frac{m}{2} \left\lfloor \frac{\left(3+(-1)^{\lambda}\right)(\delta_h-1)}{2\lambda} \right\rfloor, \\ \qquad \textit{if } \delta > \frac{q^h-1}{\lambda} + 1 \ \textit{and } \delta_h > \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell. \end{cases} \tag{5.58}$$

Proof. If $2 \leq \delta \leq \frac{q^h-1}{\lambda} + 1$, then we have $\widetilde{f}(\delta) = 0$ and $g(\delta) = 0$.

If $\frac{q^h-1}{\lambda} + 1 < \delta$, then we distinguish the following two cases.

Case 1. Suppose that $\delta_h \leq \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell$. Then we have $\widetilde{\mu}(\delta) = \delta_h$ and $w_\delta = \delta_h q^h$. By substituting them into equation (5.23), we obtain

$$\widetilde{f}(\delta) = \left\lfloor \frac{\delta_h + \delta_h q^h}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_h q^h}{\lambda} \right\rfloor + \sum_{t=1}^{\delta_h - 1} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor \right]$$

$$= \sum_{t=1}^{\delta_h} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor \right].$$

In addition, it is straight forward to verify that

$$\tau(\delta) = \begin{cases} 1, & \text{if } \lambda \mid 2\delta_h, \\ 0, & \text{if } \lambda \nmid 2\delta_h. \end{cases}$$

Recalling equaiton (5.25), it follows that

$$g(\delta)=\begin{cases}\left\lfloor\frac{\left(3+(-1)^{\lambda}\right)(\delta_h-1)}{2\lambda}\right\rfloor+1, & \text{if } \lambda\mid 2\delta_h,\\ \left\lceil\frac{\left(3+(-1)^{\lambda}\right)(\delta_h-1)}{2\lambda}\right\rceil, & \text{if } \lambda\nmid 2\delta_h.\end{cases}$$

Case 2. Suppose that $\delta_h>\sum_{\ell=0}^{h-1}\delta_\ell q^\ell$, then $\widetilde{\mu}(\delta)=\sum_{\ell=0}^{h-1}\delta_\ell q^\ell=\delta_0$. $w_\delta=\delta_h q^h$ and $\tau(\delta)=0$. By substituting these values into equations (5.23) and (5.25), we obtain

$$\widetilde{f}(\delta)=\left\lfloor\frac{\delta_0+\delta_h}{\lambda}\right\rfloor-\left\lfloor\frac{2\delta_h}{\lambda}\right\rfloor+\sum_{t=1}^{\delta_h}\left[\left\lfloor\frac{2t}{\lambda}\right\rfloor-\left\lfloor\frac{t}{\lambda}\right\rfloor\right]$$

and

$$g(\delta)=\left\lfloor\frac{\left(3+(-1)^{\lambda}\right)(\delta_h-1)}{2\lambda}\right\rfloor.$$

Finally, substituting the values of $g(\delta)$ and $\widetilde{f}(\delta)$ for corresponding cases into equation (5.27), we derive the desired equation (5.58). □

To prove Corollary 5.2, we need the following lemma.

Lemma 5.8. *Suppose that $a\geq 1$ is an integer. Then*

$$\sum_{t=q,q\nmid t}^{aq}\left[\left\lfloor\frac{\lfloor tq^{-1}\rfloor+t}{\lambda}\right\rfloor-\left\lfloor\frac{t}{\lambda}\right\rfloor\right]=\frac{a(a-1)(q-1)}{2\lambda}.$$

Proof. Notice that each integer $t\in[q,aq]$ such that $q\nmid t$ adimits a unique decomposition

$$t=iq+j\quad\text{with } i\in[1,a-1]\text{ and } j\in[1,q-1].$$

It follows that

$$\begin{aligned}\left\lfloor\frac{\lfloor tq^{-1}\rfloor+t}{\lambda}\right\rfloor-\left\lfloor\frac{t}{\lambda}\right\rfloor&=\left\lfloor\frac{i+iq+j}{\lambda}\right\rfloor-\left\lfloor\frac{iq+j}{\lambda}\right\rfloor\\&=\left\lfloor\frac{j+2i}{\lambda}\right\rfloor-\left\lfloor\frac{j+i}{\lambda}\right\rfloor.\end{aligned}$$

Then by applying Lemma 5.3, we obtain

$$\sum_{t=q,q\nmid t}^{aq}\left[\left\lfloor\frac{\lfloor tq^{-1}\rfloor+t}{\lambda}\right\rfloor-\left\lfloor\frac{t}{\lambda}\right\rfloor\right]=\sum_{i=1}^{a-1}\sum_{j=1}^{q-1}\left[\left\lfloor\frac{j+2i}{\lambda}\right\rfloor-\left\lfloor\frac{j+i}{\lambda}\right\rfloor\right]$$
$$=\sum_{i=1}^{a-1}\frac{(q-1)i}{\lambda}$$
$$=\frac{a(a-1)(q-1)}{2\lambda}.$$

This completes the proof. $\square$

Corollary 5.2. *Let $m\geq 5$ be an odd integer and $\delta\in\left[2,\frac{q^{h+2}-1}{\lambda}+1\right]$ be an integer.*

$$\dim(\mathcal{C}_{(q,n,\delta)})$$
$$=\begin{cases} n-mN(\delta), \\ \qquad \text{if } \delta\leq\frac{q^{h+1}-1}{\lambda}+1, \\ n-mN(\delta)+m\left(\left\lfloor\frac{\delta_0+\delta_{h+1}+\delta_h}{\lambda}\right\rfloor-\left\lfloor\frac{2\delta_{h+1}+\delta_h}{\lambda}\right\rfloor\right) \\ +m\left(\sum_{i=1}^{\delta_h}\left[\left\lfloor\frac{2\delta_{h+1}+i}{\lambda}\right\rfloor-\left\lfloor\frac{\delta_{h+1}+i}{\lambda}\right\rfloor\right]++\frac{\delta_{h+1}^2(q-1)}{\lambda}\right), \\ \qquad \text{if } \delta>\frac{q^{h+1}-1}{\lambda}+1, \delta_h>0 \text{ and } \delta_{h+1}>\sum_{\ell=0}^{h-1}\delta_\ell q^\ell, \\ n-mN(\delta)+m\left(\frac{\delta_{h+1}^2(q-1)}{\lambda}+\sum_{i=1}^{\delta_h}\left[\left\lfloor\frac{2\delta_{h+1}+i}{\lambda}\right\rfloor-\left\lfloor\frac{\delta_{h+1}+i}{\lambda}\right\rfloor\right]\right), \\ \qquad \text{if } \delta>\frac{q^{h+1}-1}{\lambda}+1, \delta_h>0 \text{ and } \delta_{h+1}\leq\sum_{\ell=0}^{h-1}\delta_\ell q^\ell, \\ n-mN(\delta)+m\left(\frac{\left(\delta_{h+1}^2-\delta_{h+1}+\delta_1\right)(q-1)}{\lambda}+\left\lfloor\frac{\delta_1+\delta_0+\delta_{h+1}}{\lambda}\right\rfloor-\left\lfloor\frac{\delta_1+\delta_{h+1}}{\lambda}\right\rfloor\right), \\ \qquad \text{if } \delta>\frac{q^{h+1}-1}{\lambda}+1, \delta_h=0 \text{ and } \delta_{h+1}q>\sum_{\ell=0}^{h-1}\delta_\ell q^\ell, \\ n-mN(\delta)+m\frac{\delta_{h+1}^2(q-1)}{\lambda}, \\ \qquad \text{if } \delta>\frac{q^{h+1}-1}{\lambda}+1, \delta_h=0 \text{ and } \delta_{h+1}q\leq\sum_{\ell=0}^{h-1}\delta_\ell q^\ell. \end{cases} \tag{5.59}$$

Proof. If $\delta\leq\frac{q^{h+1}-1}{\lambda}+1$, we can directly have $f(\delta)=0$.

If $\delta>\frac{q^{h+1}-1}{\lambda}+1$, then we have $k_\delta=1$. We distinguish following cases.

Case 1. Suppose that $\delta_h>0$. Then we have $s_\delta=0$. This leads to

- $\mathcal{T}_0(\delta) = \{t \in \mathbb{Z} : q \le t \le \delta_{h+1}q + \delta_h - 1 \text{ and } q \nmid t\}$;
- $\mathcal{T}_1(\delta) = \{t \in \mathbb{Z} : 1 \le t \le \delta_{h+1}\}$;
- $w_\delta = \delta_{h+1}q^{h+1} + \delta_h q^h$;
- $\mu(\delta) = \min\left\{\delta_{h+1}, \sum_{\ell=0}^{h-1} \delta_\ell q^\ell\right\}$.

Recall equation (5.22). It follows that

$$\begin{aligned} f(\delta) = &\left\lfloor \frac{\mu(\delta) + w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \mu(\delta)/q + w_\delta}{\lambda} \right\rfloor \\ &+ \sum_{t=q, q\nmid t}^{\delta_{h+1}q+\delta_h-1} \left[\left\lfloor \frac{\lfloor tq^{-1} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor \right] \\ &+ \sum_{t=1}^{\delta_{h+1}} \left[\left\lfloor \frac{tq + t}{\lambda} \right\rfloor - \left\lfloor \frac{2t}{\lambda} \right\rfloor \right]. \end{aligned} \tag{5.60}$$

Note that $\mu(\delta) = \delta_{h+1}$ if $\delta_{h+1} \le \sum_{\ell=0}^{h-1} \delta_\ell q^\ell$, and $\mu(\delta) = \sum_{\ell=0}^{h-1} \delta_\ell q^\ell = \delta_0$ if $\delta_{h+1} > \sum_{\ell=0}^{h-1} \delta_\ell q^\ell$.

We obtain

$$\begin{aligned} &\left\lfloor \frac{\mu(\delta) + w_\delta}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor \mu(\delta)/q \rfloor + w_\delta}{\lambda} \right\rfloor \\ &= \begin{cases} \left\lfloor \frac{\delta_0 + \delta_{h+1} + \delta_h}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_{h+1} + \delta_h}{\lambda} \right\rfloor, & \text{if } \delta_{h+1} > \sum_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ \left\lfloor \frac{2\delta_{h+1} + \delta_h}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_{h+1} + \delta_h}{\lambda} \right\rfloor, & \text{if } \delta_{h+1} \le \sum_{\ell=0}^{h-1} \delta_\ell q^\ell. \end{cases} \end{aligned} \tag{5.61}$$

By applying Lemma 5.8, we derive

$$\sum_{t=q, q\nmid t}^{\delta_{h+1}q} \left[\left\lfloor \frac{\lfloor tq^{-1} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor \right] = \frac{\delta_{h+1}(\delta_{h+1} - 1)(q-1)}{2\lambda}.$$

Since each integer $t \in [\delta_{h+1}q+1, \delta_{h+1}q+\delta_h-1]$ can be uniquely expressed as $t = \delta_{h+1}q+i$ with $i \in [1, \delta_h-1]$, we have

$$\sum_{t=\delta_{h+1}q+1}^{\delta_{h+1}q+\delta_h-1} \left[\left\lfloor \frac{\lfloor tq^{-1}\rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor\right] = \sum_{i=1}^{\delta_h-1} \left[\left\lfloor \frac{2\delta_{h+1}+i}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_{h+1}+i}{\lambda} \right\rfloor\right].$$

Adding above two sums, we get

$$\begin{aligned}&\sum_{t=q,q\nmid t}^{\delta_{h+1}q+\delta_h-1} \left[\left\lfloor \frac{\lfloor tq^{-1}\rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor\right] \\ =&\frac{\delta_{h+1}(\delta_{h+1}-1)(q-1)}{2\lambda} + \sum_{i=1}^{\delta_h-1} \left[\left\lfloor \frac{2\delta_{h+1}+i}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_{h+1}+i}{\lambda} \right\rfloor\right].\end{aligned} \tag{5.62}$$

Furthermore, it is straightforward to verify that

$$\begin{aligned}\sum_{t=1}^{\delta_{h+1}} \left[\left\lfloor \frac{tq+t}{\lambda} \right\rfloor - \left\lfloor \frac{2t}{\lambda} \right\rfloor\right] &= \sum_{t=1}^{\delta_{h+1}} \frac{t(q-1)}{\lambda} \\ &= \frac{\delta_{h+1}(\delta_{h+1}+1)(q-1)}{2\lambda}.\end{aligned} \tag{5.63}$$

We now can conclude from (5.60) – (5.63) that

$$f(\delta) = \begin{cases} \left\lfloor \frac{\delta_0+\delta_{h+1}+\delta_h}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_{h+1}+\delta_h}{\lambda} \right\rfloor + \frac{\delta_{h+1}^2(q-1)}{\lambda} + \sum\limits_{i=1}^{\delta_h-1} \left[\left\lfloor \frac{2\delta_{h+1}+i}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_{h+1}+i}{\lambda} \right\rfloor\right], \\ \qquad \text{if } \delta_h > 0 \text{ and } \delta_{h+1} > \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell, \\ \frac{\delta_{h+1}^2(q-1)}{\lambda} + \sum\limits_{i=1}^{\delta_h} \left[\left\lfloor \frac{2\delta_{h+1}+i}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_{h+1}+i}{\lambda} \right\rfloor\right], \\ \qquad \text{if } \delta_h > 0 \text{ and } \delta_{h+1} \le \sum\limits_{\ell=0}^{h-1} \delta_\ell q^\ell. \end{cases}$$

Case 2. Suppose that $\delta_h = 0$. Then we have $s_\delta = 1$. This leads to

- $\mathcal{T}_0(\delta) = \{t \in \mathbb{Z} : q \le t \le \delta_{h+1}q-1 \text{ and } q \nmid t\}$;
- $\mathcal{T}_1(\delta) = \{t \in \mathbb{Z} : 1 \le t \le \delta_{h+1}-1\}$;

- $w_\delta = \delta_{h+1}q^{h+1}$;

- $\mu(\delta) = \min\left\{\delta_{h+1}q, \sum\limits_{\ell=0}^{h-1}\delta_\ell q^\ell\right\}$

Note that $\mu(\delta) = \sum\limits_{\ell=0}^{h-1}\delta_\ell q^\ell = \delta_1 q + \delta_0$ if $\delta_{h+1}q > \sum\limits_{\ell=0}^{h-1}\delta_\ell q^\ell$, and $\mu(\delta) = \delta_{h+1}q$ if $\delta_{h+1}q \leq \sum\limits_{\ell=0}^{h-1}\delta_\ell q^\ell$. By substituting these terms into equation (5.22), we can use an analogous argument as in **Case 1** to obtain

$$f(\delta) = \begin{cases} \frac{\delta_{h+1}^2(q-1)}{\lambda}, & \text{if } \delta_h = 0 \text{ and } \delta_{h+1}q \leq \sum\limits_{\ell=0}^{h-1}\delta_\ell q^\ell, \\ \frac{(\delta_{h+1}^2-\delta_{h+1}+\delta_1)(q-1)}{\lambda} + \left\lfloor \frac{\delta_1+\delta_0+\delta_{h+1}}{\lambda} \right\rfloor - \left\lfloor \frac{\delta_1+\delta_{h+1}}{\lambda} \right\rfloor, & \\ & \text{if } \delta_h = 0 \text{ and } \delta_{h+1}q > \sum\limits_{\ell=0}^{h-1}\delta_\ell q^\ell. \end{cases}$$

Finally, substituting the value of $f(\delta)$ into equation (5.26) for each corresponding case, we can conclude that (5.59) holds. This completes the proof. □

5.4 Bose distance of BCH code of length $\frac{q^m-1}{\lambda}$

In this section, we investigate the Bose distance of BCH codes $\mathcal{C}_{(q,n,\delta)}$ for $\delta \in \left[2, \frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}\right]$. Note that if $q \nmid \delta$, we can apply Lemma 3.1 to conclude that δ is not a coset leader modulo n, and hence $d_B(\mathcal{C}_{(q,n,\delta)}) = d_B(\mathcal{C}_{(q,n,\delta+1)})$. Thus, it is enough to focus on BCH codes $\mathcal{C}_{(q,n,\delta)}$ with $q \nmid \delta$. Their Bose distances are established as follows.

- For $\delta \in \left[2, \frac{q^{m-h}-1}{\lambda}\right]$ with $q \nmid \delta$, the result is given in Theorem 5.2.

- For $\delta \in \left[\frac{q^{m-h}-1}{\lambda}, \frac{q^{\lfloor(2m-1)/3\rfloor+1}-1}{\lambda}\right]$ with $q \nmid \delta$, the Bose distance is determined in Theorems 5.3 and 5.4.

Theorem 5.2. *Let m and $\delta \in \left[2, \frac{q^{m-h}-1}{\lambda}\right]$ be two integers with $q \nmid \delta$. Then $d_B(\mathcal{C}_{(q,n,\delta)}) = \delta$.*

Proof. It is clear that $2 \leq \lambda\delta < q^{m-h}$ and $q \nmid \lambda\delta$. By [57, Theorem 2.3], it follows that $\lambda\delta$ is a coset leader modulo λn. Then applying Lemma 3.2, we conclude that δ is a coset leader modulo n. Then the result follows. $\square$

Theorem 5.3. *Suppose that $m \geq 5$ is odd and $\delta \in \left[\frac{q^{h+1}-1}{\lambda}+1, \frac{q^{\lfloor (2m-1)/3 \rfloor+1}-1}{\lambda}\right]$ is an integer such that $q \nmid \delta$. Let $j_\delta = \left\lfloor \log_q(\lambda\delta) \right\rfloor - h$ and $\sum_{\ell=0}^{h+j_\delta} \delta_\ell q^\ell$ be the q-adic expansion of $\lambda\delta$. Define r_δ as the smallest integer in $[-j_\delta+1, j_\delta]$ such that $\delta_{h+r_\delta} > 0$ and $\hat{\delta} = \sum_{\ell=h+r_\delta}^{h+j_\delta} \delta_\ell q^\ell + \sum_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}$. Then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } \sum_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell > \sum_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(m-h-r_\delta)}, \\ \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 1, & \text{if } \sum_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell \leq \sum_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)} \\ & \text{and } \delta_{h-r_\delta+1} + \lambda - q \neq \hat{\delta} \bmod \lambda, \\ \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 2, & \text{if } \sum_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell \leq \sum_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)} \\ & \text{and } \delta_{h-r_\delta+1} + \lambda - q = \hat{\delta} \bmod \lambda. \end{cases} \tag{5.64}$$

Proof. We show that equation (5.64) holds by considering the following cases.

Case 1. Suppose that $\sum_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell > \sum_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}$. By Remarks 5.4 and 5.5, the inequality implies that $\lambda\delta \notin \mathcal{A}_{j_\delta}$ for every integer $i \in [-j_\delta+1, j_\delta]$. Therefore, by Theorem 3.2, we conclude $\lambda\delta \notin \mathcal{S}$. Note that the assumptions $q \nmid \delta$ and $\lambda \mid q-1$ imply $q \nmid \lambda\delta$. It follows that $\lambda\delta$ is a coset leader modulo λn. Applying Lemma 3.2, we further obtain that δ is a coset leader modulo n. Consequently, we have $d_B(\mathcal{C}_{(q,n,\delta)}) = \delta$.

Case 2. Suppose that $\sum\limits_{\ell=0}^{h-j_\delta} \delta_\ell q^\ell \le \sum\limits_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}$. With an argument similar to that in the proof of Theorem 4.4, we can show that each integer in $[\lambda\delta, \hat{\delta}]$ is not a coset leader modulo λn. Applying Lemma 3.2, it follows that each integer in $[\delta, \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor]$ is not a coset leader modulo n. Notice that when m is odd,

$$\hat{\delta} = \lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + \hat{\delta} \bmod \lambda = \sum_{\ell=h+r_\delta}^{h+j_\delta} \delta_\ell q^\ell + \sum_{\ell=h-r_\delta+1}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)}.$$

Thus, we have

$$\lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + \lambda = \sum_{\ell=h+r_\delta}^{h+j_\delta} \delta_\ell q^\ell + \sum_{\ell=h-r_\delta+2}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta+1)} + \delta_{h-r_\delta+1} - \hat{\delta} \bmod \lambda + \lambda.$$

This implies that

$$q \mid \lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + \lambda \quad \text{if and only if} \quad \delta_{h-r_\delta+1} + \lambda - q = \hat{\delta} \bmod \lambda.$$

Then we distinguish the following two subcases:

Subcase 1. If $\delta_{h-r_\delta+1} + \lambda - q \neq \hat{\delta} \bmod \lambda$, then $q \nmid \lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + \lambda$. Applying a similar argument as in Case 1, we can show that $\lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + \lambda$ is a coset leader modulo $\lambda n = q^m - 1$. By applying Lemma 3.2, it follows that $\left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 1$ is a coset leader modulo n. Consequently, $d_B(\mathcal{C}_{(q,n,\delta)}) = \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 1$.

Subcase 2. If $\delta_{h-r_\delta+1} + \lambda - q = \hat{\delta} \bmod \lambda$, then $q \mid \lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + \lambda$ and $q \nmid \lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 2\lambda$. This implies that $\lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + \lambda$ is not a coset leader of λn. Furthermore, using a similar argument as in Case 1 again, we can conclude that while $\lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 2\lambda$ is a coset leader modulo λn. By applying Lemma 3.2, it follows that $\left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 1$ is not a coset leader modulo n, while $\left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 2$ is a coset leader modulo n. Therefore, we have $d_B(\mathcal{C}_{(q,n,\delta)}) = \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 2$. □

Theorem 5.4. *Suppose that $m \geq 4$ is even and $\delta \in \left[\frac{q^h-1}{\lambda} + 1, \frac{q^{\lfloor (2m-1)/3 \rfloor + 1} - 1}{\lambda}\right]$ is an integer such that $q \nmid \delta$. Let $j_\delta = \left\lfloor \log_q(\lambda\delta) \right\rfloor - h$ and $\sum_{\ell=0}^{h+j_\delta} \delta_\ell q^\ell$ be the q-adic expansion of $\lambda\delta$. Define r_δ as the smallest integer in $[-j_\delta, j_\delta]$ such that $\delta_{h+r_\delta} > 0$ and $\hat{\delta} = \sum_{\ell=h+r_\delta}^{h+j_\delta} \delta_\ell q^\ell + \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)}$.*

- *If $r_\delta \neq 0$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell > \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)}, \\ \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 1, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell \leq \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)} \\ & \text{and } \delta_{h-r_\delta} + \lambda - q \neq \hat{\delta} \bmod \lambda, \\ \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 2, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell \leq \sum_{\ell=h-r_\delta}^{h+j_\delta} \delta_\ell q^{\ell-(h-r_\delta)} \\ & \text{and } \delta_{h-r_\delta} + \lambda - q = \hat{\delta} \bmod \lambda. \end{cases} \tag{5.65}$$

- *If $r_\delta = 0$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell \geq \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}, \\ \frac{\hat{\delta}}{\lambda}, & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell < \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h} \text{ and } \lambda \mid \hat{\delta}, \\ \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 1 & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell < \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}, \lambda \nmid \hat{\delta} \\ & \text{and } \delta_h + \lambda - q \neq \hat{\delta} \bmod \lambda, \\ \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 2 & \text{if } \sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell < \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}, \lambda \nmid \hat{\delta} \\ & \text{and } \delta_h + \lambda - q = \hat{\delta} \bmod \lambda. \end{cases} \tag{5.66}$$

Proof. We can use an argument analogous to that in the proof of Theorem 5.3 to conclude that 5.65) holds if $r_\delta \neq 0$. Thus, we now only demonstrate equation (5.66) by considering the following cases.

Case 1. Suppose that $\sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell \geq \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}$. If the inequality is strict, by Theorem 3.2 together and Remarks 5.4–5.5, we have $\lambda\delta \notin \mathcal{S} \cup \mathcal{H}$; If equality holds, by Lemma 3.3, we $\lambda\delta \in \mathcal{H}$. Note that the assumptions $q \nmid \delta$ and $\lambda \mid q-1$ imply $q \nmid \lambda\delta$. Therefore, in either case, $\lambda\delta$ is a coset leader modulo λn. By Lemma 3.2, it follows that δ is a coset leader of modulo n. Therefore, $d_B(\mathcal{C}_{(q,n,\delta)}) = \delta$.

Case 2. Suppose that $\sum_{\ell=0}^{h-j_\delta-1} \delta_\ell q^\ell < \sum_{\ell=h}^{h+j_\delta} \delta_\ell q^{\ell-h}$. We can use an analogous argument, as in the proof of Theorem 4.4 to show that each integer in $[\lambda\delta, \hat{\delta})$ is not a coset leader modulo λn. By Lemma 3.2, it follows that each integer $a \in \left[\delta, \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor\right)$ is not a coset leader modulo n. Then we distinguish the following two subcases:

Subcase 1. Assume that $\lambda \mid \hat{\delta}$. Using Lemma 3.3, it is straightforward to verify that $\hat{\delta} \in \mathcal{H}$, and hence $\hat{\delta}$ is a coset leader modulo λn. It follows that $\frac{\hat{\delta}}{\lambda}$ is a coset leader modulo n. Therefore, we can obtain $d_B(\mathcal{C}_{(q,n,\delta)}) = \frac{\hat{\delta}}{\lambda}$.

Subcase 2. Assume that $\lambda \nmid \hat{\delta}$. Then we have $\lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor < \hat{\delta}$. Recalling that each integer in $[\lambda\delta, \hat{\delta})$ is not a coset leader modulo λn, this implies that $\lambda \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor$ is not a coset leader modulo λn. By Lemma 3.2,it follows that $\left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor$ is not a coset leader modulo n. Then we can use an analogous argument as in the proof of Case 2 of Theorem 5.3 to conclude that $d_B(\mathcal{C}_{(q,n,\delta)}) = \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 1$ if $\delta_h + \lambda - q \neq \hat{\delta} \bmod \lambda$, and $d_B(\mathcal{C}_{(q,n,\delta)}) = \left\lfloor \frac{\hat{\delta}}{\lambda} \right\rfloor + 2$ if $\delta_h + \lambda - q = \hat{\delta} \bmod \lambda$. $\square$

Using the formulas provided in the above sections, we identify several narrow-sense BCH codes of length $\frac{q^m-1}{\lambda}$ that are either optimal or have parameters matching those of the best known linear codes in the database. Most of these codes occur in the primitive case $\lambda = 1$, which are presented in Table 4.2 and Table 4.3 in Chapter 4. In addition, we list further examples of narrow-sense BCH codes $\mathcal{C}_{(q,(q^m-1)/\lambda,\delta)}$ with $\lambda \neq 1$ in Table 5.1. The parameters of these codes are nearly optimal or best known. All parameters were verified by Magma, and for all BCH codes in the table, the Bose distance d_B coincides with the minimum distance d.

Table 5.1: Examples of BCH code $\mathcal{C}_{(q,(q^m-1)/\lambda,\delta)}$ with $\lambda \neq 1$

q	m	λ	n	δ	k	d_B	Optimality
3	4	2	40	$9-10$	18	10	$d_{best} = 13$
3	4	2	40	11	16	11	$d_{best} = 15$
3	4	2	40	$12-13$	12	13	$d_{best} = 18$
3	5	2	121	2	116	2	$d_{optimal} = 3$
3	5	2	121	$3-4$	111	4	$d_{optimal} = 5$
3	5	2	121	5	106	5	$d_{best} = 6$
3	5	2	121	$6-7$	101	7	$d_{best} = 8$
3	5	2	121	8	96	8	$d_{best} = 9$
3	5	2	121	$9-10$	91	10	$d_{best} = 11$
3	5	2	121	11	86	11	$d_{best} = 13$
3	5	2	121	$12-13$	81	13	$d_{best} = 15$
3	5	2	121	$14-16$	76	16	$d_{best} = 17$
3	5	2	121	17	71	17	$d_{best} = 19$
3	5	2	121	$18-19$	66	19	$d_{best} = 21$
3	5	2	121	20	61	20	$d_{best} = 23$
3	5	2	121	$21-22$	56	22	$d_{best} = 27$
3	5	2	121	$23-25$	51	25	$d_{best} = 29$
3	5	2	121	26	46	26	$d_{best} = 33$
3	5	2	121	$27-31$	41	31	$d_{best} = 37$
3	5	2	121	$32-34$	36	34	$d_{best} = 42$
3	5	2	121	35	31	35	$d_{best} = 45$
3	5	2	121	$36-38$	26	38	$d_{best} = 49$
3	5	2	121	$39-40$	21	40	$d_{best} = 55$
4	4	3	85	2	81	2	$d_{optimal} = 3$
4	4	3	85	3	77	3	$d_{optimal} = 5$
4	4	3	85	$4-5$	73	5	$d_{best} = 6$
4	4	3	85	6	69	6	$d_{best} = 8$
4	4	3	85	7	65	7	$d_{best} = 9$
4	4	3	85	$8-9$	61	9	$d_{best} = 11$

5.5 BCH codes with designed distance $\delta = \frac{aq^{h+k}+b}{\lambda}$

As an illustration of our main results, this section presents the dimension and Bose distance of the BCH code $\mathcal{C}_{(q,n,\delta)}$ for $\delta = \frac{aq^{h+k}+b}{\lambda}$, where k, a and b are integers satisfying $m-2h \le k \le \lfloor (2m-1)/3 \rfloor - h$, $1 \le a \le q-1$, $\lambda \le b \le q^{m-h-k}$ and $q \nmid b$.

Corollary 5.3. *Let $m \ge 5$ be an odd integer and $k \in [1, \lfloor (2m-1)/3 \rfloor - h]$ be an integer. If $\lambda\delta = aq^{h+k} + b$ for some integers $a \in [1, q-1]$ and $b \in [\lambda, q^{h-k+1}]$ with $q \nmid b$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta, & \text{if } b > aq^{2k-1}, \\ \left\lfloor \frac{aq^{h+k}+aq^{2k-1}}{\lambda} \right\rfloor + 1, & \text{if } b \le aq^{2k-1} \end{cases} \tag{5.67}$$

and

$$\dim(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} n - mN(\delta) + \frac{q-1}{\lambda} ma^2 q^{2k-3} \left[(q-1)k+1\right], & \text{if } b \ge aq^{2k-1} + \lambda, \\ n - \frac{q-1}{\lambda} maq^{h+k-1} + \frac{q-1}{\lambda} maq^{2k-3} \left[a(q-1)k + a - q\right], & \text{if } b < aq^{2k-1} + \lambda. \end{cases} \tag{5.68}$$

Proof. Note that $q \nmid b$ implies that $q \nmid \lambda\delta$. Since λ is a factor $q-1$, it follows that $q \nmid \delta$. Then by applying Theorem 5.3, we can directly derive equation (5.67).

We now demonstrate that (5.68) holds. It is clear that $V(\lambda(\delta-1))$ has the form

$$(\mathbf{0}_{h-k}, a, \mathbf{0}_{2k-1}, \delta_{h-k}, \ldots, \delta_0)$$

with $\sum_{\ell=0}^{h-k} \delta_\ell q^\ell = b - \lambda$. By definition, it follows that

- $s_\delta = k_\delta = k$;
- $w_\delta = aq^{h+k}$;
- $\mu(\delta) = \min\left\{b - \lambda, aq^{2k-1}\right\}$;
- $\mathcal{T}_i(\delta) = \left[q^{k-i}, aq^{k-i}\right] \cap \{t \in \mathbb{Z} : q \nmid t\}$ for each integer $i \in [-k+1, k]$.

Then applying Lemma 5.6, we can obtain

$$\sum_{t\in\mathcal{T}_i(\delta)}\left[\left\lfloor\frac{\lfloor tq^{2i}\rfloor+t}{\lambda}\right\rfloor-\left\lfloor\frac{\lfloor tq^{2i-1}\rfloor+t}{\lambda}\right\rfloor\right]$$

$$=\begin{cases}\frac{1}{2\lambda}(a^2-1)(q-1)^2q^{2k-3}, & \text{if } i\in[-k+2,k-1],\\ \frac{1}{2\lambda}a(a-1)(q-1)q^{2k-2}, & \text{if } i=k \text{ or } -k+1.\end{cases}$$

It follows that

$$\sum_{i=-k_\delta+1}^{k_\delta}\sum_{t\in\mathcal{T}_i(\delta)}N(tq^{2i-1}+1)=\sum_{i=-k+1}^{k}\sum_{t\in\mathcal{T}_i(\delta)}N(tq^{2i-1}+1)$$

$$=\frac{1}{\lambda}\left[a(a-1)(q-1)q^{2k-2}+(a^2-1)(k-1)(q-1)^2q^{2k-3}\right].$$

By substituting the values of k_δ, $\mu(\delta)$ and the above expression into (5.22), we obtain

$$f(\delta)=\begin{cases}\frac{q-1}{\lambda}a^2q^{2k-3}\left[k(q-1)+1\right], & \text{if } b\geq aq^{2k-1}+\lambda,\\ \frac{q-1}{\lambda}aq^{2k-3}\left[ak(q-1)+a-q\right]+\frac{b+a-\lambda}{\lambda}-\left\lfloor\frac{\lfloor(b-\lambda+aq)/q\rfloor}{\lambda}\right\rfloor, & \text{if } b<aq^{2k-1}+\lambda.\end{cases}$$

Furthermore, notice that

$$N(\delta)-\left[\frac{b+a-\lambda}{\lambda}-\left\lfloor\frac{\lfloor(b-\lambda+aq)/q\rfloor}{\lambda}\right\rfloor\right]$$

$$=\frac{aq^{h+k}+b-\lambda}{\lambda}-\left\lfloor\frac{aq^{h+k}+b-\lambda}{\lambda q}\right\rfloor-\frac{b+a-\lambda}{\lambda}+\left\lfloor\frac{\lfloor(b-\lambda+aq)/q\rfloor}{\lambda}\right\rfloor$$

$$=\frac{aq^{h+k-1}(q-1)}{\lambda}-\left\lfloor\frac{aq+b-\lambda}{\lambda q}\right\rfloor+\left\lfloor\frac{\lfloor(b-\lambda+aq)/q\rfloor}{\lambda}\right\rfloor$$

$$=\frac{aq^{h+k-1}(q-1)}{\lambda}.$$

Therefore, we can apply Theorem 5.1 to derive the desired equality in (5.68). $\square$

Corollary 5.4. *Let $m\geq 4$ be an even intger and $0\leq k\leq\lfloor(2m-1)/3\rfloor-h$ be an integer. If $\lambda\delta=aq^{h+k}+b$ for some integers $a\in[1,q-1]$ and $b\in[\lambda,q^{h-k}]$ with $q\nmid b$.*

- *If $k=0$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta & \text{if } b \geq a, \\ \frac{aq^h+a}{\lambda}, & \text{if } b < a \text{ and } \lambda \mid 2a, \\ \left\lfloor \frac{aq^h+a}{\lambda} \right\rfloor + 1, & \text{if } b < a, \lambda \nmid 2a \text{ and } a+\lambda-q \neq 2a \bmod \lambda, \\ \left\lfloor \frac{aq^h+a}{\lambda} \right\rfloor + 2, & \text{if } b < a, \lambda \nmid 2a \text{ and } a+\lambda-q = 2a \bmod \lambda, \end{cases} \tag{5.69}$$

$$\dim(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} n-mN(\delta)+m\left[\frac{a+b-\lambda}{\lambda}-\left\lfloor\frac{2a}{\lambda}\right\rfloor+\sum_{t=1}^{a}\left[\left\lfloor\frac{2t}{\lambda}\right\rfloor-\left[\left\lfloor\frac{t}{\lambda}\right\rfloor\right]\right]\right]-\frac{m(a-1)\left(3+(-1)^{\lambda}\right)}{4\lambda}, \\ \qquad \text{if } b < a+\lambda, \\ n-mN(\delta)+m\sum_{t=1}^{a}\left[\left\lfloor\frac{2t}{\lambda}\right\rfloor-\left\lfloor\frac{t}{\lambda}\right\rfloor\right]-\frac{m(a-1)\left(3+(-1)^{\lambda}\right)}{4\lambda}, \\ \qquad \text{if } b \geq a+\lambda \text{ and } \lambda \nmid 2a, \\ n-mN(\delta)+m\sum_{t=1}^{a}\left[\left\lfloor\frac{2t}{\lambda}\right\rfloor-\left\lfloor\frac{t}{\lambda}\right\rfloor\right]-\frac{m(a-1)\left(3+(-1)^{\lambda}\right)}{4\lambda}-\frac{m}{2}, \\ \qquad \text{if } b \geq a+\lambda \text{ and } \lambda \mid 2a. \end{cases} \tag{5.70}$$

- *If $k \geq 1$, then*

$$d_B(\mathcal{C}_{(q,n,\delta)}) = \begin{cases} \delta & \text{if } b > aq^{2k}, \\ \left\lfloor \frac{aq^{h+k}+aq^{2k}}{\lambda} \right\rfloor + 1, & \text{if } b \leq aq^{2k} \text{ and } a+\lambda-q \neq 2a \bmod \lambda, \\ \left\lfloor \frac{aq^{h+k}+aq^{2k}}{\lambda} \right\rfloor + 2, & \text{if } b \leq aq^{2k} \text{ and } a+\lambda-q = 2a \bmod \lambda, \end{cases} \tag{5.71}$$

$$\dim(\mathcal{C}_{(q,n,\delta)})$$

$$= \begin{cases} n - mN(\delta) + m\frac{q-1}{\lambda}a^2q^{2k-2}\left[\left(k-\frac{1}{2}\right)(q-1)+q\right], \\ \qquad \textit{if } b > aq^{2k}+\lambda \textit{ and } \lambda \textit{ is odd,} \\ n - mN(\delta) + m\frac{q-1}{\lambda}a^2q^{2k-2}\left[\left(k-\frac{1}{2}\right)(q-1)+q\right] - \frac{m(q-1)(q^{k-1}-1)}{2\lambda}, \\ \qquad \textit{if } b > aq^{2k}+\lambda \textit{ and } \lambda \textit{ is even,} \\ n + m\frac{q-1}{\lambda}aq^{2k-2}\left[a(k-\frac{1}{2})(q-1)+(a-1)q\right] - \frac{maq^{h+k-1}(q-1)}{\lambda}, \\ \qquad \textit{if } b \le aq^{2k}+\lambda \textit{ and } \lambda \textit{ is odd,} \\ n + m\frac{q-1}{\lambda}aq^{2k-2}\left[a(k-\frac{1}{2})(q-1)+(a-1)q\right] \\ -\frac{maq^{h+k-1}(q-1)}{\lambda} - \frac{m(q-1)(q^{k-1}-1)}{2\lambda}, \\ \qquad \textit{if } b \le aq^{2k}+\lambda \textit{ and } \lambda \textit{ is even.} \end{cases} \tag{5.72}$$

Proof. By Theorem 5.4, it is easy to conclude that the(5.69) holds if $k = 0$, and (5.71) holds if $k \geq 1$. Therefore, we only demonstrate that (5.70) and (5.72)hold.

If $k = 0$, then we have $\lambda(\delta - 1) = aq^h + b - \lambda$ with $0 \leq b - \lambda < q^{h-1}$. It follows that

- $\frac{q^h-1}{\lambda} + 1 < \delta \leq \frac{q^{h+1}-1}{\lambda} + 1$;
- $\delta_h = a$;
- $\widetilde{\mu}(\delta) = \min\{b - \lambda, a\}$;
- $w_\delta = aq^h$;
- $\tau(\delta) = 1$ if $a \leq b - \lambda$ and $\lambda \mid 2a$, and $\tau(\delta) = 0$ if otherwise.

By substituting the above values for the corresponding case into equations (5.23) and (5.25), we derive

$$\widetilde{f}(\delta) = \begin{cases} \frac{a+b-\lambda}{\lambda} - \left\lfloor \frac{2a}{\lambda} \right\rfloor + \sum\limits_{t=1}^{a} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor\right], & \text{if } b < a + \lambda, \\ \sum\limits_{t=1}^{a} \left[\left\lfloor \frac{2t}{\lambda} \right\rfloor - \left\lfloor \frac{t}{\lambda} \right\rfloor\right], & \text{if } b \geq a + \lambda, \end{cases}$$

and

$$g(\delta) = \begin{cases} \frac{(a-1)(3+(-1)^{\lambda})}{2\lambda} + 1, & \text{if } b \geq a+\lambda \text{ and } \lambda \mid 2a, \\ \frac{(a-1)(3+(-1)^{\lambda})}{2\lambda}, & \text{otherwise.} \end{cases}$$

Then by Theorem 5.1, it follows that (5.70) holds.

If $k \geq 1$, then we have $k_\delta = k$ and $V(\lambda(\delta-1))$ has the form

$$(\mathbf{0}_{h-k-1}, a, \mathbf{0}_{2k}, \delta_{h-k-1}, \ldots, \delta_0)$$

with $\sum_{\ell=0}^{h-k} \delta_\ell q^\ell = b - \lambda$. By definition, it follows that

- $w_\delta = aq^h$;
- $s_\delta = k_\delta = k$;
- $\tau(\delta) = 0$;
- $\widetilde{\mu}(\delta) = \min\left\{b-\lambda, aq^{2k}\right\}$;
- $\phi(\delta) = aq^k - 1$
- $\mathcal{T}_i(\delta) = \left[q^{k-i}, aq^{k-i}-1\right] \cap \{t \in \mathbb{Z} : q \nmid t\}$ for each integer $i \in [-k, k]$.

Then applying Lemmas 5.7 and 5.6, we obtain

$$\sum_{t \in \mathcal{T}_i(\delta)} \left[\left\lfloor \frac{\lfloor tq^{2i} \rfloor + t}{\lambda} \right\rfloor - \left\lfloor \frac{\lfloor tq^{2i-1} \rfloor + t}{\lambda} \right\rfloor\right]$$

$$= \begin{cases} \frac{1}{2\lambda}(a^2-1)(q-1)^2 q^{2k-2}, & \text{if } i \in [-k+1, k-1] \setminus \{0\}, \\ \frac{1}{2\lambda} a(a-1)(q-1)q^{2k-1}, & \text{if } i = k \text{ or } -k \\ \begin{pmatrix} \frac{1}{2\lambda}(a^2-1)(q-1)^2 q^{2k-2} \\ + \frac{(3+(-1)^{\lambda})}{4\lambda}(a-1)(q-1)q^{k-1} \end{pmatrix}, & \text{if } i = 0. \end{cases}$$

It follows that

$$
\begin{aligned}
&\sum_{i=-k_\delta}^{k_\delta}\sum_{t\in\mathcal{T}_i(\delta)}\left[\left\lfloor\frac{\lfloor tq^{2i}\rfloor+t}{\lambda}\right\rfloor-\left\lfloor\frac{\lfloor tq^{2i-1}\rfloor+t}{\lambda}\right\rfloor\right]\\
=&\frac{1}{\lambda}(k-\frac{1}{2})(a^2-1)(q-1)^2q^{2k-2}+\frac{1}{\lambda}a(a-1)(q-1)q^{2k-1}\\
&+\frac{(3+(-1)^\lambda)(a-1)q^{k-1}(q-1)}{4\lambda}.
\end{aligned}
$$

By substituting the values of k_δ, $\tau(\delta)$ w_δ, $\widetilde{\mu}(\delta)$, $\phi(\delta)$ and the above expression into (5.23) and (5.25), we obtain

$$
\widetilde{f}(\delta)=\begin{cases}
\frac{q-1}{\lambda}a^2q^{2k-2}\left[\left(k-\frac{1}{2}\right)(q-1)+q\right]+\frac{q-1}{2\lambda}aq^{k-1}, \\
\qquad \text{if } b>aq^{2k}+\lambda \text{ and } \lambda \text{ is odd,}\\
\frac{q-1}{\lambda}a^2q^{2k-2}\left[\left(k-\frac{1}{2}\right)(q-1)+q\right]+\frac{q-1}{2\lambda}\left[(2a-1)q^{k-1}+1\right], \\
\qquad \text{if } b>aq^{2k}+\lambda \text{ and } \lambda \text{ is even,}\\
\begin{pmatrix}\frac{q-1}{\lambda}aq^{2k-2}\left[a(k-\frac{1}{2})(q-1)+(a-1)q\right]\\ +\frac{q-1}{2\lambda}aq^{k-1}+\frac{a+b-\lambda}{\lambda}-\left\lfloor\frac{\lfloor(a+bq-\lambda)/q\rfloor}{\lambda}\right\rfloor\end{pmatrix}, \\
\qquad \text{if } b\le aq^{2k}+\lambda \text{ and } \lambda \text{ is odd,}\\
\begin{pmatrix}\frac{q-1}{\lambda}aq^{2k-2}\left[a(k-\frac{1}{2})(q-1)+(a-1)q\right]+\frac{a+b-\lambda}{\lambda}\\ +\frac{q-1}{2\lambda}\left[(2a-1)q^{k-1}+1\right]-\left\lfloor\frac{\lfloor(a+bq-\lambda)/q\rfloor}{\lambda}\right\rfloor\end{pmatrix}, \\
\qquad \text{if } b\le aq^{2k}+\lambda \text{ and } \lambda \text{ is even,}
\end{cases}
$$

and

$$
g(\delta)=\begin{cases}\frac{a(q-1)q^{k-1}}{\lambda}, & \text{if } \lambda \text{ is odd,}\\ \frac{2a(q-1)q^{k-1}}{\lambda}, & \text{if } \lambda \text{ is even.}\end{cases}
$$

By Theorem 5.1, it follows that (5.72) holds. □

5.6 Some non-narrow-sense BCH codes

In this section, we determine the Bose distance and dimension of certain non-narrow-sense BCH codes $\mathcal{C}_{(q,n,\delta,b)}$.

Theorem 5.5. *Let $m \geq 4$ and b be two integers with $\frac{q^{m-h}-1}{\lambda}+1 \leq b < \frac{q^{\lfloor (2m-1)/3 \rfloor +1}-1}{\lambda}$. Let $j_\delta = \lfloor \log_q(\lambda\delta) \rfloor - h$, let $\sum_{\ell=0}^{h+j_b} b_\ell q^\ell$ be the q-adic expansion of λb, and let r_b be the smallest integer in $[m-2h-j_b, j_b]$ such that $b_{h+r_b} > 0$. If $\sum_{\ell=0}^{h-j_b-1} b_\ell q^\ell > \sum_{\ell=h-r_b}^{h+j_b} b_\ell q^{\ell-(h-r_b)}$, then*

$$\dim(\mathcal{C}_{(q,n,\delta,b)}) = n - m(\delta - 1) \tag{5.73}$$

and

$$d_B(\mathcal{C}_{(q,n,\delta,b)}) = \delta \tag{5.74}$$

for any integer δ such that $2 \leq \delta \leq \frac{q^{h-j_b}-1}{\lambda} - \left\lfloor \frac{\sum_{\ell=0}^{h-j_b-1} b_\ell q^\ell}{\lambda} \right\rfloor + 1$.

Proof. We demonstrate the proof only for the case where m is even, as the case m is odd follows similarly. First, observe that

$$V\left(\sum_{\ell=h+r_b}^{h+j_b} b_\ell q^\ell + q^{h-j_b} - 1\right) = (\mathbf{0}_{h-1-j_b}, b_{h+j_b}, \ldots, b_{h+r_b}, \mathbf{0}_{2r_b}, q-1, \ldots, q-1),$$

and

$$V(\lambda b) \leq V(\lambda a) \leq V\left(\sum_{\ell=h+r_b}^{h+j_b} b_\ell q^\ell + q^{h-j_b} - 1\right)$$

for all integers $a \in \left[b, b + \frac{q^{h-j_b}-1}{\lambda} - \lceil \frac{\sum_{\ell=0}^{h-j_b-1} b_\ell q^\ell}{\lambda} \rceil \right]$. Since $\sum_{\ell=0}^{h-j_b-1} b_\ell q^\ell > \sum_{\ell=h-r_b}^{h+j_b} b_\ell q^{\ell-(h-r_b)}$, it follows that $V(\lambda a)$ must have the form

$$V(\lambda a) = (\mathbf{0}_{h-1-j_b}, b_{h+j_b}, \ldots, b_{h+r_b}, \mathbf{0}_{2r_b}, a_{h-j_b-1}, \ldots, a_0) \tag{5.75}$$

with $\sum_{\ell=0}^{h-j_b-1} a_\ell q^\ell > \sum_{\ell=h-r_b}^{h+j_b} b_\ell q^{\ell-(h-r_b)}$ for all integers $a \in \left[b, b + \frac{q^{h-j_b}-1}{\lambda} - \left\lfloor \frac{\sum_{\ell=0}^{h-j_b-1} b_\ell q^\ell}{\lambda} \right\rfloor \right]$.

Next, we define a function f for the integers in $\left[b, b+\frac{q^{h-j_b-1}}{\lambda}-\left\lfloor\frac{\sum_{\ell=0}^{h-j_b-1} b_\ell q^\ell}{\lambda}\right\rfloor\right]$ as

$$f(a)=\frac{a}{q^{t_a}},$$

where t_a is largest integer such that $q^{t_a} \mid a$. We now show that

$$f(a) \in \mathcal{L}_m^n \quad \text{for all } a \in \left[b, b+\frac{q^{h-j_b}-1}{\lambda}-\left\lfloor\frac{\sum_{\ell=0}^{h-j_b-1} b_\ell q^\ell}{\lambda}\right\rfloor\right] \tag{5.76}$$

by considering the following cases.

Case 1. Suppose that $t_a=0$, i.e., $q \nmid a$. Then $f(a)=a$. It follows that $V(\lambda f(a))$ has the form given in (5.75). By Remarks 3.4 and 3.5, this implies that $\lambda f(a) \notin \mathcal{B}_{j_b}(i)$ for any $i \in [-j_b, j_b]$. Applying Theorem 3.2, we conclude that $\lambda f(a) \notin \mathcal{H} \cup \mathcal{S}$. Therefore, $\lambda f(a) \in \mathcal{L}_m^{\lambda n}$. By Lemma 3.2, this implies that $f(a) \in \mathcal{L}_m^n$.

Case 2. Suppose that $1 \leq t_a \leq j_b$. In this case, we first have $f(a) \leq b-1$. Since $V(\lambda a)$ has the form given in (5.75), we derive

$$V(\lambda f(a))=(\mathbf{0}_{h-1-j_b+t_a}, b_{h+j_b}, \ldots, b_{h+r_b}, \mathbf{0}_{2r_b}, a_{h-j_b-1}, \ldots, a_{t_a}).$$

Furthermore, the inequality $\sum_{\ell=0}^{h-j_b-1} a_\ell q^\ell > \sum_{\ell=h-r_b}^{h+j_b} b_\ell q^{\ell-(h-r_b)}$ implies that $a_{j_b+r_b}>0$. It follows that $\lambda f(a) \notin \mathcal{B}_{j_b-t_a}(i)$ for any $i \in [t_a-j_b, j_b-t_a]$, and hence $\lambda f(a) \notin \mathcal{H} \cup \mathcal{S}$. This implies that $\lambda f(a) \in \mathcal{L}_m^{\lambda n}$, and hence $f(a) \in \mathcal{L}_m^n$.

Case 3. Suppose $t_a \geq j_b+1$. In this case, we have $\lambda f(a)<q^h$ and $\lambda f(a) q^h \bmod \lambda n \neq \lambda f(a)$. By Lemma 3.1, we have $|C_{\lambda n}(\lambda f(a))|=m$. Moreover, by applying [57, Theorem 2.3], we conclude that $\lambda f(a)$ is a coset leader modulo λn. It follows that $f(a) \in \mathcal{L}_m^n$.

By now we have demonstrated that (5.76) holds. Noticing that $C_n(a) = C_n(f(a))$ and f is injective, it follows that

$$\left| \bigcup_{a=b}^{b+\delta-2} C_n(a) \right| = \left| \bigcup_{a=b}^{b+\delta-2} C_n(f(a)) \right| = \sum_{a=b}^{b+\delta-2} |C_n(f(a))| = m(\delta-1)$$

and

$$\bigcup_{a=b}^{b+\delta-2} C_n(a) = \bigcup_{a=b}^{b+\delta-2} C_n(f(a)) \neq \bigcup_{a=b}^{b+\delta-1} C_n(f(a)) = \bigcup_{a=b}^{b+\delta-1} C_n(a)$$

for any integer δ such that $2 \leq \delta \leq \frac{q^{h-j_b}-1}{\lambda} - \left\lfloor \frac{\sum_{\ell=0}^{h-j_b-1} b_\ell q^\ell}{\lambda} \right\rfloor + 1$. Therefore, both (5.73) and (5.74) hold. □

Example 5.1. *Applying the above theorem, we find the following optimal BCH codes.*

- *Let* $q = 3$, $m = 4$ *and* $\lambda = 1$. *We have* $n = 80$. *The BCH code* $\mathcal{C}_{(3,80,2,b)}$ *has parameters* $[80, 76, 2]$ *for all integers* $b \in [11, 17] \cup [21, 25]$.
- *Let* $q = 4$, $m = 4$ *and* $\lambda = 1$. *We have* $n = 255$. *The BCH code* $\mathcal{C}_{(4,255,2,b)}$ *has parameters* $[255, 251, 2]$ *for all integers* $b \in [18, 30] \cup [35, 46] \cup [52, 62]$.

Chapter 6

Conclusion and future directions

This thesis has presented a study on the dimension and Bose distance of BCH codes of length $\frac{q^m-1}{\lambda}$, where q is a prime power, m is a positive integer, and λ is a divisor of $q-1$. This family includes primitive BCH codes as a special case.

A central contribution of this work is the establishment of explicit formulas for both the dimension and Bose distance of some narrow-sense primitive and non-narrow-sense BCH codes, covering designed distances over a significantly wider range than previously known.

Our results rely critically on the analysis of the distribution of coset leaders modulo q^m-1 in the interval $\left[1, q^{\lfloor (2m-1)/3 \rfloor +1}\right]$. By utilizing a one-to-one, order-preserving map between integers in $[0, q^m-2]$ and sequences of length m over non-negative integers less than q, we partition integers that are neither divisible by q nor coset leaders within $\left[q^{h+k}, q^{h+k+1}\right)$ into distinct classes with uniform representations for $m-2h \le k \le \lfloor \frac{2m-1}{3} \rfloor - h$. This classification enables a systematic computation of the number of such integers in each class.

Furthermore, we divide the interval $[1, \delta-1]$ into subintervals according to the distribution of coset leaders. This allows us to formulate an equation expressing the number of integers that are neither divisible by q nor coset leaders in each subinterval. As a result, we derive the exact count of coset leaders in $[1, \delta-1]$ for every integer

$\delta \in \left[2, q^{\lfloor (2m-1)/3 \rfloor + 1}\right]$. Combined with our results on the sizes of q-cyclotomic cosets, we ultimately determine the dimension of the primitive BCH codes $\mathcal{C}_{(q,n,\delta)}$ for all $\delta \in \left[2, q^{\lfloor (2m-1)/3 \rfloor + 1}\right]$.

Additionally, we show that the Bose distance of $\mathcal{C}_{(q,n,\delta)}$ is equal to the smallest integer not less than δ. Thus, based on our analysis of the distribution of coset leaders, the Bose distance of narrow-sense primitive BCH codes can be efficiently determined.

In extending these results to BCH codes of length $\frac{q^m-1}{\lambda}$, we observe that the coset leaders modulo $\frac{q^m-1}{\lambda}$ are exactly those coset leaders modulo q^m-1 that are divisible by λ. Leveraging this observation and our prior analysis of coset leader modulo q^m-1, we successfully obtain the dimension and Bose distance for this broader class of codes.

Several promising directions for future research emerge from this work:

- Although our results significantly extend the known range of designed distances for which the dimension and Bose distance are determined, the problem remains far from fully solved. Further improvements may require new technical insights or novel discoveries regarding the distribution of coset leaders.

- A natural next step is to pursue the true minimum distance of these codes, going beyond the Bose distance lower bound. This remains a challenging open problem.

- The techniques and results on cyclotomic cosets, particularly those concerning the distribution and properties of coset leaders established in this thesis, could be adapted and applied to BCH codes with other lengths, such as antiprimitive BCH codes, potentially enabling broader generalizations.

In summary, this work provides a substantial advancement in the understanding of the parameters of BCH codes and establishes a foundation for further theoretical investigations and practical applications in BCH codes.

Bibliography

[1] Salah A. Aly, A. Klappenecker, and P. K. Sarvepalli, "On quantum and classical BCH codes," *IEEE Trans. Inf. Theory*, vol. 53, no. 3, pp. 1183–1188, Mar. 2007.

[2] E. Arikan, "Channel polarization: A method for constructing capacity-achieving codes for symmetric binary-input memoryless channels,"*IEEE Trans. Inf. Theory*, vol. 55, no. 7, pp. 3051 – 3073, July 2009.

[3] D. Augot, P. Charpin, and N. Sendrier, "Studying the locator polynomials of minimum weight codewords of BCH codes," *IEEE Trans. Inf. Theory*, vol. 38, no. 3, pp. 960–973, May 1992.

[4] D. Augot and N. Sendrier, "Idempotents and the BCH bound," *IEEE Trans. Inf. Theory*, vol. 40, no. 1, pp. 204–207, Jan. 1994.

[5] E. R. Berlekamp, "The enumeration of information symbols in BCH codes," *Bell System Tech. J.*, vol. 46, no. 8, pp. 1861–1880, May 1967.

[6] E. R. Berlekamp, "Binary BCH codes for correcting multiple errors," *Algebraic Coding Theory*, New York: McGraw-Hill, 1968.

[7] C. Berrou, A. Glavieux, and P. Thitimajshima, "Near Shannon limit error-correcting coding and decoding: Turbo-codes. 1", *Proceedings of ICC'93-IEEE International Conference on Communications* Vol. 2, pp. 1064-1070, May 1993.

[8] A. Betten, M. Braun, H. Fripertinger, A. Kerber, A. Kohnert, and A. Wassermann, *Error-Correcting Linear Codes: Classification by Isometry and Applications*, Berlin, Germany: Springer-Verlag, 2006.

[9] R. C. Bose and D. K. Ray-Chaudhuri, "Further results on error correcting binary group codes," *Inf. Control*, vol. 3, no. 3, pp. 279–290, Sep. 1960.

[10] R. C. Bose and D. K. Ray-Chaudhuri, "On a class of error correcting binary group codes," *Inf. Control*, vol. 3, no. 1, pp. 68–79, Mar. 1960.

[11] C. Carlet and S. Guilley, "Complementary dual codes for counter-measures to side-channel attacks," *Adv. Math. Commun.*, vol. 10, no. 1, pp. 131–150, Feb. 2016.

[12] P. Charpin, "Weight distributions of cosets of two-error-correcting binary BCH codes, extended or not," *IEEE Trans. Inf. Theory*, vol. 40, no. 5, pp. 1425–1442, Sep. 1994.

[13] P. Charpin, T. Helleseth, and V. A. Zinoviev, "The coset distribution of triple-error-correcting binary primitive BCH codes," *IEEE Trans. Inf. Theory*, vol. 52, no. 4, pp. 1727–1732, Apr. 2006.

[14] P. Charpin, "Open problems on cyclic codes," in *Handbook Coding Theory*, vol. 1, V. Pless and W. C. Huffman, Eds. Amsterdam, The Netherlands: Elsevier, 1998, ch. 11, pp. 963–1063.

[15] A. Cherchem, A. Jamous, H. Liu, and Y. Maouche, "Some new results on dimension and Bose distance for various classes of BCH codes," *Finite Fields Appl.*, vol. 65, p. 101673, Aug. 2020.

[16] Y. Desaki, T. Fujiwara, and T. Kasami, "The weight distributions of extended binary primitive BCH codes of length 128," *IEEE Trans. Inf. Theory*, vol. 43, no. 4, pp.1364–1371, July 1997.

[17] C. Ding, "Parameters of several classes of BCH codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 10, pp. 5322–5330, Oct. 2015.

[18] C. Ding, X. Du, and Z. Zhou, "The Bose and minimum distance of a class of BCH codes," *IEEE Trans. Inf. Theory*, vol. 61, no. 5, pp. 2351–2356, May 2015.

[19] C. Ding, C. Fan, and Z. Zhou, "The dimension and minimum distance of two classes of primitive BCH codes," *Finite Fields Appl.*, vol. 45, pp. 237–263, May 2017.

[20] C. Ding and C. Li, "BCH cyclic codes," *Discrete Math.*, vol. 347, no. 5, 113918, May 2024.

[21] S. Dong, C. Li, S. Mesnager, and H. Qian, "Parameters of squares of primitive narrow-sense BCH codes and their complements,"*IEEE Trans. Inf. Theory*, vol. 69, no. 8, pp. 5017–5031, Aug. 2023.

[22] M. Fan, C. Li, and C. Ding, "The Hermitian dual codes of several classes of BCH codes," *IEEE Trans. Inf. Theory*, vol. 69, no. 7, pp. 4484–4497, July 2023.

[23] T. Fujiwara, T. Takata, T. Kasami, and S. Lin, "An approximation to the weight distribution of binary primitive BCH codes with designed distances 9 and 11 (corresp.)," *IEEE Trans. Inf. Theory*, vol. 32, no. 5, pp. 706–709, Sep. 1986.

[24] C. Gan, C. Li, H. Qian, and X. Shi, "On Bose distance of a class of BCH codes with two types of designed distances," *Des. Codes Cryptogr.*, vol. 92, pp. 2031–2053, Mar. 2024.

[25] D. Gorenstein and N. Zierler, "A class of error-correcting codes in p^m symbols," *J. Soc. Indust. Appl. Math.*, vol. 9, no. 2, pp. 207–214, June 1961.

[26] R. Hamming, "Error detecting and error correcting codes," *Bell Syst. Tech. J.,* vol. 29, no. 2, pp. 147 –160, Apr. 1950.

[27] H. Helgert and R. Stinaff, "Shortened bch codes (corresp.)," *IEEE Trans. Inf. Theory*, vol. 19, no. 6, pp. 818–820, Nov. 1973.

[28] A. Hocquenghem, "Codes correcteurs d'erreurs," *Chiffers*, vol. 2, pp. 147–156, 1959.

[29] X. Hou, *Lectures on finite fields* (Graduate Studies in Mathematics), vol. 190. Providence, RI, USA: American Mathematical Society, 2018.

[30] T. Kasami, T. Fujiwara, and S. Lin, "An approximation to the weight distribution of binary linear codes," *IEEE Trans. Inf. Theory*, vol. 31, no. 6, pp. 769–780, Nov. 1985.

[31] T. Kasami and S. Lin, "Some results on the minimum weight of primitive BCH codes (corresp.)," *IEEE Trans. Inf. Theory*, vol. 18, no. 6, pp. 824–825, Nov. 1972.

[32] O. Keren and S. Litsyn, "More on the distance distribution of BCH codes," *IEEE Trans. Inf. Theory*, vol. 45, no. 1, pp. 251–255, Jan. 1999.

[33] I. Krasikov and S. Litsyn, "On the distance distributions of BCH codes and their duals," *Des. Codes Cryptogr.*, vol. 23, pp. 223–232, July 2001.

[34] C. Li, C. Ding, and S. Li, "LCD cyclic codes over finite fields," *IEEE Trans. Inf. Theory*, vol. 63, no. 7, pp. 4344–4356, July 2017.

[35] S. Li, C. Li, C. Ding, and H. Liu, "Two families of LCD BCH codes," *IEEE Trans. Inf. Theory*, vol. 63, no. 9, pp. 5699–5717, Sep. 2017.

[36] C. Li, P. Wu, and F. Liu, "On two classes of primitive BCH codes and some related codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 6, pp. 3830–3840, June 2018.

[37] S. Ling and C. Xing, *Coding theory: a first course*, Cambridge University Press, 2004.

[38] X. Ling, S. Mesnager, Y. Qi, and C. Tang," A class of narrow-sense BCH codes over $\mathbb{F}_q$ of length $\frac{q^m-1}{2}$", *Designs, Codes and Cryptography*, vol. 88, no. 2, pp. 413–427, Nov. 2020.

[39] H. Liu, C. Ding, and C. Li, "Dimensions of three types of BCH codes over GF(q)," *Discrete Math.*, vol. 340, no. 8, pp. 1910–1927, Aug. 2017.

[40] Y. Liu, R. Li, Q. Fu, L. Lu, and Y. Rao, "Some binary BCH codes with length $n = 2^m + 1$," *Finite Fields Appl.*, vol. 55, pp. 109–133, Jan. 2019.

[41] F. J. MacWilliams and N. J. A. Sloane, *The Theory of Error-correcting Codes,* (North-Holland Mathematical Library). Amsterdam, The Netherlands: North-Holland, 1977.

[42] H. B. Mann, "On the number of information symbols in Bose-Chaudhuri codes," *Inf. Control.*, vol. 5, no. 2, pp. 153–162, June 1962.

[43] J. Massey, "Shift-register synthesis and BCH decoding," *IEEE Trans. Inf. Theory*, vol. 15, no. 1, pp. 122–127, Jan. 1969.

[44] E. M. Mouloua and M. Najmeddine, "On the parameters of a class of narrow sense primitive BCH codes," *J. Algebra Comb. Discrete Struct. Appl.*, pp. 149–159, Aug. 2023.

[45] S. Noguchi, X.-N. Lu, M. Jimbo, and Y. Miao, "BCH codes with minimum distance proportional to code length," *SIAM J. Discrete Math.*, vol. 35, no. 1, pp. 179–193, Feb. 2021.

[46] B. Pang, S. Zhu, and X. Kai, "Five families of the narrow-sense primitive BCH codes over finite fields," *Designs, Codes and Cryptography*, vol. 89, pp. 2679–2696, Oct. 2021.

[47] W. Peterson, "Encoding and error-correction procedures for the Bose-Chaudhuri codes," *IRE Transactions on information theory*, vol. 6, no. 4, pp. 459–470, Sep. 1960.

[48] W. Peterson, “Some new results on finite fields with applications to BCH codes, ” *Combinatorial Mathematics and Its Applications,* R. C. Bose and T. A. Dowling, Eds. Chapel Hill, NC, USA: Univ. North Carolina Press, 1969, ch. 9

[49] I. S. Reed and G. Solomon, “Polynomial codes over certain finite fields, ” *J. Soc. Ind. Appl. Math.,* vol. 8, no. 2, pp. 300–304, 1960.

[50] R. Schoof and M. Van Der Vlugt, “Hecke operators and the weight distributions of certain codes,” *J. Combinatorial Theory Ser. A*, vol. 57, no. 2, pp. 163–186, Jul. 1991.

[51] Z. Sun,“The Exact Parameters of A Family of BCH Codes.” arXiv preprint arXiv:2507.15247, 2025.

[52] Z. Sun, C. Li, and C. Ding, “An infinite family of binary cyclic codes with best parameters,” *IEEE Trans. Inf. Theory*, vol. 70, no. 4, pp. 2411 – 2418, Apr. 2023.

[53] L. Wang, D. Lu and S. Zhu “Parameters of some BCH codes over $\mathbb{F}_q$ of length $\frac{q^m-1}{2}$,”*Advances in Mathematics of Communications,* vol. 18, no. 8, pp. 1559 – 1574, Dec. 2024.

[54] X. Wang, J. Wang, C. Li, and Y. Wu, “Two classes of narrow-sense BCH codes and their duals,” *IEEE Trans. Inf. Theory*, vol. 70, no. 1, pp. 131– 144, Jan. 2023.

[55] X. Wang, C. Xiao, and D. Zheng, “The duals of narrow-sense BCH codes with length $q^m - 1/\lambda$,” *IEEE Trans. Inf. Theory*, vol. 70, no. 11, pp. 7777 – 7789, Nov. 2024.

[56] R. Xu and C. Li, “Products of some primitive BCH codes and their complements,” *IEEE Trans. Inf. Theory*, vol. 70, no. 12, pp. 8546 – 8561, Dec. 2024.

[57] D. W. Yue and G. Z. Feng, “Minimum cyclotomic coset representatives and their applications to BCH codes and Goppa codes,” *IEEE Trans. Inf. Theory*, vol. 46, no. 7, pp. 2625–2628, Nov. 2000.

[58] D. W. Yue and Z. M. Hu, “On the dimension and minimum distance of BCH codes over GF(q), ” *Journal of Electronics (China),* vol. 13, no. 3, pp. 216 – 221, July 1996.

[59] J. Zhang, X. Kai, and P. Li, “Some results on the dimension and Bose distance of the antiprimitive BCH codes,” *Discrete Math.*, vol. 347, no. 10, 114104, Oct. 2024.

[60] S. Zhu, Z. Sun, and X. Kai, "A class of narrow-sense BCH codes," *IEEE Trans. Inf. Theory*, vol. 65, no. 8, pp. 4699–4714, Aug. 2019.