On Codes for Multimedia Fingerprinting: Traceability, Bounds, and Constructions

Graduate School of Systems and Information Engineering

University of Tsukuba

March 2015

Jing Jiang

ON CODES FOR MULTIMEDIA FINGERPRINTING: TRACEABILITY, BOUNDS, AND CONSTRUCTIONS

Jing Jiang
University of Tsukuba, 2015

Advisor: Ying Miao

Anti-collusion codes can be used to construct fingerprints resistant to collusion attacks on multimedia contents, and colluder tracing algorithms can be used to identify or trace the sources of pirate copies of copyrighted multimedia contents. Cheng and Miao [17] introduced the notion of an anti-collusion code called separable code ($\bar{t}$-SC) against the averaging collusion attack on multimedia content, and designed colluder tracing algorithm based on such codes to identify colluders. However, the power of such codes is limited by some constraints, such as the maximum size of the code and the computational complexity of the tracing algorithm based on such a code.

This thesis introduces three new types of anti-collusion codes, called strong separable code ($\bar{t}$-SSC), multimedia identifiable parent property code (t-MIPPC), strong multimedia identifiable parent property code (t-SMIPPC), to resist the averaging collusion attack on multimedia content. We then design the colluder tracing algorithms based on these new codes.

	Catch Colluders	Complexity
Binary $\bar{t}$-SC ([17])	all	$O(nM^t)$
Binary $\bar{t}$-SSC	all	$O(nM)$
Binary t-MIPPC	at least one	$O(nM^t)$
Binary t-SMIPPC	at least one	$O(nM)$

The above table describes the traceability of the four types of codes described in this thesis including separable codes and our three newly introduced codes. For example, any binary $\bar{t}$-SC can be used to identify all colluders with computational complexity $O(nM^t)$ when the number of colluders in the averaging collusion attack is at most t, where n is the length of the code and M is the number of authorized users. In addition, an important point which is not revealed in the table is that the maximum number of the codewords of a t-MIPPC (or a t-SMIPPC, respectively) is more than that of a $\bar{t}$-SC (or a $\bar{t}$-SSC, respectively).

From the above results, we know that these four types of codes can be used in different scenarios where requirements are different. In this thesis, we also construct these four types of codes via Combinatorics, Graph Theory, and Finite Geometries such as generalized packings, bipartite graphs, projective planes, generalized quadrangles, and difference matrices. Furthermore, by investigating the upper bounds on the size of these codes, we show that some of the codes constructed in this thesis are optimal.

ACKNOWLEDGMENTS

First of all, I would like to thank my supervisor Prof. Ying Miao for his endless patience in giving me professional advices on multimedia fingerprinting and writing this thesis. I am grateful for his support and all I have learned from him during my studies at University of Tsukuba.

I am thankful to Prof. Ryoh Fuji-Hara and Prof. Masahiro Hachimori, who served as the members of my advisory group, for their careful reading and useful comments to improve the readability of this thesis.

I would like to thank Prof. Kazuo Kishimoto, Prof. Hiroyasu Ando, Prof. Hiroki Koga and Prof. Masanori Sawa, for serving as my committee menbers. I also want to thank them for their brilliant comments and suggestions.

I would also like to thank Prof. Dianhua Wu. He had introduced me to the field of combinatorics in my master's course. I am grateful for his kind advices not only on my study but also on my private life.

I would like to give special thanks to Prof. Hung-Lin Fu and Dr. Yuan-Hsun Lo for their knowledge and fruitful discussions about bipartite graphs, the main tool used in Section 2.2. I have learned a lot through joint works with them.

I would further like to thank Dr. Minquan Cheng with whom I've had useful discussions on topics related to this thesis. I also thank him for his helpful advices on both of my study and private life. I would like to thank Dr. Xun Wang and all our laboratory members.

Finally, I wish to express my gratitude to my mother Lianxi Gong, my wife Fanhua, and her family for their warm supports. Their love, support and patience were basic source of my encouragement for living and studying in Japan. I could not have completed this work without their hearty encouragement.

Contents

Chapter 1

Introduction

Multimedia contents, such as video, audio, image, can be copied and distributed easily, especially in the Internet age. This damages the interests of copyright owners and distributors. It is desired to devise techniques for copyright protection of multimedia contents.

Cryptographic approaches are such techniques to ensure that only authorized users are able to use copyrighted contents. Unfortunately, cryptographic approaches are limited in that once the content is decrypted, it can potentially be copied and redistributed freely. Fingerprinting techniques which by providing unique identification of data in a certain manner can be used to fight against illegal redistribution of copyrighted contents.

The main purpose of this thesis is to construct anti-collusion codes and discuss their tracing algorithms for multimedia fingerprinting.

1.1 Related work

Similar to human fingerprints, which are unique and can be used to identify their owner in the case of a criminal act, multimedia fingerprints uniquely identify a piece of multimedia data and allow the content to be traced to their rightful owner. If a naive purchaser redistributed his copy illegally, the fingerprint embedded in that copy will allow the distributor to identify the malicious user and proceed with an appropriate legal action. Hence, any authorized user would not like to sent his/her decrypted content to any unauthorized user. So, nowadays ensuring the appropriate use of multimedia content is no longer a traditional security issue with a single adversary. The global nature of the Internet has also brought adversaries closer to each other, and it is easy for a group of authorized users with differently marked versions of the same content to mount attacks against the fingerprints. These attacks, which are known as collusion attacks, can provide a cost-effective approach for attenuating each of the colluders' fingerprints. An improperly designed embedding and identification scheme may be vulnerable in the sense that a small coalition of colluders can successfully produce a new version of the content with no detectable traces. It is desirable, therefore, to design fingerprints that can resist collusion and identify the colluders, thereby discouraging attempts at collusion by the authorized users.

The problem of designing fingerprints that can withstand collusion and allow for the identification of colluders has been studied extensively in recent years. One of the first works on such problem was presented by Boneh and Shaw [12]. This work considered the problem of fingerprinting generic data that satisfied an underlying principle referred to as the marking assumption. They assumed a fingerprint to be a collection of n marks, each mark has q possible values, which are embedded in some places of the content unknown to users. Given any two fingerprints, positions in which the corresponding marks differ are termed detectable marks and these can be modified. A feasible set is the set of fingerprints spanned by a coalition taking into account all the detectable positions. A coalition of users is capable of creating a fingerprint, which could be any fingerprint from the feasible set.

Under their collusion framework, Boneh and Shaw introduced a frameproof code which is fingerprinting code that can be used to prevent any coalition from framing any user not in the coalition, and proposed a construction of t-frameproof codes with error-correcting codes in which no coalition of t users can frame someone outside the group. Frameproof codes and their applications have been then studied extensively, see for instance, [10, 20, 46, 48]. Boneh and Shaw in their work also showed that it is not possible to construct totally t-secure codes, which are fingerprinting codes that are capable of tracing at least one colluder out of a coalition of at most t colluders. Instead, they used randomization techniques to construct codes that are able to capture at least one colluder out of a coalition of at most t colluders with arbitrarily high probability.

Chor et al. presented a similar work in [18]. This work is concerned with the distribution of large amounts of contents, such as pay-per-view television broadcast, CD ROM distribution of data and online databases. The data supplier will encrypt the data and distribute a decoder which contains a set of keys needed to decrypt data to each authorized user. A coalition of colluders might create a pirate decoder that consists of keys from some of the colluders' decoders and redistribute to an unauthorized user. The authors designed a traitor tracing scheme which will reveal at least one colluder on the confiscation of a pirate decoder once the unauthorized user decrypt data using the pirate decoder.

In these cases described above for generic data, the ability to trace a colluder relied on the marking assumption that the identifying information cannot be blindly altered by coalition. However, Boneh and Shaw's marking assumption is not well suited for the multimedia domain since there are distinct embedding approaches. Engle [24] pointed out whether the marking assumption holds or not depends on the embedding fingerprinting approach. Fortunately, the marking assumption which corresponds to the spread spectrum embedding approach significantly limits the capability of colluders to conduct attacks. Selectively manipulating parts in a fingerprinting code is not directly possible, and instead other forms of attacks, such as the averaging collusion attack, must be used by adversaries to attempt to subvert a multimedia fingerprinting. This suggests that by jointly considering the encoding, embedding, and detection processes involved with fingerprinting multimedia, we have the potential to substantially enhance the performance of multimedia fingerprinting.

In order to resist the averaging collusion attack based on spread spectrum embedding technology, Trappe et al. [51, 52] introduced the notion of an AND anti-collusion code (AND-ACC) where the logical AND operation is exploited to identify colluders. Furthermore, they constructed AND-ACCs by using the bit complement of the incidence matrix of a combinatorial structure called balanced incomplete block design. Projective geometries were used to construct such anti-collusion codes in [23]. Constructions via other mathematical structures such as cover-free families can be found in [38]. Li and Trappe [39] also investigated collusion-resistant fingerprints from sequence sets satisfying the Welch bound equality.

Recently, Cheng and Miao [17] introduced a new concept of t-resilient logical anti-collusion code (LACC), where not only the logical AND operation but also the logical OR operation is exploited to identify colluders. LACCs have weaker requirements than AND-ACCs but they have the same traceability as AND-ACCs do. They also found an equivalence between an LACC and a binary separable code (SC). Constructions for LACCs and SCs were presented in [16, 17, 27].

1.2 Multimedia fingerprinting

In this section, we give a brief review on the basic concepts of multimedia fingerprinting, collusion and detection. The interested reader is referred to [17, 40] for more detailed information.

Fingerprints for multimedia data can be embedded through a variety of watermarking techniques prior to their authorized distribution. One of the widely employed robust embedding techniques is spread-spectrum additive embedding, which can survive collusion attacks to trace and identify colluders [21, 43]. In spread-spectrum embedding, a watermarked signal, often represented by a linear combination of noise-like orthonormal basis signals, is added to the host signal. Let $\mathbf{x}$ be the host multimedia signal, $\{\mathbf{u}_i \mid 1 \leq i \leq n\}$ be an orthonormal basis of noise-like signals, and $\{\mathbf{w}_j = (\mathbf{w}_j(1), \mathbf{w}_j(2), \ldots, \mathbf{w}_j(n)) = \sum_{i=1}^{n} b_{ij}\mathbf{u}_i \mid 1 \leq j \leq M\}$, $b_{ij} \in \{0, 1\}$, be a family of scaled watermarks to achieve the imperceptibility as well as to control the energy of the embedded watermark. Each authorized user U_j, $1 \leq j \leq M$, who has purchased the rights to access $\mathbf{x}$, is then assigned with a watermarked version of the content

$$\mathbf{y}_j = \mathbf{x} + \mathbf{w}_j. \tag{1.1}$$

The fingerprint $\mathbf{w}_j$ assigned to U_j can be represented uniquely by a vector (called codeword) $\mathbf{b}_j = (b_{1j}, b_{2j}, \dots, b_{nj})^T \in \{0,1\}^n$ because of the linear independence of the basis $\{\mathbf{u}_i \mid 1 \le i \le n\}$.

Collusion attacks can be broadly classified into linear and nonlinear attacks underlying spread-spectrum embedding. These two types of collusion attacks were investigated in [26, 35, 49, 50, 51, 52, 54, 57]. A set of typical nonlinear collision attacks, such as minimum/maximum/median attack, minmax attack, modified negative attack, randomized negative attack, were considered in [57]. For the detailed information, the interested reader is referred to [57]. Furthermore, Wang et al. [54] showed that all manipulations of nonlinear collusion attacks can be explained by linear collusion attacks with noise.

Now let us consider linear attacks which is one of the most feasible way to perform a collusion attack. When t authorized users, say $U_{j_1}, U_{j_2}, \dots, U_{j_t}$, who have the same host content but distinct fingerprints come together, we assume that they have no way of manipulating the individual orthonormal signals, that is, the underlying codeword needs to be taken and proceeded as a single entity, but they can carry on a linear collusion attack to generate a pirate copy from their t fingerprinted contents, so that the venture traced by the pirate copy can be attenuated. For fingerprinting through additive embedding, this is done by linearly combining the t fingerprinted contents $\sum_{l=1}^{t} \lambda_{j_l} \mathbf{y}_{j_l}$, where the weights $\{\lambda_{j_l} \in \mathbb{R}^+ \mid 1 \le l \le t\}$ satisfy the condition $\sum_{l=1}^{t} \lambda_{j_l} = 1$ to maintain the average intensity of the original multimedia signal. In such a collusion attack, the energy of each of the watermarks $\mathbf{w}_{j_l}$ is reduced by a factor of $\lambda_{j_l}^2$, therefore, the trace of U_{j_l}'s fingerprint becomes weaker and thus U_{j_l} is less likely to be caught by the detector. In fact, since normally no colluder is willing to take more of a risk than any other colluder, the fingerprinted signals are typically averaged with an equal weight for each user. Averaging attack choosing $\lambda_{j_l} = 1/t$, $1 \le l \le t$, is the most fair choice for each colluder to avoid detection, as claimed in [49, 52]. Furthermore, this attack also makes the pirate copy have better perceptional quality that it can be more similar to the host signal than the fingerprinted signals are.

Any circulated copy of the host multimedia content may experience an additional distortion $\mathbf{z}$ before it is tested for the existence of a fingerprint. This additional noise $\mathbf{z}$ could be due to the effects of unintentional signal processing or from attacks mounted by adversaries in an attempt to hinder the detection of the watermark. Based on the averaging attack model, the observed content $\mathbf{y}$ after collusion is

$$\mathbf{y} = \frac{1}{t}\sum_{l=1}^{t} \mathbf{y}_{j_l} + \mathbf{z} = \frac{1}{t}\sum_{l=1}^{t} \mathbf{w}_{j_l} + \mathbf{x} + \mathbf{z} = \sum_{l=1}^{t}\sum_{i=1}^{n} \frac{b_{ij_l}}{t}\mathbf{u}_i + \mathbf{x} + \mathbf{z}, \tag{1.2}$$

where $\mathbf{z}$ is usually assumed to follow an i.i.d. Gaussian $\mathcal{N}(0, \sigma_{\mathbf{z}}^2)$. Then from the detection theory [44], the optimum detector is the correlation vector $\mathbf{T} =$

$(\mathbf{T}(1), \mathbf{T}(2), \cdots, \mathbf{T}(n))$, where $\mathbf{T}(i) = \frac{1}{\sigma_{\mathbf{z}}}\langle \mathbf{y} - \mathbf{x}, \mathbf{u}_i \rangle$, $1 \leq i \leq n$, and $\langle \mathbf{y} - \mathbf{x}, \mathbf{u}_i \rangle$ is the inner product of $\mathbf{y} - \mathbf{x}$ and $\mathbf{u}_i$. It is straightforward to check that

$$\mathbf{T} = \frac{1}{t\sigma_{\mathbf{z}}} B \mathbf{\Phi}^T + \frac{1}{\sigma_{\mathbf{z}}}(\langle \mathbf{z}, \mathbf{u}_1 \rangle, \ldots, \langle \mathbf{z}, \mathbf{u}_n \rangle), \tag{1.3}$$

where $B = (b_{ij})$, $1 \leq i \leq n, 1 \leq j \leq M$, and the vector $\mathbf{\Phi} \in \{0,1\}^M$ indicates colluders via the location of the coordinates whose value is 1. The parameter $\sigma_{\mathbf{z}}$ depends on the embedded watermark-to-noise ratio (WNR), and is assumed known. Without loss of generality, let $\sigma_{\mathbf{z}} = 1$, then $(\langle \mathbf{z}, \mathbf{u}_1 \rangle, \ldots, \langle \mathbf{z}, \mathbf{u}_n \rangle)/\sigma_{\mathbf{z}}$ follows an $\mathcal{N}(\mathbf{0}_n, \mathbf{1}_n/t)$ distribution.

Thus, the model (1.2) can be equivalently presented as a null hypothesis testing

$$\begin{aligned} H_0 &: f(\mathbf{T} \mid \mathbf{\Phi} = 0) = \mathcal{N}(\mathbf{0}_n, \mathbf{1}_n), \\ H_1 &: f(\mathbf{T} \mid \mathbf{\Phi}) = \mathcal{N}(\frac{1}{t}\mathbf{B}\mathbf{\Phi}^T, \mathbf{1}_n), \end{aligned} \tag{1.4}$$

where we refer the reader back to (1.2) and (1.3) to arrive at this result.

Our goal is to efficiently estimate $\mathbf{\Phi}$ for any given colluded vector $\mathbf{T}$.

1.3 Outline of this thesis

This thesis focuses on the constructions of anti-collusion codes and the design of tracing algorithms for multimedia contents under the averaging collusion attack. The high-level idea of the structure in this thesis is as follows: Chapter 2 considers the optimality of $\bar{t}$-separable codes ($\bar{t}$-SCs), which were introduced in [17] to resist the averaging collusion attack; Chapters 3-5 introduce three types of codes resistant to the averaging attack for different models, consider the colluder tracing algorithms based on them, and investigate the optimality of these codes by combinatorial methods. Concatenation construction, as mentioned in [1], is a powerful method to construct infinite families of codes with a required property and long length by combining a "seed" code with the property and short length, together with an appropriate code with long length. This makes the study of "seed" codes interesting. In fact, the constructions in this thesis are all for "seed" codes with short length.

In Chapter 2, we investigate $\overline{2}$-SCs of length 2 from the standpoint of graph theory, and derive an upper bound on the size of a $\overline{2}$-SC of length 2 by considering the bounds of maximum size of bipartite graphs with girth 6. We then construct several infinite series of such codes by projective planes, some of which meet the derived upper bounds. This means that we construct several infinite series of optimal $\overline{2}$-SCs of length 2. These results improve the best bounds so far on $\overline{2}$-SCs of length 2 in [16]. We also consider $\overline{2}$-SCs of length 4 in this chapter. The combinatorial properties of $\overline{2}$-SCs of length 4 are investigated, and a construction of such codes is presented by means of incomplete squares, in which some entries are missing.

In Chapter 3, we want to decrease the computational complexity of the tracing algorithm based on $\overline{t}$-SCs but keep catching all colluders. Rather than devising better algorithms for $\overline{t}$-SCs, we introduce a new notion of a strong separable code ($\overline{t}$-SSC). We show that any binary $\overline{t}$-SSC can be used to identify, as a $\overline{t}$-SC does, all colluders when the number of colluders in the averaging attack is at most t. The computational complexity of such algorithm is $O(nM)$, which is obviously more efficient than the computational complexity $O(nM^t)$ of the algorithm based on a $\overline{t}$-SC, where n is the length of the code and M is the number of authorized users. Then we derive optimal $\overline{2}$-SSCs of length 2 by discussing the relationships between SSCs and SCs. We also investigate $\overline{2}$-SSCs of length 3 from a combinatorial viewpoint, and give a construction of such codes.

In the next chapter, Chapter 4, we concern with a new model guaranteeing exact identification of at least one member of the pirate coalition of size at most t, and introduce a new concept of a multimedia identifiable parent property code (t-MIPPC). Although t-MIPPCs can not be used to identify all the colluders when the size of the coalition is at most t, nevertheless they can be used to identify at least one colluder, thereby helping stop the proliferation of the fraudulent content in digital marketplace. The advantage of a t-MIPPC is the maximum number of the codewords, which corresponds to the number of authorized users. We show that the maximum number of the codewords of a t-MIPPC is more than that of a $\overline{t}$-SC. By considering bipartite graphs with girth at least 8, we derive a tight bound on the size of a 3-MIPPC of length 2. We also construct several series of (asymptotically) optimal 3-MIPPCs of length 2 from a geometric structure called generalized quadrangle.

In Chapter 5, in order to improve the computational complexity of the algorithm for t-MIPPCs, we introduce a new notion of a strong multimedia identifiable parent property code (t-SMIPPC). Then we state that any binary t-SMIPPC can be used to identify, as a t-MIPPC does, at least one colluder when the number of colluders in the averaging attack is at most t with computational complexity $O(nM)$, which is more efficient than the computational complexity $O(nM^t)$ of the algorithm based on a t-MIPPC. According to the relationships between SMIPPCs and other fingerprinting codes, such as SCs and MIPPCs, we derive optimal q-ary t-SMIPPCs of length 2 with $t = 2, 3$. The highlight of this chapter is the constructions of optimal q-ary 2-SMIPPCs of length 3 with $q \equiv 0, 1, 2, 5 \pmod 6$.

Finally, we give a brief summary of this thesis and some interesting open problems in Chapter 6.

Chapter 2

Separable Codes

Separable codes ($\bar{t}$-SCs) were introduced in [17] to construct logical anti-collusion codes (LACCs), which can be used to construct fingerprints resistant to the averaging collusion attack on multimedia contents. In this chapter, we pay our attention to the constructions of separable codes. We first recall the known results on separable codes in Section 2.1. In Section 2.2, we provide an improved upper bound on the size of a $\overline{2}$-SC of length 2 by a graph theoretical approach, and a lower bound on the size of such a code by deleting suitable points and lines from a projective plane, which coincides with the improved upper bound in some places. These correspond to the bounds of maximum size of bipartite graphs with girth 6 and a construction of such maximal bipartite graphs. In Section 2.3, we show the forbidden configurations of $\overline{2}$-SCs of length 4, and then give a construction of $\overline{2}$-SCs of length 4.

2.1 Known results on separable codes

Let n, M and q be positive integers, and Q an alphabet with $|Q| = q$. A set $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_M\} \subseteq Q^n$ is called an (n, M, q) code and each $\mathbf{c} = (\mathbf{c}(1), \mathbf{c}(2), \ldots, \mathbf{c}(n))^T$ in $\mathcal{C}$ is called a codeword. Without loss of generality, we may assume $Q = \{0, 1, \ldots, q-1\}$. When $Q = \{0, 1\}$, we also use the word "binary". Given an (n, M, q) code $\mathcal{C}$, the incidence matrix $M(\mathcal{C})$ is the $n \times M$ matrix on Q in which the columns are the M codewords in $\mathcal{C}$. Often, we make no difference between an (n, M, q) code and its incidence matrix unless otherwise stated.

For any code $\mathcal{C} \subseteq Q^n$, we define the set of i-th coordinates of $\mathcal{C}$ as

$$\mathcal{C}(i) = \{\mathbf{c}(i) \in Q \mid \mathbf{c} = (\mathbf{c}(1), \mathbf{c}(2), \ldots, \mathbf{c}(n))^T \in \mathcal{C}\}$$

for any $1 \leq i \leq n$. For any subset of codewords $\mathcal{C}^{'} \subseteq \mathcal{C}$, we define the descendant code (or feasible set) of $\mathcal{C}^{'}$ as

$$\mathsf{desc}(\mathcal{C}^{'}) = \{(\mathbf{x}(1), \mathbf{x}(2), \ldots, \mathbf{x}(n))^T \in Q^n \mid \mathbf{x}(i) \in \mathcal{C}^{'}(i), 1 \leq i \leq n\}, \tag{2.1}$$

that is,

$$\mathsf{desc}(\mathcal{C}^{'}) = \mathcal{C}^{'}(1) \times \mathcal{C}^{'}(2) \times \cdots \times \mathcal{C}^{'}(n).$$

The set $\mathsf{desc}(\mathcal{C}^{'})$ consists of the n-tuples that could be produced by a coalition holding the codewords in $\mathcal{C}^{'}$.

Example 2.1.1 Consider the following $(4, 3, 2)$ code $\mathcal{C}$:

$$\mathcal{C} = \begin{array}{c} \begin{array}{ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix} \end{array}$$

Obviously,

$$\begin{aligned} \mathsf{desc}(\{\mathbf{c}_1\}) &= \{(0,0,1,1)^T\} = \{\mathbf{c}_1\}, \\ \mathsf{desc}(\{\mathbf{c}_2\}) &= \{(1,0,0,1)^T\} = \{\mathbf{c}_2\}, \\ \mathsf{desc}(\{\mathbf{c}_3\}) &= \{(0,0,0,1)^T\} = \{\mathbf{c}_3\}. \end{aligned}$$

Consider the descendant codes of 2-subsets.

$$\begin{aligned} &\{\mathbf{c}_1, \mathbf{c}_2\}(1) = \{0,1\},\ \{\mathbf{c}_1, \mathbf{c}_2\}(2) = \{0\}, \\ &\{\mathbf{c}_1, \mathbf{c}_2\}(3) = \{0,1\},\ \{\mathbf{c}_1, \mathbf{c}_2\}(4) = \{1\}. \end{aligned}$$

Hence

$$\begin{aligned} \mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) &= \{\mathbf{c}_1, \mathbf{c}_2\}(1) \times \{\mathbf{c}_1, \mathbf{c}_2\}(2) \times \{\mathbf{c}_1, \mathbf{c}_2\}(3) \times \{\mathbf{c}_1, \mathbf{c}_2\}(4) \\ &= \{0,1\} \times \{0\} \times \{0,1\} \times \{1\} \\ &= \{(0,0,0,1)^T, (0,0,1,1)^T, (1,0,0,1)^T, (1,0,1,1)^T\}. \end{aligned}$$

Similarly,

$$\begin{aligned} \mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_3\}) &= \{(0,0,0,1)^T, (0,0,1,1)^T\}, \\ \mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3\}) &= \{(0,0,0,1)^T, (1,0,0,1)^T\}. \end{aligned}$$

Definition 2.1.2 *Let $\mathcal{C}$ be an $(n, M, 2)$ code with $Q = \{0, 1\}$ and $t \geq 2$ be an integer.*

(1) *$\mathcal{C}$ is a t-resilient AND anti-collusion code, or t-AND-ACC$(n, M, 2)$, if for any two distinct $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$ with $1 \leq |\mathcal{C}_1| \leq t$ and $1 \leq |\mathcal{C}_2| \leq t$, we have the following inequality:*

$$\bigwedge_{\mathbf{c} \in \mathcal{C}_1} \mathbf{c} \neq \bigwedge_{\mathbf{c} \in \mathcal{C}_2} \mathbf{c},$$

where $\bigwedge$ is the bitwise logical operator AND.

(2) *$\mathcal{C}$ is a t-resilient logical anti-collusion code, or t-LACC$(n, M, 2)$, if for any two distinct $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$ with $1 \leq |\mathcal{C}_1| \leq t$ and $1 \leq |\mathcal{C}_2| \leq t$, we have at least one of the following inequalities:*

$$\bigvee_{\mathbf{c} \in \mathcal{C}_1} \mathbf{c} \neq \bigvee_{\mathbf{c} \in \mathcal{C}_2} \mathbf{c}, \quad \bigwedge_{\mathbf{c} \in \mathcal{C}_1} \mathbf{c} \neq \bigwedge_{\mathbf{c} \in \mathcal{C}_2} \mathbf{c},$$

where $\bigvee$ is the bitwise logical operator OR.

Example 2.1.3 Consider the following $(3, 4, 2)$ code $\mathcal{C}$:

$$\mathcal{C} = \begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \begin{pmatrix} 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix} \end{array}$$

Then

$$\mathbf{c}_1 \bigvee \mathbf{c}_2 = (1,1,1)^T, \ \mathbf{c}_1 \bigvee \mathbf{c}_3 = (1,1,1)^T, \ \mathbf{c}_1 \bigvee \mathbf{c}_4 = (1,1,0)^T,$$
$$\mathbf{c}_2 \bigvee \mathbf{c}_3 = (1,1,1)^T, \ \mathbf{c}_2 \bigvee \mathbf{c}_4 = (1,0,1)^T, \ \mathbf{c}_3 \bigvee \mathbf{c}_4 = (0,1,1)^T.$$

However,

$$\mathbf{c}_1 \bigwedge \mathbf{c}_2 = (1,0,0)^T, \ \mathbf{c}_1 \bigwedge \mathbf{c}_3 = (0,1,0)^T, \ \mathbf{c}_2 \bigwedge \mathbf{c}_3 = (0,0,1)^T;$$
$$\mathbf{c}_1 \bigwedge \mathbf{c}_4 = (0,0,0)^T; \ \mathbf{c}_2 \bigwedge \mathbf{c}_4 = (0,0,0)^T; \ \mathbf{c}_3 \bigwedge \mathbf{c}_4 = (0,0,0)^T.$$

Therefore, by performing these twelve logical operations, we can know that $\mathcal{C}$ is a 2-LACC$(3, 4, 2)$, although is not a 2-AND-ACC$(3, 4, 2)$.

The notions of AND-ACCs and LACCs were introduced in [52] and [17], respectively, for protecting multimedia contents, which, with code modulation, can be used to construct families of fingerprints with the ability to survive collusion and trace colluders. From these definitions, we immediately know that a t-AND-ACC$(n, M, 2)$ is also a t-LACC$(n, M, 2)$, and a t-LACC of length n surpasses a t-AND-ACC of the same length in the number of codewords assigned to distinct authorized users of the multimedia content. The authors [17] also showed that any t-LACC$(n, M, 2)$ can be used to identify all colluders when the number of colluders in the averaging attack is at most t.

We now pay our attention to the colluder tracing algorithm based on a t-LACC. In the multimedia scenario, for any set of colluders holding codewords $\mathcal{C}_0 \subseteq \mathcal{C}$ and for any index $1 \leq i \leq n$, their detection statistics $\mathbf{T}(i)$ mentioned in Section 1.2 possesses the whole information on $\mathcal{C}_0(i)$; namely, we have $\mathbf{T}(i) = 1$ if and only if $\mathcal{C}_0(i) = \{1\}$, $\mathbf{T}(i) = 0$ if and only if $\mathcal{C}_0(i) = \{0\}$, and $0 < \mathbf{T}(i) < 1$ if and only if $\mathcal{C}_0(i) = \{0, 1\}$. Therefore, we can capture a set $R = \mathcal{C}_0(1) \times \cdots \times \mathcal{C}_0(n) \subseteq \mathcal{C}(1) \times \cdots \times \mathcal{C}(n)$ in the multimedia scenario from the detection statistics $\mathbf{T}$.

Theorem 2.1.4 ([17]) *Under the assumption that the number of colluders in the averaging attack is at most t, any t-LACC$(n, M, 2)$ can be used to identify all the colluders with computational complexity $O(nM^t)$.*

```
Algorithm 2.1: LACCTraceAlg($R$)
    Given $R$;
    Find $\mathcal{C}_0 \subseteq \mathcal{C}$ satisfying $|\mathcal{C}_0| \leq t$ and $R = \mathsf{desc}(\mathcal{C}_0)$;
    output $\mathcal{C}_0$ as the set of colluders.
```

In order to construct LACCs, they introduced the notion of a separable code defined as follows.

Definition 2.1.5 ([17]) *Let $\mathcal{C}$ be an (n, M, q) code and $t \geq 2$ be an integer. $\mathcal{C}$ is a $\bar{t}$-separable code, or $\bar{t}$-SC(n, M, q), if for any $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$ such that $1 \leq |\mathcal{C}_1| \leq t$, $1 \leq |\mathcal{C}_2| \leq t$ and $\mathcal{C}_1 \neq \mathcal{C}_2$, we have $\mathsf{desc}(\mathcal{C}_1) \neq \mathsf{desc}(\mathcal{C}_2)$, that is, there is at least one coordinate i, $1 \leq i \leq n$, such that $\mathcal{C}_1(i) \neq \mathcal{C}_2(i)$.*

Example 2.1.6 Consider the following $(3, 3, 2)$ code $\mathcal{C}$:

$$\mathcal{C} = \begin{array}{c} \begin{array}{ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 \end{array} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{pmatrix} \end{array}$$

We can directly obtain that

$$\begin{aligned}
\mathsf{desc}(\{\mathbf{c}_1\}) &= \{0\} \times \{0\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_2\}) &= \{1\} \times \{0\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_3\}) &= \{0\} \times \{1\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) &= \{0, 1\} \times \{0\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_3\}) &= \{0\} \times \{0, 1\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3\}) &= \{0, 1\} \times \{0, 1\} \times \{0\}.
\end{aligned}$$

Obviously, $\mathsf{desc}(\{\mathbf{c}_1\})$, $\mathsf{desc}(\{\mathbf{c}_2\})$, $\mathsf{desc}(\{\mathbf{c}_3\})$, $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\})$, $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_3\})$ and $\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3\})$ are all distinct. This is sufficient to show that $\mathcal{C}$ is a $\bar{2}$-SC$(3, 3, 2)$.

In fact, a $\bar{t}$-SC$(n, M, 2)$ and a t-LACC$(n, M, 2)$ are equivalent.

Theorem 2.1.7 ([17]) *Let $\mathcal{C}$ be an $(n, M, 2)$ code. Then $\mathcal{C}$ is a t-LACC if and only if it is a $\bar{t}$-SC$(n, M, 2)$.*

In other words, any binary $\overline{t}$-SC can be used to identify all colluders when the number of colluders in the averaging attack is at most t from Theorems 2.1.4 and 2.1.7.

Let $M_{SC}(\overline{t}, n, q) = \max\{M \mid \text{there exists a } \overline{t}\text{-SC}(n, M, q)\}$. A $\overline{t}$-SC(n, M, q) is said to be optimal if $M = M_{SC}(\overline{t}, n, q)$, and asymptotically optimal if $\lim\limits_{q\to\infty} \frac{M}{M_{SC}(\overline{t},n,q)}$ $= 1$. Cheng et al. [16] derived the following upper bound.

Theorem 2.1.8 ([16]) *$M_{SC}(\overline{t}, n, q) \leq q^{n-1} + \frac{q(q-1)}{2}$ holds for any $t \geq 2$.*

The following concatenation construction can be used to derive SCs with long length from SCs with short length, and makes the study of SCs with short length interesting.

Lemma 2.1.9 ([17]) *If there exist both a $\overline{t}$-SC(n_1, M, q) and a $\overline{t}$-SC$(n_2, q, 2)$, then there also exists a $\overline{t}$-SC$(n_1 n_2, M, 2)$.*

Several constructions on separable codes can be found in [16], and we only list the main results here.

Theorem 2.1.10 ([17]) *For any positive integer q, $M_{SC}(\overline{2}, 2, q) \leq qk + h$, where $k = \lfloor \frac{1+\sqrt{4q-3}}{2} \rfloor$, and*

$$h = \begin{cases} \lfloor \frac{q(q-1-k^2+k)}{2k} \rfloor, & \text{if} \quad k^2 - k + 1 \leq q \leq k^2; \\ \lfloor \frac{qk}{(k+1)^2 - q} \rfloor, & \text{if} \quad k^2 + 1 \leq q \leq k^2 + k. \end{cases}$$

Furthermore, $M_{SC}(\overline{2}, 2, q) = qk + h$ if $q = k^2 - k + 1$ for any prime power $k - 1 \geq 2$ and $q = k^2 + k$ for any prime power $k \geq 2$.

Theorem 2.1.11 ([17]) *There exists an optimal $\overline{2}$-SC$(3, q^2 + \frac{q(q-1)}{2}, q)$ for any integer q.*

2.2 $\overline{2}$-SCs of length 2

In this section, we improve the results in Theorem 2.1.10. In fact, we obtain a tighter upper bound on $M_{SC}(\overline{2}, 2, q)$ via graph theoretical approach. By using projective geometrical terminologies, we also obtain a lower bound on $M_{SC}(\overline{2}, 2, q)$, parts of which agree with the new derived upper bound. In other words, we construct several infinite series of optimal $\overline{2}$-SC$(2, M, q)$s.

2.2.1 Related combinatorial objects

In this subsection, we recall several combinatorial structures related to $\overline{2}$-SCs of length 2.

For any (n, M, q) code $\mathcal{C}$ on $Q = \{0, 1, \ldots, q-1\}$, we define the following shortened code $\mathcal{A}_i^j$ for $i \in Q$ and $1 \leq j \leq n$:

$$\mathcal{A}_i^j = \{(\mathbf{c}(1), \ldots, \mathbf{c}(j-1), \mathbf{c}(j+1), \ldots, \mathbf{c}(n))^T \mid (\mathbf{c}(1), \ldots, \mathbf{c}(n))^T \in \mathcal{C}, \mathbf{c}(j) = i\}.$$

Obviously, for any $(2, M, q)$ code, $\mathcal{A}_i^1 \subseteq Q$ holds for any $i \in Q$, and $|\mathcal{A}_0^1| + |\mathcal{A}_1^1| + \cdots + |\mathcal{A}_{q-1}^1| = M$.

Definition 2.2.1 *Let K be a subset of non-negative integers, and v, b be two positive integers. A generalized $(v, b, K, 1)$ packing is a pair $(X, \mathcal{B})$ where X is a set of v elements and $\mathcal{B}$ is a set of b subsets of X called blocks that satisfy*

(1) *$|B| \in K$ for any $B \in \mathcal{B}$;*

(2) *every pair of distinct elements of X occurs in at most one block of $\mathcal{B}$.*

Example 2.2.2 Let $X = \{0, 1, 2, 3, 4\}$ be the element set. Then $(X, \mathcal{B})$ forms a generalized $(5, 5, \{2, 3\}, 1)$ packing, where

$$\mathcal{B} = \{\{0, 4\}, \{1, 3\}, \{3, 4\}, \{0, 2, 3\}, \{1, 2, 4\}\}.$$

Cheng et al. [16] showed a relationship between separable codes and generalized packings.

Lemma 2.2.3 ([16]) *There exists a $\overline{2}$-$SC(2, M, q)$ defined on $Q = \{0, 1, \ldots, q-1\}$ if and only if there exists a generalized $(q, q, K, 1)$ packing $(Q, \{\mathcal{A}_0^1, \mathcal{A}_1^1, \ldots, \mathcal{A}_{q-1}^1\})$, with $K = \{|\mathcal{A}_0^1|, |\mathcal{A}_1^1|, \ldots, |\mathcal{A}_{q-1}^1|\}$, and $M = |\mathcal{A}_0^1| + |\mathcal{A}_1^1| + \cdots + |\mathcal{A}_{q-1}^1|$.*

Example 2.2.4 Construct a $\overline{2}$-SC$(2, 13, 5)$ from the generalized $(5, 5, \{2, 3\}, 1)$ packing mentioned in Example 2.2.2. Let

$$B_0 = \{0, 4\}, B_1 = \{1, 3\}, B_2 = \{3, 4\}, B_3 = \{0, 2, 3\}, B_4 = \{1, 2, 4\}.$$

For any $i \in X = \{0, 1, 2, 3, 4\}$ and any element $x \in B_i$, we construct a codeword $(i, x)^T$. Then we can obtain a code

$$\mathcal{C} = \begin{pmatrix} 0 & 0 & 1 & 1 & 2 & 2 & 3 & 3 & 3 & 4 & 4 & 4 \\ 0 & 4 & 1 & 3 & 3 & 4 & 0 & 2 & 3 & 1 & 2 & 4 \end{pmatrix}.$$

We can directly check that $\mathcal{C}$ is a $\overline{2}$-SC$(2, 13, 5)$.

Note that balanced incomplete block designs [52] and packing designs [38] which were used to construct AND-ACC are special classes of generalized packings, so they can only be used to construct some special classes of $\overline{2}$-SCs of length 2.

A generalized $(q, q, \{k\}, 1)$ packing can be constructed by developing a near difference set. A $(q, k, 1)$ near difference set defined on an additively written group G of order $|G| = q$ is a k-subset F of G such that the differences $\{x - y \mid x, y \in F, x \neq y\}$ contains $k(k-1)$ distinct elements of G.

Example 2.2.5 Let $F = \{0, 1, 3\}$ be a subset of Z_7. Then the differences $\{x - y \mid x, y \in F, x \neq y\} = \{0, 1, 2, 3, 4, 5, 6\}$. This implies that F is a $(7, 3, 1)$ near difference set defined on Z_7.

Lemma 2.2.6 *For any integer $k \geq 2$, let $q \geq k^2 - k + 1$. If there exists a $(q, k, 1)$ near difference set, then there exists a generalized $(q, q, \{k\}, 1)$ packing.*

Proof: Let F be a $(q, k, 1)$ near difference set defined on an additively written group G. For any $g \in G$, define $F + g = \{x + g \mid x \in F\}$ and $\mathcal{B} = \{F + g \mid g \in G\}$. Then $(G, \mathcal{B})$ is the desired generalized $(q, q, \{k\}, 1)$ packing. □

Near difference sets are not easy to construct. However, a $(k^2 + k + 1, k, 1)$ near difference set always exists [45] for any prime power k. This Singer difference set generates a generalized $(k^2 + k + 1, k^2 + k + 1, \{k\}, 1)$ packing, which corresponds to an optimal $\overline{2}$-SC$(2, (k+1)(k^2 + k + 1), k^2 + k + 1)$ described in Theorem 2.1.10.

2.2.2 Basic concepts in Graph Theory

In order to investigate $\overline{2}$-SCs of length 2, we need some basic concepts in Graph Theory.

Let V be a finite set, and $E(V) = \{\{u, v\} \mid u, v \in V, u \neq v\}$.

Definition 2.2.7 *A pair $G = (V, E)$ with $E \subseteq E(V)$ is called a (simple) graph (on V). The elements of V are the vertices of G and those of E the edges of G. Given a graph G, the vertex set of G is denoted by $V(G)$ and its edge set by $E(G)$. The number $|V(G)|$ is called the order of G, and $|E(G)|$ is the size of G.*

A graph H is a subgraph of a graph G, if $V(H) \subseteq V(G)$ and $E(H) \subseteq E(G)$.

Example 2.2.8 Consider the following graphs:

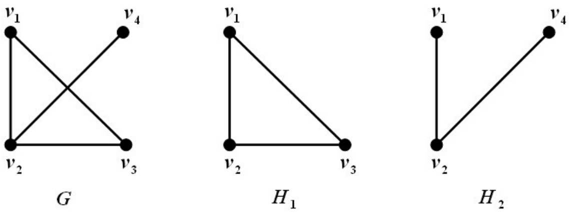

Figure 2.1: Graphs

Then $V(G) = \{v_1, v_2, v_3, v_4\}$ and $E(G) = \{\{v_1, v_2\}, \{v_1, v_3\}, \{v_2, v_3\}, \{v_2, v_4\}\}$. The order and the size of G are $|V(G)| = 4$ and $|E(G)| = 4$, respectively. H_1 and H_2 are subgraphs of G.

Definition 2.2.9 *For a graph $G = (V, E)$, vertices u and v are adjacent if $\{u, v\} \in E$. The neighbourhood of a vertex $v \in V$ is the set*

$$N_G(v) = \{u \in G \mid \{u, v\} \in E\}.$$

The degree of v, denoted by $\mathsf{deg}_G(v)$, is the number of its neighbours, that is, $\mathsf{deg}_G(v) = |N_G(v)|$.

From the above definition and Example 2.2.8, it is easy to see that $\mathsf{deg}_G(v_1) = \mathsf{deg}_G(v_3) = 2$, $\mathsf{deg}_G(v_2) = 3$ and $\mathsf{deg}_G(v_4) = 1$.

Definition 2.2.10 *Given a graph G, we call $(v_1, v_2, \ldots, v_h)$ a cycle of length $h \geq 3$, denoted by C_h, if $\{v_i, v_{i+1}\} \in E(G)$ for all $1 \leq i \leq h-1$, $\{v_1, v_h\} \in E(G)$, and $v_j \neq v_k$ for $1 \leq j < k \leq h$.*

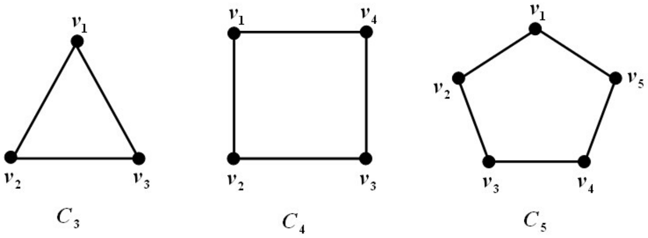

Figure 2.2: Cycles

Definition 2.2.11 *Two graphs G and H are isomorphic if there exists a bijection Let $f\colon V(G) \to V(H)$ such that*

$$\{u, v\} \in E(G) \Leftrightarrow \{f(u), f(v)\} \in E(H)$$

for all $u, v \in V(G)$.

In fact, two isomorphic graphs enjoy the same graph theoretical properties.

Example 2.2.12 The following graphs are isomorphic.

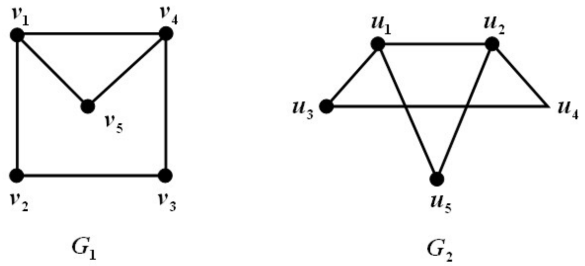

Figure 2.3: Isomorphic graphs

Indeed, the required isomorphism is given by $v_1 \to u_1$, $v_2 \to u_3$, $v_3 \to u_4$, $v_4 \to u_2$, $v_5 \to u_5$.

The graph G is the complete graph, if every two vertices are adjacent. All complete graphs of order n are isomorphic with each other, and they will be denoted by K_n. A clique in a graph G is a subgraph of G such that every two vertices are adjacent, that is, a complete subgraph of G.

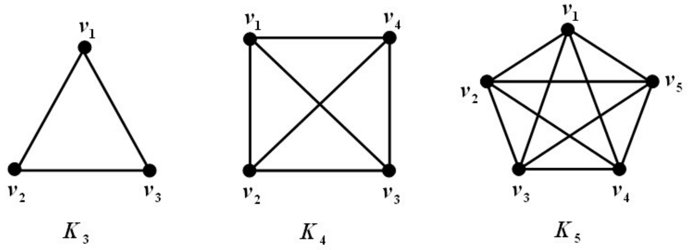

Figure 2.4: Complete graphs

Definition 2.2.13 *A graph G is called bipartite, denoted by $G_{X,Y}$, if $V(G)$ has a partition to two subsets X and Y such that each edge in $E(G)$ connects a vertex of X and a vertex of Y.*

A bipartite graph G is a complete (m, k)-bipartite graph, if $|X| = m$, $|Y| = k$, and $\{u, v\} \in E(G)$ for all $u \in X$ and $v \in Y$. All complete (m, k)-bipartite graphs are isomorphic. Let $K_{m,k}$ denote such a graph.

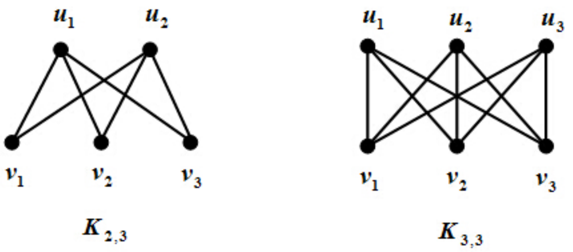

Figure 2.5: Complete bipartite graphs

Given a generalized $(v, b, K, 1)$ packing $(Q, \mathcal{B})$, we can define its associated element-block graph as the bipartite graph $G_{Q,\mathcal{B}}$ with vertex partition Q and $\mathcal{B}$ such that $x \in Q$ is adjacent to $B \in \mathcal{B}$ if and only if $x \in B$. It is clear that the corresponding element-block graph of a generalized $(v, b, K, 1)$ packing $(Q, \mathcal{B})$ is a C_4-free subgraph (that is, a subgraph containing no C_4) of the complete bipartite graph $K_{v,b}$, because any pair of distinct elements of Q can occur in at most one block of $\mathcal{B}$. In other words, the girth of this bipartite graph is at least 6, where the girth of a graph is the length of a shortest cycle contained in the graph.

Example 2.2.14 Consider the generalized $(5, 5, \{2, 3\}, 1)$ packing mentioned in Example 2.2.2. Let

$$B_0 = \{0, 4\}, B_1 = \{1, 3\}, B_2 = \{3, 4\}, B_3 = \{0, 2, 3\}, B_4 = \{1, 2, 4\}.$$

Then its associated element-block graph is as follows.

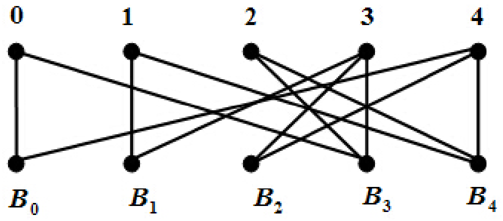

Figure 2.6: $G_{X,\mathcal{B}}$

Zarankiewicz numbers [56] involve bounds on the maximum number of edges in a bipartite graph without a particular subgraph. We denote by $z(m, n; s, t)$, $m \leq n$ and $s \leq t$, the maximum number of edges in a subgraph of $K_{m,n}$ that does not contain a subgraph isomorphic to $K_{s,t}$. In particular, when $m = n$ and $s = t$, simply put $z(n; t) = z(n, n; t, t)$. It is clear that $z(q; 2)$, which is the maximum size of a C_4-free bipartite subgraph of $K_{q,q}$, is equal to $M_{SC}(\overline{2}, 2, q)$ by Lemma 2.2.3.

Meanwhile, García-Vázquez et al. [28] stated that any C_4-free bipartite subgraph of $K_{q,q}$ with size $z(q;2)$ must have girth 6. Therefore, our problem is equivalent to finding the maximum size of bipartite graphs with girth 6, and constructing such maximal bipartite graphs.

We can see our problem in one more way. Given a generalized $(q, q, K, 1)$ packing $(Q, \mathcal{B})$, if we define two elements of Q are adjacent in $B \in \mathcal{B}$ if they occur in the same block B, then each block can be seen as a clique of order $|B|$ belonging to K. Since each pair of distinct elements of Q occurs in a block of $\mathcal{B}$ at most once, this generalized $(q, q, K, 1)$ packing can be viewed as a packing of the complete graph K_q by q cliques of orders belonging to K, where a packing of a graph G is a set of subgraphs of G such that their edge sets are pairwise disjoint. Therefore, in order to evaluate $z(q;2) = M_{SC}(\overline{2}, 2, q)$, it is sufficient to pack K_q by q cliques so that the sum of order of the q cliques is maximum.

It is well known [11] that $z(q;2) \leq \frac{q+q\sqrt{4q-3}}{2}$ and the equality holds when $q = k^2 + k + 1$ for any prime power k. Goddard et al. [29] found the exact values of $z(q;2)$ for $q \leq 10$. Theorem 2.1.10 is an improvement of the results made by Cheng et al. [16]. It is also known [11] that if q is sufficiently large then

$$q^{3/2} - q^{4/3} < z(q;2) \leq \frac{q + q\sqrt{4q-3}}{2};$$

In particular, $\lim_{q\to\infty} \frac{z(q;2)}{q^{3/2}} = 1$.

2.2.3 Upper bound

Bipartite graphs with high girth and their related graphs have been extensively investigated, see, e.g., [7, 14, 25, 28, 30, 33, 37, 36, 41, 42, 55]. We start this section with the following lemma.

Lemma 2.2.15 ([13]) *Suppose $(X, \mathcal{B})$ is a generalized $(v, b, \{k, k+1\}, 1)$ packing, for some k, with $\mathcal{B} = \{B_1, B_2, \dots, B_b\}$. If $\binom{v}{2} - \sum_{i=1}^{b} \binom{|B_i|}{2} < k$, then $G_{X,\mathcal{B}}$, the element-block graph of $(X, \mathcal{B})$, is a C_4-free subgraph of $K_{v,b}$ with maximum size.*

If K_q can be packed by q cliques $K_{x_1}, K_{x_2}, \dots, K_{x_q}$ with leave L (a set of the edges which are not covered by the q cliques), where $x_i \leq x_j$ for $1 \leq i < j \leq q$, then we say K_q admits a feasible $(x_1, x_2, \dots, x_q)$ packing with leave L. For convenience, we replace $(x_1, x_2, \dots, x_q)$ packing by $(k^{q-h}, (k+1)^h)$ packing when

$$k = x_1 = \cdots = x_{q-h} \text{ and } x_{q-h+1} = \cdots = x_q = k+1$$

for some $k \in \mathbb{N}$ and $1 \leq h \leq q$. For any $(k^{q-h}, (k+1)^h)$ packing $\mathcal{P}$ of K_q, we have

$$q\binom{k}{2} \leq (q-h)\binom{k}{2} + h\binom{k+1}{2} \leq \binom{q}{2},$$

which implies $k \le \frac{1+\sqrt{4q-3}}{2}$. In order to maximize $\sum_{i=1}^{q} x_i$ which subjects to an $(x_1, x_2, \ldots, x_q)$ packing, Lemma 2.2.15 promises to consider a feasible $(k^{q-h}, (k+1)^h)$ packing with $k = \lfloor \frac{1+\sqrt{4q-3}}{2} \rfloor$ and $|L| < k$. Therefore, our objective is to find the maximum index h. Note that $k = \lfloor \frac{1+\sqrt{4q-3}}{2} \rfloor$ implies $k^2 - k + 1 \le q < k^2 + k + 1$. In this subsection, we investigate $z(q;2)$ by fixing the index k and then classifying q, from $k^2 - k + 1$ to $k^2 + k$, into several cases. The following Theorem 2.2.16 is contained in Theorem 2.1.10.

Theorem 2.2.16 ([11, 16]) *For any prime power $k - 1 \ge 2$, $z(k^2 - k + 1; 2) = k^3 - k^2 + k$. For any prime power $k \ge 2$, $z(k^2 + k; 2) = k^3 + 2k^2$.*

Theorem 2.2.17 *For any $k^2 + 1 \le q \le k^2 + k - 2$ and $k \ge 2$, we have*

$$z(q;2) \le qk + \left\lfloor \frac{(k-1)q}{(k+1)^2 - (q+1)} \right\rfloor .$$

Proof: Let $q = k^2 + k - s$, $s = 2, 3, \ldots, k-1$. Assume $\mathcal{P}$ is a $(k^{q-h}, (k+1)^h)$ packing of K_q, where $0 \le h \le q - 1$. We claim by contradiction that $h \le \lfloor \frac{(k-1)q}{(k+1)^2-(q+1)} \rfloor$. That is, suppose $h > \lfloor \frac{(k-1)q}{(k+1)^2-(q+1)} \rfloor$.

For $i \ge 0$, let r_i be the number of vertices that is contained in exactly i cliques of order $k+1$ in $\mathcal{P}$. Since the degree of each vertex is $k^2+k-s-1$, trivially $r_i = 0$ for all $i > k$. We now claim $r_k = 0$. Suppose not, that is, there exists a vertex v contained in exactly k cliques of order $k+1$, say $C^{(1)}, C^{(2)}, \ldots, C^{(k)}$. Let $A = \{v\} \cup \bigcup_{i=1}^{k} V(C^{(i)})$ and $B = V(K_q) \setminus A$. Since there is no other subgraph isomorphic to K_{k+1} out of A except $C^{(1)}, C^{(2)}, \ldots, C^{(k)}$, each of the remaining cliques of order $k+1$ must contain at least one vertex in B. That is, each of such cliques needs at least k edges between A and B. Therefore, we have at most $k + \lfloor \frac{(k^2+1)(k-s-1)}{k} \rfloor$ cliques of order $k+1$. Thus,

$$k(k-s) \ge k + \lfloor \frac{(k^2+1)(k-s-1)}{k} \rfloor \ge h > \lfloor \frac{(k-1)q}{(k+1)^2 - (q+1)} \rfloor .$$

This implies $ks^2 - ks - k + s < 0$, so $ks(s-1) \le k - s < k$, that is, $s(s-1) < 1$, which contradicts $2 \le s \le k-1$. So $r_k = 0$.

Consider the number of ordered pairs (v, C), where v is a vertex in the clique C of order $k+1$ in $\mathcal{P}$. Under our assumption, there are exactly h cliques of order $k+1$, then

$$h(k+1) = (k-1)r_{k-1} + (k-2)r_{k-2} + \cdots + (k-s)r_{k-s} + \cdots + r_1. \qquad (2.2)$$

This implies that

$$h(k+1) \le (k-1)(r_{k-1} + \cdots + r_{k-s+1}) + (k-s)(q - (r_{k-1} + \cdots + r_{k-s+1})),$$

so

$$\frac{h(k+1)-q(k-s)}{s-1} \leq r_{k-1}+\cdots+r_{k-s+1}. \tag{2.3}$$

Now, we delete all the h cliques of order $k+1$ from K_q. Denote by G the remaining subgraph. We again consider the number of ordered pairs (v', C'), where v' is a vertex in the clique C' of order k in $\mathcal{P}$. On one hand there are exactly $q-h$ cliques of order k, and on the other hand there are exactly r_i vertices of degree $q-1-ki$, for $i=0,1,\ldots,k-1$. Since the vertex of degree $q-1-ki$ can be contained in at most $\frac{q-1-ki}{k-1}$ cliques of order k, we have

$$(q-h)k \leq r_{k-1}+2r_{k-2}+\cdots+(s-1)r_{k-s+1}+(s+1)r_{k-s}+\cdots+(k+1)r_0. \tag{2.4}$$

Combining (2.2) and (2.4) we have

$$h(k+1)+(q-h)k \leq k(r_{k-1}+\cdots+r_{k-s+1})+(k+1)(q-(r_{k-1}+\cdots+r_{k-s+1})),$$

and thus

$$r_{k-1}+\cdots+r_{k-s+1} \leq q-h. \tag{2.5}$$

Finally, (2.3) and (2.5) imply that $h \leq \frac{q(k-1)}{k+s} = \frac{(k-1)q}{(k+1)^2-(q+1)}$, a contradiction to the hypothesis. Thus we complete the proof. □

Theorem 2.2.18 *For any $q=k^2$ with $k \geq 2$, we have*

$$z(q;2) \leq qk + \lfloor \frac{(3k^2+k-1)-\sqrt{5k^4+6k^3-k^2-2k+1}}{2} \rfloor.$$

Proof: Assume $\mathcal{P}$ is a $(k^{q-h},(k+1)^h)$ packing of K_q. For $i \geq 0$, let r_i be the number of vertices that is contained in exactly i cliques of order $k+1$ in $\mathcal{P}$. Since $q=k^2$, we have $r_i=0$ for all $i \geq k$. Similar to the proof of Theorem 2.2.17, we first consider the number of ordered pairs (v,C), where v is a vertex in the clique C of order $k+1$ in $\mathcal{P}$. Then after deleting those cliques of order $k+1$, we consider the number of ordered pairs (v', C'), where v' is a vertex in the clique C' of order k in $\mathcal{P}$. Note that in the remaining graph after deleting h cliques of order $k+1$, there are exactly r_i vertices of degree k^2-ik-1. Then we have

$$\begin{cases} h(k+1) & = & (k-1)r_{k-1}+\cdots+2r_2+r_1 \\ (q-h)k & \leq & r_{k-1}+\cdots+(k-2)r_2+(k-1)r_1+(k+1)r_0 \end{cases}$$

which implies $h \leq r_0$. This concludes that the h cliques of order $k+1$ are out of at most k^2-h vertices somewhere in $\mathcal{P}$. We immediately have

$$h\binom{k+1}{2} \leq \binom{k^2-h}{2}.$$

That is,

$$h^2+(1-k-3k^2)h+(k^4-k^2) \geq 0.$$

Since $h \leq k^2$, we have $h \leq \frac{(3k^2+k-1)-\sqrt{5k^4+6k^3-k^2-2k+1}}{2}$. Hence we complete the proof. □

Theorem 2.2.19 *For any $k^2-k+2 \le q \le k^2-1$ and $k \ge 2$, we have $z(q;2) \le qk$.*

Proof: Let $q = k^2 - s$, where $s = 1, 2, \dots, k-2$. Assume $\mathcal{P}$ is a $(k^{q-h}, (k+1)^h)$ packing of K_q. Suppose $h \ge 1$. Define G to be the graph by deleting one of the cliques of order $k+1$, say $\widehat{K}$, from K_q. Let $A \subseteq V(G)$ be the collection of vertices whose degree is equal to $q-1-k$, and $B = V(G) \setminus A$. Note that $|A| = k+1$ and $|B| = q-k-1$. Now, consider the number of ordered pairs (v, C), where v is a vertex in the clique C in $\mathcal{P}$ different from $\widehat{K}$. Notice that for each $v \in A$, $\mathsf{deg}_G(v) = k^2 - s - 1 - k = (k-1)^2 + (k-s-2)$. Then v is contained in at most $k-1$ cliques different from $\widehat{K}$. Similarly, each vertex in B can be contained in at most k cliques. By counting the number of pairs (v, C), we have

$$(h-1)(k+1) + (q-h)k \le (k+1)(k-1) + (q-k-1)k.$$

This implies that $h \le 0$, a contradiction occurs. Thus the result follows. □

2.2.4 Lower bound

Now we derive a lower bound on $z(q;2) = M_{SC}(\overline{2}, 2, q)$ via projective planes. A projective plane P consists of a set of lines, a set of points, and a relation between points and lines called incidence, having the following properties:

(1) Given any two distinct points, there is exactly one line incident with both of them.

(2) Given any two distinct lines, there is exactly one point incident with both of them.

(3) There are four points such that no line is incident with more than two of them.

For a projective plane P, there is a positive integer k such that any line of P has exactly $k+1$ points. This number k is the order of P. Clearly, a projective plane of order k is a generalized $(k^2+k+1, k^2+k+1, \{k+1\}, 1)$ packing $(X, \mathcal{B})$ in which every pair of distinct elements of X occurs in exactly one block of $\mathcal{B}$. It is well-known [31] that a projective plane of order k always exists for any prime power k.

Theorem 2.2.20 *For any prime power $k \ge 2$, let $k^2 - 1 \le q \le k^2 + k - 1$. Then there exists a generalized $(q, q, \{k, k+1\}, 1)$ packing, $(X', \mathcal{B}')$, with $|X'| = |\mathcal{B}'| = q$ such that exactly $k^3 - k^2 - k - qk + 2q + 1$ blocks out of $\mathcal{B}'$ are of size k. That is,*

$$z(q;2) \ge 2qk - k^3 + k^2 + k - q - 1.$$

Proof: We start from a projective plane of order k, $(X, \mathcal{B})$. Note that $|X| = |\mathcal{B}| = k^2 + k + 1$, and for any $B \in \mathcal{B}$, $|B| = k + 1$. Pick an arbitrary point $a \in X$ and an arbitrary line $B^* = \{x_1, x_2, \ldots, x_{k+1}\} \in \mathcal{B}$ which does not contain the point a. For each $i = 1, \ldots, k+1$, let $B_i \in \mathcal{B}$ be the line containing the points a and x_i. Let $2 \leq s \leq k+2$. Deleting s lines $B^*, B_1, \ldots, B_{s-1}$ and s points $a, x_1, \ldots, x_{s-1}$ from $(X, \mathcal{B})$, we obtain a generalized $(q, q, \{k, k+1\}, 1)$ packing, $(X', \mathcal{B}')$, with $q = k^2 + k + 1 - s$, $X' = X \setminus \{a, x_1, \ldots, x_{s-1}\}$, $\mathcal{B}' = \mathcal{B} \setminus \{B^*, B_1, \ldots, B_{s-1}\}$, having $\Delta = (s-1)(k-1) + (k+1-s+1) = k^3 - k^2 - k - qk + 2q + 1$ blocks of size k and $k^2 + k + 1 - \Delta - s$ blocks of size $k+1$. Therefore, $z(q; 2) \geq k\Delta + (k+1)(k^2 + k + 1 - \Delta - s) = 2qk - k^3 + k^2 + k - q - 1$. □

Applying Theorems 2.1.10, 2.2.17 and 2.2.19, we immediately have the following result.

Corollary 2.2.21 *For any prime power $k \geq 2$, $z(k^2 - 1; 2) = k^3 - k$, $z(k^2 + k - 2; 2) = k^3 + 2k^2 - 4k + 1$, $z(k^2 + k - 1; 2) = k^3 + 2k^2 - 2k$.*

In Corollary 2.2.21, when $q = k^2 + k - 2$, $k^2 + k - 1$, the same results are also obtained independently by G. Damaásdi et al. [22]. It is also easy to verify that the corresponding $\overline{2}$-SC$(2, M, q)$s constructed in Theorem 2.2.20 are asymptotically optimal for all $k^2 - 1 \leq q \leq k^2 + k - 1$ with prime power k. The lower bound described in Theorem 2.2.20 is better than $q^{3/2} - q^{4/3}$ described in [11] for any prime power k.

2.2.5 Summary

The main results in the previous subsections can be summarized in the following theorem.

Theorem 2.2.22 *For any positive integer q, $M_{SC}(\overline{2}, 2, q) \leq qk + h$, where $k = \lfloor \frac{1+\sqrt{4q-3}}{2} \rfloor$, and*

$$h = \begin{cases} 0 & \text{if } k^2 - k + 1 \leq q \leq k^2 - 1; \\ \lfloor \frac{(3k^2+k-1)-\sqrt{5k^4+6k^3-k^2-2k+1}}{2} \rfloor & \text{if } q = k^2; \\ \lfloor \frac{(k-1)q}{(k+1)^2-(q+1)} \rfloor & \text{if } k^2 + 1 \leq q \leq k^2 + k - 2; \\ k^2 - k & \text{if } q = k^2 + k - 1; \\ k^2 & \text{if } q = k^2 + k. \end{cases}$$

Furthermore, $M_{SC}(\overline{2}, 2, q) = qk + h$ if $q \in \{k^2-1, k^2+k-2, k^2+k-1, k^2+k, k^2+k+1\}$ for any prime power $k \geq 2$.

This is in fact the main results of this section. The following Figures 2.7 and 2.8 illustrate our improvement on the upper bound of $M_{SC}(\overline{2}, 2, q)$. Figure 2.7 depicts the known upper bound given in [16] and the new upper bound given in Theorem 2.2.22 when $k = 12$, while Figure 2.8 depicts those upper bounds when $q = k^2$. It can be seen that our new upper bound is much tighter than the known upper bound.

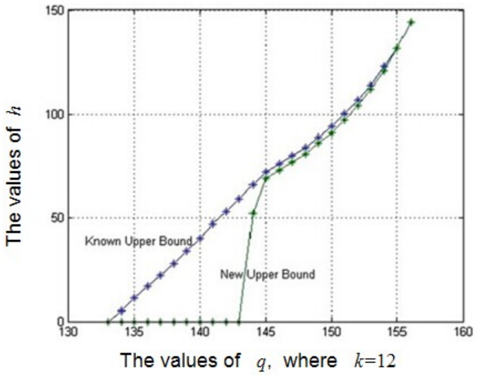

Figure 2.7: Bounds for $k = 12$

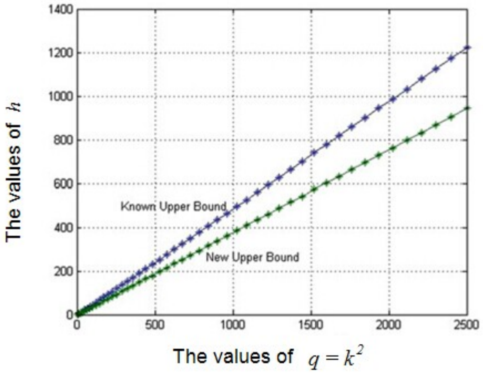

Figure 2.8: Bounds for $q = k^2$

2.3 $\overline{2}$-SCs of length 4

Theorem 2.1.11 shows that optimal $\overline{2}$-SCs of length 3 always exit, and thus we investigate $\overline{2}$-SCs of length 4 in this section. We in fact derive the forbidden configurations of $\overline{2}$-SCs of length 4, and construct an infinite family of such codes, which are asymptotically optimal.

For any (n, M, q) code $\mathcal{C}$ with $n > 2$ over $Q = \{0, 1, \ldots, q-1\}$, we define another shortened code $\mathcal{A}_{i,k}^{j_1,j_2}$ for $i, k \in Q$ and $1 \leq j_1 < j_2 \leq n$ as follows:

$$\mathcal{A}_{i,k}^{j_1,j_2} = \{(c(1), \ldots, c(j_1-1), c(j_1+1), \ldots, c(j_2-1), c(j_2+1), \ldots, c(n))^T | \\ (c(1), \ldots, c(n))^T \in \mathcal{C},\ c(j_1) = i, c(j_2) = k\}.$$

Obviously, $\mathcal{A}_{i,k}^{j_1,j_2} \subseteq Q^{n-2}$ and $|\mathcal{A}_{0,0}^{j_1,j_2}| + |\mathcal{A}_{0,1}^{j_1,j_2}| + \ldots + |\mathcal{A}_{q-1,q-1}^{j_1,j_2}| = M$ always hold for any integers j_1, j_2, where $1 \leq j_1 < j_2 \leq n$.

Theorem 2.3.1 *A $(4, M, q)$ code $\mathcal{C}$ is a $\overline{2}$-SC$(4, M, q)$ on Q if and only if the following two conditions hold.*

(1) $|\mathcal{A}_{i_1}^{j_1} \bigcap \mathcal{A}_{i_2}^{j_1}| \leq 1$ *holds for any positive integers* $j_1 \in \{1, 2, 3, 4\}$ *and distinct* $i_1, i_2 \in Q$.

(2) $|\mathcal{A}_{i_1,k_1}^{j_1,j_2} \bigcap \mathcal{A}_{i_2,k_2}^{j_1,j_2}| \leq 1$ *holds for any vector* $(j_1, j_2) \in \{(1, 2), (1, 3), (1, 4)\}$ *and* $i_1, i_2, k_1, k_2 \in Q$, *where* $i_1 \neq i_2$ *and* $k_1 \neq k_2$.

Proof: First, let $\mathcal{C}$ be a $\overline{2}$-SC$(4, M, q)$.

(I) Suppose that there exist $j_1 \in \{1, 2, 3, 4\}$ and distinct $i_1, i_2 \in Q$, such that $|\mathcal{A}_{i_1}^{j_1} \bigcap \mathcal{A}_{i_2}^{j_1}| \geq 2$. Without loss of generality, we may assume $j_1 = 1$. Let $\mathbf{a}_1^T$ and $\mathbf{a}_2^T$ be two distinct elements of $\mathcal{A}_{i_1}^1 \cap \mathcal{A}_{i_2}^1$, then $\mathsf{desc}(\{(i_1, \mathbf{a}_1)^T, (i_2, \mathbf{a}_2)^T\}) = \mathsf{desc}(\{(i_1, \mathbf{a}_2)^T, (i_2, \mathbf{a}_1)^T\})$, which is a contradiction to the definition of a $\bar{t}$-SC with $t = 2$.

(II) Suppose that there exist $(j_1, j_2) \in \{(1, 2), (1, 3), (1, 4)\}$ and $i_1, i_2, k_1, k_2 \in Q$, where $i_1 \neq i_2$ and $k_1 \neq k_2$, such that $|\mathcal{A}_{i_1,k_1}^{j_1,j_2} \bigcap \mathcal{A}_{i_2,k_2}^{j_1,j_2}| \geq 2$. Without loss of generality, we may assume $(j_1, j_2) = (1, 2)$. Let $\{\mathbf{b}_1^T, \mathbf{b}_2^T\} \subseteq \mathcal{A}_{i_1,k_1}^{1,2} \cap \mathcal{A}_{i_2,k_2}^{1,2}$, then $\mathsf{desc}(\{(i_1, k_1, \mathbf{b}_1)^T, (i_2, k_2, \mathbf{b}_2)^T\}) = \mathsf{desc}(\{(i_1, k_1, \mathbf{b}_2)^T, (i_2, k_2, \mathbf{b}_1)^T\})$, which is a contradiction to the definition of a $\bar{t}$-SC with $t = 2$.

Conversely, suppose that conditions (1) and (2) always hold. We want to show that $\mathcal{C}$ is a $\overline{2}$-SC$(4, M, q)$. Assume that $\mathcal{C}$ is not a $\overline{2}$-SC$(4, M, q)$. Then at least one of the following cases should occur. However, we can prove none of them is possible.

(I) There exist two distinct codewords of $\mathcal{C}$, say $\mathbf{a} = (a_1, a_2, a_3, a_4)^T$ and $\mathbf{b} = (b_1, b_2, b_3, b_4)^T$, such that $\mathsf{desc}(\{\mathbf{a}\}) = \mathsf{desc}(\{\mathbf{b}\})$. Then $a_1 = b_1$, $a_2 = b_2$, $a_3 = b_3$ and $a_4 = b_4$, which implies that $\mathbf{a} = \mathbf{b}$, a contradiction. So this case is impossible.

(II) There exist two distinct codewords of $\mathcal{C}$, say $\mathbf{a} = (a_1, a_2, a_3, a_4)^T$ and $\mathbf{b} = (b_1, b_2, b_3, b_4)^T$, such that $\mathsf{desc}(\{\mathbf{a}, \mathbf{b}\}) = \mathsf{desc}(\{\mathbf{a}\})$. Then $\{a_1, b_1\} = \{a_1\}$, $\{a_2, b_2\} = \{a_2\}$, $\{a_3, b_3\} = \{a_3\}$ and $\{a_4, b_4\} = \{a_4\}$, that is, $a_1 = b_1$, $a_2 = b_2$, $a_3 = b_3$ and $a_4 = b_4$, which implies that $\mathbf{a} = \mathbf{b}$, a contradiction. So this case is also impossible.

(III) There exist three distinct codewords of $\mathcal{C}$, say $\mathbf{a} = (a_1, a_2, a_3, a_4)^T$, $\mathbf{b} = (b_1, b_2, b_3, b_4)^T$ and $\mathbf{c} = (c_1, c_2, c_3, c_4)^T$, such that $\mathsf{desc}(\{\mathbf{a}, \mathbf{b}\}) = \mathsf{desc}(\{\mathbf{c}\})$. Then $\{a_1, b_1\} = \{c_1\}$, $\{a_2, b_2\} = \{c_2\}$, $\{a_3, b_3\} = \{c_3\}$ and $\{a_4, b_4\} = \{c_4\}$, that is, $a_1 = b_1 = c_1$, $a_2 = b_2 = c_2$, $a_3 = b_3 = c_3$ and $a_4 = b_4 = c_4$, which implies that $\mathbf{a} = \mathbf{b} = \mathbf{c}$, a contradiction. So this case is also impossible.

(IV) There exist three distinct codewords of $\mathcal{C}$, say $\mathbf{a} = (a_1, a_2, a_3, a_4)^T$, $\mathbf{b} = (b_1, b_2, b_3, b_4)^T$ and $\mathbf{c} = (c_1, c_2, c_3, c_4)^T$, such that $\mathsf{desc}(\{\mathbf{a}, \mathbf{b}\}) = \mathsf{desc}(\{\mathbf{b}, \mathbf{c}\})$. Then $\{a_1, b_1\} = \{b_1, c_1\}$, $\{a_2, b_2\} = \{b_2, c_2\}$, $\{a_3, b_3\} = \{b_3, c_3\}$ and $\{a_4, b_4\} = \{b_4, c_4\}$, that is, $a_1 = c_1$, $a_2 = c_2$, $a_3 = c_3$ and $a_4 = c_4$, which implies that $\mathbf{a} = \mathbf{c}$, a contradiction. This case is again impossible.

(V) There exist four distinct codewords of $\mathcal{C}$, say $\mathbf{a} = (a_1, a_2, a_3, a_4)^T$, $\mathbf{b} = (b_1, b_2, b_3, b_4)^T$, $\mathbf{c} = (c_1, c_2, c_3, c_4)^T$ and $\mathbf{d} = (d_1, d_2, d_3, d_4)^T$, such that $\mathsf{desc}(\{\mathbf{a}, \mathbf{b}\}) = \mathsf{desc}(\{\mathbf{c}, \mathbf{d}\})$. Then $\{a_1, b_1\} = \{c_1, d_1\}$, $\{a_2, b_2\} = \{c_2, d_2\}$, $\{a_3, b_3\} = \{c_3, d_3\}$ and $\{a_4, b_4\} = \{c_4, d_4\}$. This can be divided into the following subcases:

(1) $\{a_1, b_1\} = \{c_1, d_1\}$:

(11) $a_1 = b_1 = c_1 = d_1$; (12) $a_1 \neq b_1, a_1 = c_1, b_1 = d_1$;
(13) $a_1 \neq b_1, a_1 = d_1, b_1 = c_1$.

(2) $\{a_2, b_2\} = \{c_2, d_2\}$:

(21) $a_2 = b_2 = c_2 = d_2$; (22) $a_2 \neq b_2, a_2 = c_2, b_2 = d_2$;
(23) $a_2 \neq b_2, a_2 = d_2, b_2 = c_2$.

(3) $\{a_3, b_3\} = \{c_3, d_3\}$:

(31) $a_3 = b_3 = c_3 = d_3$; (32) $a_3 \neq b_3, a_3 = c_3, b_3 = d_3$;
(33) $a_3 \neq b_3, a_3 = d_3, b_3 = c_3$.

(4) $\{a_4, b_4\} = \{c_4, d_4\}$:

(41) $a_4 = b_4 = c_4 = d_4$; (42) $a_4 \neq b_4, a_4 = c_4, b_4 = d_4$;
(43) $a_4 \neq b_4, a_4 = d_4, b_4 = c_4$.

So at least one of 81 subcases $\{(1i_1), (2i_2), (3i_3), (4i_4)\}$, $i_1, i_2, i_3, i_4 \in \{1, 2, 3, 4\}$, should occur for $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ and $\mathbf{d}$. It is readily checked that none of these 81 subcases is possible. For example, consider the subcase $\{(11), (21), (32), (43)\}$, that is,

$$\begin{array}{ll} (11)\ a_1 = b_1 = c_1 = d_1; & (21)\ a_2 = b_2 = c_2 = d_2; \\ (32)\ a_3 \neq b_3, a_3 = c_3, b_3 = d_3; & (43)\ a_4 \neq b_4, a_4 = d_4, c_4 = b_4. \end{array}$$

Then $\{(a_1, a_2, a_3)^T, (a_1, a_2, b_3)^T\} \subseteq \mathcal{A}^4_{a_4} \cap \mathcal{A}^4_{b_4}$, a contradiction to the assumption that $|\mathcal{A}^4_{a_4} \cap \mathcal{A}^4_{b_4}| \leq 1$, which means that this subcase is impossible. For another example, consider the subcase $\{(12), (22), (33), (43)\}$, that is,

$$\begin{array}{l} (12)\ a_1 \neq b_1, a_1 = c_1, b_1 = d_1; (22)\ a_2 \neq b_2, a_2 = c_2, b_2 = d_2; \\ (33)\ a_3 \neq b_3, a_3 = d_3, c_3 = b_3;\ (43)\ a_4 \neq b_4, a_4 = d_4, c_4 = b_4. \end{array}$$

Then $\{(a_3, a_4)^T, (b_3, b_4)^T\} \subseteq \mathcal{A}^{1,2}_{a_1,a_2} \cap \mathcal{A}^{1,2}_{b_1,b_2}$, a contradiction to the assumption that $|\mathcal{A}^{1,2}_{a_1,a_2} \cap \mathcal{A}^{1,2}_{b_1,b_2}| \leq 1$, which means that this subcase is impossible.

Therefore, $\mathcal{C}$ is a $\overline{2}$-SC$(4, M, q)$. □

Next, we are going to construct $\overline{2}$-SC$(4, M, q)$s by means of incomplete squares, in which some entries are missing. Let $s \leq q$, and $B_{i_j} = (a_{kx}^{(i_j)})$, $1 \leq j \leq s$, be incomplete squares, where $i_j, k, x, a_{kx}^{(i_j)} \in Q$. For each entry $a_{kx}^{(i_j)} \in Q$ of the s incomplete squares, we construct a codeword $\mathbf{c} = (i_j, k, x, a_{kx}^{(i_j)})^T \in \mathcal{C}$, then we can derive a $(4, M, q)$ code $\mathcal{C}$, where M is the number of nonempty entries of the s incomplete squares.

Lemma 2.3.2 *If there exist s incomplete squares satisfying the following conditions $(a) - (g)$, then there exists a $\overline{2}$-SC$(4, M, q)$, where M is the number of nonempty entries of the s incomplete squares.*

(a) *There exists at most one element in each position of each incomplete square.*

(b) *For any $i, k, x_1 \neq x_2 \in Q$, $a_{kx_1}^{(i)} \neq a_{kx_2}^{(i)}$.*

(c) *For any $i, k_1 \neq k_2, x \in Q$, $a_{k_1x}^{(i)} \neq a_{k_2x}^{(i)}$.*

(d) *For any $i_1 \neq i_2, k, x \in Q$, $a_{kx}^{(i_1)} \neq a_{kx}^{(i_2)}$.*

(e) *For any $i_1 \neq i_2, k_1 \neq k_2 \in Q$, there exists at most one $x \in Q$ such that $a_{k_1x}^{(i_1)} = a_{k_2x}^{(i_2)}$.*

(f) *For any $i_1 \neq i_2, x_1 \neq x_2 \in Q$, there exists at most one $k \in Q$ such that $a_{kx_1}^{(i_1)} = a_{kx_2}^{(i_2)}$.*

(g) *For any $i_1 \neq i_2 \in Q$ and any $(k_1, x_1) \neq (k_2, x_2) \in Q^2$, $(a_{k_1x_1}^{(i_1)}, a_{k_1x_1}^{(i_2)}) \neq (a_{k_2x_2}^{(i_1)}, a_{k_2x_2}^{(i_2)})$.*

Proof: We construct a $(4, M, q)$ code as described above and show it is a $\overline{2}$-SC$(4, M, q)$ by Theorem 2.3.1.

(1) Suppose there exist distinct $i_1, i_2 \in Q$, such that $|\mathcal{A}_{i_1}^1 \bigcap \mathcal{A}_{i_2}^1| \geq 2$. Let $(k, x, y)^T \in \mathcal{A}_{i_1}^1 \bigcap \mathcal{A}_{i_2}^1$. Then $(i_1, k, x, y)^T, (i_2, k, x, y)^T \in \mathcal{C}$, so $a_{kx}^{(i_1)} = a_{kx}^{(i_2)} = y$. This is a contradiction to condition (d).

(2) Suppose there exist distinct $k_1, k_2 \in Q$, such that $|\mathcal{A}_{k_1}^2 \bigcap \mathcal{A}_{k_2}^2| \geq 2$. Let $(i, x, y)^T \in \mathcal{A}_{k_1}^2 \bigcap \mathcal{A}_{k_2}^2$. Then $(i, k_1, x, y)^T, (i, k_2, x, y)^T \in \mathcal{C}$, so $a_{k_1x}^{(i)} = a_{k_2x}^{(i)} = y$. This is a contradiction to condition (c).

(3) Suppose there exist distinct $x_1, x_2 \in Q$, such that $|\mathcal{A}_{x_1}^3 \bigcap \mathcal{A}_{x_2}^3| \geq 2$. Let $(i, k, y)^T \in \mathcal{A}_{x_1}^3 \bigcap \mathcal{A}_{x_2}^3$. Then $(i, k, x_1, y)^T, (i, k, x_2, y)^T \in \mathcal{C}$, so $a_{kx_1}^{(i)} = a_{kx_2}^{(i)} = y$. This is a contradiction to condition (b).

(4) Suppose there exist distinct $y_1, y_2 \in Q$, such that $|\mathcal{A}^4_{y_1} \bigcap \mathcal{A}^4_{y_2}| \geq 2$. Let $(i,k,x)^T \in \mathcal{A}^4_{y_1} \bigcap \mathcal{A}^4_{y_2}$. Then $(i,k,x,y_1)^T, (i,k,x,y_2)^T \in \mathcal{C}$. So there exist two elements y_1 and y_2 in the k-th row and the x-th column of B_i, a contradiction to condition (a).

(5) Suppose there exist $i_1 \neq i_2, k_1 \neq k_2 \in Q$, such that $|\mathcal{A}^{1,2}_{i_1,k_1} \bigcap \mathcal{A}^{1,2}_{i_2,k_2}| \geq 2$. Let $(x_1,y_1)^T \neq (x_2,y_2)^T \in \mathcal{A}^{1,2}_{i_1,k_1} \bigcap \mathcal{A}^{1,2}_{i_2,k_2}$. Then $(i_1,k_1,x_1,y_1)^T, (i_1,k_1,x_2,y_2)^T$, $(i_2,k_2,x_1,y_1)^T, (i_2,k_2,x_2,y_2)^T \in \mathcal{C}$, so $a^{(i_1)}_{k_1x_1} = a^{(i_2)}_{k_2x_1} = y_1$, $a^{(i_1)}_{k_1x_2} = a^{(i_2)}_{k_2x_2} = y_2$.

1) If $x_1 = x_2$, according to $a^{(i_1)}_{k_1x_1} = y_1$ and $a^{(i_1)}_{k_1x_2} = y_2$, we can derive $y_1 = y_2$, which implies $(x_1,y_1)^T = (x_2,y_2)^T$, a contradiction.

2) If $x_1 \neq x_2$, then $a^{(i_1)}_{k_1x_1} = a^{(i_2)}_{k_2x_1} = y_1$ and $a^{(i_1)}_{k_1x_2} = a^{(i_2)}_{k_2x_2} = y_2$, a contradiction to condition (e)

(6) Suppose there exist $i_1 \neq i_2, x_1 \neq x_2 \in Q$, such that $|\mathcal{A}^{1,3}_{i_1,x_1} \bigcap \mathcal{A}^{1,3}_{i_2,x_2}| \geq 2$. Let $(k_1,y_1)^T \neq (k_2,y_2)^T \in \mathcal{A}^{1,3}_{i_1,x_1} \bigcap \mathcal{A}^{1,3}_{i_2,x_2}$. Then $(i_1,k_1,x_1,y_1)^T, (i_1,k_2,x_1,y_2)^T$, $(i_2,k_1,x_2,y_1)^T, (i_2,k_2,x_2,y_2)^T \in \mathcal{C}$, so $a^{(i_1)}_{k_1x_1} = a^{(i_2)}_{k_1x_2} = y_1$, $a^{(i_1)}_{k_2x_1} = a^{(i_2)}_{k_2x_2} = y_2$.

1) If $k_1 = k_2$, according to $a^{(i_1)}_{k_1x_1} = y_1$, $a^{(i_1)}_{k_2x_1} = y_2$, we can derive $y_1 = y_2$, which implies $(k_1,y_1)^T = (k_2,y_2)^T$, a contradiction.

2) If $k_1 \neq k_2$, then $a^{(i_1)}_{k_1x_1} = a^{(i_2)}_{k_1x_2} = y_1$, $a^{(i_1)}_{k_2x_1} = a^{(i_2)}_{k_2x_2} = y_2$, a contradiction to condition (f).

(7) Suppose there exist $i_1 \neq i_2, y_1 \neq y_2 \in Q$, such that $|\mathcal{A}^{1,4}_{i_1,y_1} \bigcap \mathcal{A}^{1,4}_{i_2,y_2}| \geq 2$. Let $(k_1,x_1)^T \neq (k_2,x_2)^T \in \mathcal{A}^{1,4}_{i_1,y_1} \bigcap \mathcal{A}^{1,4}_{i_2,y_2}$. Then $(i_1,k_1,x_1,y_1)^T, (i_1,k_2,x_2,y_1)^T$, $(i_2,k_1,x_1,y_2)^T, (i_2,k_2,x_2,y_2)^T \in \mathcal{C}$, so $(a^{(i_1)}_{k_1x_1}, a^{(i_2)}_{k_1x_1}) = (a^{(i_1)}_{k_2x_2}, a^{(i_2)}_{k_2x_2}) = (y_1,y_2)$, a contradiction to condition (g)

According to Theorem 2.3.1, $\mathcal{C}$ is a $\overline{2}$-SC$(4,M,q)$. This completes the proof. □

Lemma 2.3.3 *There exist $q-2$ incomplete squares satisfying conditions $(a)-(g)$ in Lemma 2.3.2 for any prime power $q > 2$ and $M = (q-2)(q^2-q)$.*

Proof: Let $Q = \mathrm{GF}(q)$. We do the construction as follows. Let

$$B_i = (a^{(i)}_{kx}), \text{ where } a^{(i)}_{kx} = (x-k)i + k,\ x \neq k \in \mathrm{GF}(q),\ i \in \mathrm{GF}(q) \setminus \{0,1\}.$$

Then we check conditions $(a)-(g)$ in Lemma 2.3.2.

(a) Obviously, condition (a) is satisfied.

(b) Suppose there exist $i \in \mathrm{GF}(q) \setminus \{0,1\}$, $k, x_1 \neq x_2 \in \mathrm{GF}(q)$, such that $k \neq x_1, k \neq x_2$, and $a^{(i)}_{kx_1} = a^{(i)}_{kx_2}$. Then $(x_1-k)i+k = (x_2-k)i+k$. So $(x_1-x_2)i = 0$. Since $x_1 \neq x_2, i \neq 0$, then $(x_1-x_2)i \neq 0$. This is a contradiction.

(c) Suppose there exist $i \in \mathrm{GF}(q) \setminus \{0,1\}$, $k_1 \neq k_2, x \in \mathrm{GF}(q)$, such that $k_1 \neq x, k_2 \neq x$, and $a_{k_1x}^{(i)} = a_{k_2x}^{(i)}$. Then $(x-k_1)i + k_1 = (x-k_2)i + k_2$. So $(k_1-k_2)(i-1) = 0$. Since $k_1 \neq k_2, i \neq 1$, then $(k_1-k_2)(i-1) \neq 0$. This is a contradiction.

(d) Suppose there exist $i_1 \neq i_2 \in \mathrm{GF}(q) \setminus \{0,1\}$, $k, x \in \mathrm{GF}(q)$, such that $k \neq x$ and $a_{kx}^{(i_1)} = a_{kx}^{(i_2)}$. Then $(x-k)i_1+k = (x-k)i_2+k$, that is $(x-k)(i_1-i_2) = 0$. Since $x \neq k, i_1 \neq i_2$, then $(x-k)(i_1-i_2) \neq 0$. This is a contradiction.

(e) Suppose there exist $i_1 \neq i_2 \in \mathrm{GF}(q) \setminus \{0,1\}$, $k_1 \neq k_2 \in \mathrm{GF}(q)$, such that there exist $x_1 \neq x_2 \in \mathrm{GF}(q)$ satisfying $k_h \neq x_l, 1 \leq h, l \leq 2$, $a_{k_1x_1}^{(i_1)} = a_{k_2x_1}^{(i_2)}$ and $a_{k_1x_2}^{(i_1)} = a_{k_2x_2}^{(i_2)}$. Then $(x_1-k_1)i_1+k_1 = (x_1-k_2)i_2+k_2$ and $(x_2-k_1)i_1+k_1 = (x_2-k_2)i_2+k_2$, which imply $(x_1-x_2)(i_1-i_2) = 0$. Since $x_1 \neq x_2, i_1 \neq i_2$, then $(x_1-x_2)(i_1-i_2) \neq 0$. This is a contradiction.

(f) Suppose there exist $i_1 \neq i_2 \in \mathrm{GF}(q) \setminus \{0,1\}$, $x_1 \neq x_2 \in \mathrm{GF}(q)$, such that there exist $k_1 \neq k_2 \in \mathrm{GF}(q)$ satisfying $k_h \neq x_l, 1 \leq h, l \leq 2$, $a_{k_1x_1}^{(i_1)} = a_{k_1x_2}^{(i_2)}$ and $a_{k_2x_1}^{(i_1)} = a_{k_2x_2}^{(i_2)}$. Then $(x_1-k_1)i_1+k_1 = (x_2-k_1)i_2+k_1$ and $(x_1-k_2)i_1+k_2 = (x_2-k_2)i_2+k_2$, which imply $(k_1-k_2)(i_1-i_2) = 0$. Since $k_1 \neq k_2, i_1 \neq i_2$, then $(k_1-k_2)(i_1-i_2) \neq 0$. This is a contradiction.

(g) Suppose there exist $i_1 \neq i_2 \in \mathrm{GF}(q) \setminus \{0,1\}$, $(k_1, x_1) \neq (k_2, x_2) \in \mathrm{GF}(q) \times \mathrm{GF}(q)$, such that $k_h \neq x_l, 1 \leq h, l \leq 2$, and $(a_{k_1x_1}^{(i_1)}, a_{k_1x_1}^{(i_2)}) = (a_{k_2x_2}^{(i_1)}, a_{k_2x_2}^{(i_2)})$. Then $a_{k_1x_1}^{(i_1)} = a_{k_2x_2}^{(i_1)}$ and $a_{k_1x_1}^{(i_2)} = a_{k_2x_2}^{(i_2)}$. Then $(x_1-k_1)i_1+k_1 = (x_2-k_2)i_1+k_2$ and $(x_1-k_1)i_2+k_1 = (x_2-k_2)i_2+k_2$, that is, $((x_1-x_2)+(k_2-k_1))i_1 + (k_1-k_2) = 0$ and $((x_1-x_2)+(k_2-k_1))i_2 + (k_1-k_2) = 0$. Let $f(X) = ((x_1-x_2)+(k_2-k_1))X + (k_1-k_2) \in \mathrm{GF}(q)[X]$, then $\deg(f(X)) \leq 1$. But $f(i_1) = f(i_2) = 0$ and $i_1 \neq i_2$, so $f(X) \equiv 0$. Then $(x_1-x_2)+(k_2-k_1) = 0$ and $(k_1-k_2) = 0$. So $k_1 = k_2$ and $x_1 = x_2$, then $(k_1, x_1) = (k_2, x_2)$. This is a contradiction.

This completes the proof. □

Theorem 2.3.4 *There exists a $\overline{2}$-SC$(4, (q-2)(q^2-q), q)$ for any prime power $q > 2$.*

Proof: The result comes from Lemmas 2.3.2 and 2.3.3. □

Applying Theorem 2.1.8 with $n = 4$, we can derive $M_{SC}(\overline{2}, 4, q) \leq q^3 + \frac{q(q-1)}{2}$. The $\overline{2}$-SC$(4, q^3-3q^2+2q, q)$s constructed above are not optimal, but asymptotically optimal, for

$$\lim_{\text{prime } q\to\infty} \frac{(q-2)(q^2-q)}{q^3 + \frac{q(q-1)}{2}} = \lim_{\text{prime } q\to\infty} \frac{2q^3-6q^2+4q}{2q^3+q^2-q} = 1.$$

CHAPTER 3

Strong Separable Codes

As we can see from Theorem 2.1.4, the computational complexity $O(nM^t)$ of algorithm $\texttt{LACCTraceAlg}(R)$ based on t-LACCs (or binary $\overline{t}$-SCs) is not efficient for practical use, where n is the length of the code and M is the number of authorized users. Therefore, it is desirable to find some special SCs with efficient tracing algorithm. This is the main reason that we introduce the new notion of a strong separable code ($\overline{t}$-SSC) in this chapter. In fact, from Theorem 3.1.3, we know that any binary $\overline{t}$-SSC can be used to identify all colluders with computational complexity $O(nM)$ when the number of colluders in the averaging attack is at most t.

In Section 3.1, we introduce the concept of an SSC, and describe a colluder tracing algorithm based on a binary SSC. We also show a concatenation construction for binary SSCs from q-ary SSCs, which makes the study of q-ary SSCs with short length important. In Section 3.2, we discuss the relationships between strong separable codes and other fingerprinting codes. We also derive several infinite series of optimal q-ary $\overline{2}$-SSCs of length 2 from the fact that a q-ary $\overline{2}$-SSC of length 2 is equivalent to a q-ary $\overline{2}$-SC of length 2 in Section 3.2. Finally, combinatorial properties of q-ary $\overline{2}$-SSCs of length 3 are investigated and a construction for q-ary $\overline{2}$-SSCs of length 3 is also presented in Section 3.3.

3.1 Tracing algorithm for strong separable codes

In this section, we first introduce the concept of a strong separable code ($\overline{t}$-SSC), then we present a tracing algorithm based on a binary $\overline{t}$-SSC with computational complexity $O(nM)$, which is more efficient than that of a $\overline{t}$-SC, and finally we describe a concatenation construction for binary SSCs from q-ary SSCs.

Definition 3.1.1 *Let $\mathcal{C}$ be an (n, M, q) code and $t \geq 2$ be an integer. $\mathcal{C}$ is a strong $\overline{t}$-separable code, or $\overline{t}$-SSC(n, M, q), if for any $\mathcal{C}_0 \subseteq \mathcal{C}$, $1 \leq |\mathcal{C}_0| \leq t$, we have $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}' = \mathcal{C}_0$, where $S(\mathcal{C}_0) = \{\mathcal{C}' \subseteq \mathcal{C} \mid \mathrm{desc}(\mathcal{C}') = \mathrm{desc}(\mathcal{C}_0)\}$.*

From the definition above, it is clear that for any $\mathcal{C}' \in S(\mathcal{C}_0)$ and $\mathcal{C}' \neq \mathcal{C}_0$, we have $\mathcal{C}_0 \subseteq \mathcal{C}'$ and $|\mathcal{C}'| \geq t + 1$.

Example 3.1.2 Consider the following $(3,4,2)$ code $\mathcal{C}$:

$$\begin{array}{cc} & \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \mathcal{C} = & \left(\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array}\right) \end{array}$$

Then

$$\begin{aligned}
\mathsf{desc}(\{\mathbf{c}_1\}) &= \{0\} \times \{0\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_2\}) &= \{1\} \times \{0\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_3\}) &= \{0\} \times \{1\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_4\}) &= \{0\} \times \{0\} \times \{1\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) &= \{0,1\} \times \{0\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_3\}) &= \{0\} \times \{0,1\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_4\}) &= \{0\} \times \{0\} \times \{0,1\}, \\
\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3\}) &= \{0,1\} \times \{0,1\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_4\}) &= \{0,1\} \times \{0\} \times \{0,1\}, \\
\mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_4\}) &= \{0\} \times \{0,1\} \times \{0,1\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}) &= \{0,1\} \times \{0,1\} \times \{0\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4\}) &= \{0,1\} \times \{0\} \times \{0,1\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4\}) &= \{0\} \times \{0,1\} \times \{0,1\}, \\
\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}) &= \{0,1\} \times \{0,1\} \times \{0,1\}, \\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}) &= \{0,1\} \times \{0,1\} \times \{0,1\}.
\end{aligned}$$

It is easy to check that

$$\begin{aligned}
&S(\{\mathbf{c}_1\}) = \{\{\mathbf{c}_1\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_1\})} \mathcal{C}' = \{\mathbf{c}_1\}, \\
&S(\{\mathbf{c}_2\}) = \{\{\mathbf{c}_2\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_2\})} \mathcal{C}' = \{\mathbf{c}_2\}, \\
&S(\{\mathbf{c}_3\}) = \{\{\mathbf{c}_3\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_3\})} \mathcal{C}' = \{\mathbf{c}_3\}, \\
&S(\{\mathbf{c}_4\}) = \{\{\mathbf{c}_4\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_4\})} \mathcal{C}' = \{\mathbf{c}_4\}, \\
&S(\{\mathbf{c}_1, \mathbf{c}_2\}) = \{\{\mathbf{c}_1, \mathbf{c}_2\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_1, \mathbf{c}_2\})} \mathcal{C}' = \{\mathbf{c}_1, \mathbf{c}_2\}, \\
&S(\{\mathbf{c}_1, \mathbf{c}_3\}) = \{\{\mathbf{c}_1, \mathbf{c}_3\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_1, \mathbf{c}_3\})} \mathcal{C}' = \{\mathbf{c}_1, \mathbf{c}_3\}, \\
&S(\{\mathbf{c}_1, \mathbf{c}_4\}) = \{\{\mathbf{c}_1, \mathbf{c}_4\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_1, \mathbf{c}_4\})} \mathcal{C}' = \{\mathbf{c}_1, \mathbf{c}_4\}, \\
&S(\{\mathbf{c}_2, \mathbf{c}_3\}) = \{\{\mathbf{c}_2, \mathbf{c}_3\}, \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_2, \mathbf{c}_3\})} \mathcal{C}' = \{\mathbf{c}_2, \mathbf{c}_3\}, \\
&S(\{\mathbf{c}_2, \mathbf{c}_4\}) = \{\{\mathbf{c}_2, \mathbf{c}_4\}, \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_2, \mathbf{c}_4\})} \mathcal{C}' = \{\mathbf{c}_2, \mathbf{c}_4\}, \\
&S(\{\mathbf{c}_3, \mathbf{c}_4\}) = \{\{\mathbf{c}_3, \mathbf{c}_4\}, \{\mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4\}\} \text{ and } \textstyle\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_3, \mathbf{c}_4\})} \mathcal{C}' = \{\mathbf{c}_3, \mathbf{c}_4\}.
\end{aligned}$$

So the code $\mathcal{C}$ is a $\overline{2}$-SSC$(3,4,2)$.

We now pay our attention to the tracing algorithm based on a binary strong separable code.

Theorem 3.1.3 *Under the assumption that the number of colluders in the averaging attack is at most t, any $\overline{t}$-SSC$(n, M, 2)$ can be used to identify all the colluders with computational complexity $O(nM)$ by applying Algorithm 3.1.*

Proof: Let $\mathcal{C}$ be the $\overline{t}$-SSC$(n, M, 2)$, and R be the descendant code derived from the detection statistics $\mathbf{T}$. Then by applying Algorithm 3.1, one can identify all the colluders. The computational complexity is clearly $O(nM)$.

According to Algorithm 3.1, by deleting all columns $\{\mathbf{c} \in \mathcal{C} \mid \exists\, 1 \le i \le n, R(i) = \{1\}, \mathbf{c}(i) = 0, \text{ or } R(i) = \{0\}, \mathbf{c}(i) = 1\}$, we obtain a sub-matrix $\mathcal{C}_L$ of $\mathcal{C}$. Suppose that $C_0 = \{u_1, u_2, \ldots, u_r\}$, $1 \le r \le t$, is the set of colluders, and the codeword $\mathbf{c}_i$ is assigned to the colluder u_i, $1 \le i \le r$, and $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_r\}$. It is not difficult to see that $\mathcal{C}_0 \subseteq \mathcal{C}_L$. According to the definition of a $\overline{t}$-SSC, we have $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}' = \mathcal{C}_0 \neq \emptyset$, where $S(\mathcal{C}_0) = \{\mathcal{C}' \subseteq \mathcal{C} \mid \mathsf{desc}(\mathcal{C}') = \mathsf{desc}(\mathcal{C}_0) = R\}$. We prove this theorem in three steps.

(1) $\mathcal{C}_L \in S(\mathcal{C}_0)$, that is, $\mathsf{desc}(\mathcal{C}_L) = R$. For any $1 \le j \le n$, we consider the following cases.

(1.1) $R(j) = \{1\}$. For any $\mathbf{c} \in \mathcal{C}_L$, $\mathbf{c}(j) = 1$ according to the processes deriving $\mathcal{C}_L$. So $\mathcal{C}_L(j) = \{1\} = R(j)$.

(1.2) $R(j) = \{0\}$. For any $\mathbf{c} \in \mathcal{C}_L$, $\mathbf{c}(j) = 0$ according to the processes deriving $\mathcal{C}_L$. So $\mathcal{C}_L(j) = \{0\} = R(j)$.

(1.3) $R(j) = \{0, 1\}$. Since $\mathsf{desc}(\mathcal{C}_0) = R$, we know that there exist $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_0 \subseteq \mathcal{C}_L$ such that $\mathbf{c}_1(j) = 0$ and $\mathbf{c}_2(j) = 1$, respectively. This implies $\mathcal{C}_L(j) = \{0, 1\} = R(j)$.

According to (1.1)-(1.3) above, for any $1 \le j \le n$, we have $\mathcal{C}_L(j) = R(j)$, which implies $\mathsf{desc}(\mathcal{C}_L) = R$.

(2) We want to show that for any $\mathbf{x} \in \mathcal{C}_0 = \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}'$, there exists $1 \le j \le n$, such that $\mathbf{x}(j) = 1$ and $\mathbf{c}(j) = 0$ for any $\mathbf{c} \in \mathcal{C}_L \setminus \{\mathbf{x}\}$, or $\mathbf{x}(j) = 0$ and $\mathbf{c}(j) = 1$ for any $\mathbf{c} \in \mathcal{C}_L \setminus \{\mathbf{x}\}$. Assume not. Then for any $1 \le j \le n$, $\mathbf{x}(j) = 1$ implies that there exists $\mathbf{c}_1 \in \mathcal{C}_L \setminus \{\mathbf{x}\}$ such that $\mathbf{c}_1(j) = 1$, and $\mathbf{x}(j) = 0$ implies that there exists $\mathbf{c}_2 \in \mathcal{C}_L \setminus \{\mathbf{x}\}$ such that $\mathbf{c}_2(j) = 0$. Then we have $\mathsf{desc}(\mathcal{C}_L) = \mathsf{desc}(\mathcal{C}_L \setminus \{\mathbf{x}\})$. Since $\mathcal{C}_L \in S(\mathcal{C}_0)$ by (1), we can have $\mathcal{C}_L \setminus \{\mathbf{x}\} \in S(\mathcal{C}_0)$, and $\mathbf{x} \notin \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}'$, a contradiction.

(3) At last, according to Algorithm 3.1 and (2), it suffices to show that any user u assigned with a codeword $\mathbf{x} \in \mathcal{C}_0 = \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}'$ is a colluder. Assume that u is not a colluder. Then for any $\mathcal{C}' \in S(\mathcal{C}_0)$, we have $\mathcal{C}' \setminus \{\mathbf{x}\} \in S(\mathcal{C}_0)$, which implies $\mathbf{x} \notin \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}'$, a contradiction.

Algorithm 3.1: `SSCTraceAlg`(R)

```
Define $J_a$, $J_o$ to be the sets of indices where $R(j) = \{1\}$, $R(j) = \{0\}$,
respectively, and $\mathbf{J_a} = (\mathbf{J_a}(1), \ldots, \mathbf{J_a}(|J_a|))^T$, $\mathbf{J_o} = (\mathbf{J_o}(1), \ldots, \mathbf{J_o}(|J_o|))^T$ to
be the vector representing $R$'s coordinates where $R(j) = \{1\}$ and $R(j) = \{0\}$,
respectively;
$\mathbf{\Phi} = \mathbf{1}$;
$U_a = \emptyset$;
$U_o = \emptyset$;
$U = \emptyset$;
for $k = 1$ to $|J_a|$ do
    $j = \mathbf{J_a}(k)$;
    define $\mathbf{e}_j$ to be the $j$th row of $\mathcal{C}$;
    $\mathbf{\Phi} = \mathbf{\Phi} \cdot \mathbf{e}_j$;
for $k = 1$ to $|J_o|$ do
    $j = \mathbf{J_o}(k)$;
    $\mathbf{\Phi} = \mathbf{\Phi} \cdot \overline{\mathbf{e}}_j$;
for $k = 1$ to $n$ do
    $\mathbf{\Phi}_a = \mathbf{\Phi} \cdot \mathbf{e}_k$;
    $\mathbf{\Phi}_o = \mathbf{\Phi} \cdot \overline{\mathbf{e}}_k$;
    for $i = 1$ to $M$ do
        if $\mathbf{\Phi}_a(i) = 1$ then
            $U_a = \{i\} \bigcup U_a$;
    if $|U_a| = 1$ then
        $U = U \bigcup U_a$;
    for $i = 1$ to $M$ do
        if $\mathbf{\Phi}_o(i) = 1$ then
            $U_o = \{i\} \bigcup U_o$;
    if $|U_o| = 1$ then
        $U = U \bigcup U_o$;
if $|U| \leq t$ then
    output $U$;
else
    output "The set of colluders has size at least $t + 1$."
```

This completes the proof. □

Note that any user holding $\mathbf{c} \in C_L \setminus C_0$ is not a colluder. In fact, if such $\mathbf{c}$ corresponds to a colluder, then according to the hypothesis in Theorem 3.1.3, we have $|C_0 \bigcup \{\mathbf{c}\}| \leq t$. In this case, $\mathsf{desc}(C_0 \bigcup \{\mathbf{c}\}) = \mathsf{desc}(C_0)$. Then $C_0 \in S(C_0 \bigcup \{\mathbf{c}\})$, while $C_0 \bigcup \{\mathbf{c}\} \not\subseteq C_0$, a contradiction to the definition of $\overline{t}$-SSC.

A close look at the proof also shows an important fact that this tracing algorithm is also valid for any linear attack, because the detection statistics $\mathbf{T}(i)$, $1 \leq i \leq n$, for $\mathcal{C}_0$ possess the whole information on $\mathcal{C}_0$.

At the end of this section, we show a concatenation construction for binary $\overline{t}$-SSCs from q-ary $\overline{t}$-SSCs, which makes the study of q-ary $\overline{t}$-SSCs with short length, say $n = 2, 3$, important.

Lemma 3.1.4 *If there exists a $\overline{t}$-SSC(n, M, q), then there exists a $\overline{t}$-SSC$(nq, M, 2)$.*

Proof: Let $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_M\}$ be a $\overline{t}$-SSC(n, M, q) on $Q = \{0, 1, \ldots, q-1\}$, and $E = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_q\}$, where $\mathbf{e}_i$ is the i-th identity vector of length q. Let $f\colon\ Q \to E$ be a bijective mapping such that $f(i) = \mathbf{e}_{i+1}$. For any codeword $\mathbf{c} = (\mathbf{c}(1), \mathbf{c}(2), \ldots, \mathbf{c}(n))^T \in \mathcal{C}$, we define $f(\mathbf{c}) = (f(\mathbf{c}(1)), f(\mathbf{c}(2)), \ldots, f(\mathbf{c}(n)))^T$. Obviously, $f(\mathbf{c})$ is a binary vector of length nq. We define a new $(nq, M, 2)$ code $\mathcal{F} = \{f(\mathbf{c}_1), f(\mathbf{c}_2), \ldots, f(\mathbf{c}_M)\}$. We can show that $\mathcal{F}$ is a $\overline{t}$-SSC.

For any $\mathcal{F}_0 \subseteq \mathcal{F}$, $|\mathcal{F}_0| \leq t$, we only need to show that for any $\mathcal{F}_1 \subseteq \mathcal{F}$, $\mathsf{desc}(\mathcal{F}_0) = \mathsf{desc}(\mathcal{F}_1)$ implies $\mathcal{F}_0 \subseteq \mathcal{F}_1$. Suppose $\mathcal{F}_0, \mathcal{F}_1$ correspond to two codeword sets $\mathcal{C}_0, \mathcal{C}_1 \subseteq \mathcal{C}$, respectively, such that $|\mathcal{C}_0| = |\mathcal{F}_0| \leq t$, where $\mathcal{F}_0 = \{f(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_0\}$ and $\mathcal{F}_1 = \{f(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_1\}$. Since $\mathrm{desc}(\mathcal{F}_0) = \mathrm{desc}(\mathcal{F}_1)$, we have $\mathrm{desc}(\mathcal{C}_0) = \mathrm{desc}(\mathcal{C}_1)$. Then $\mathcal{C}_0 \subseteq \mathcal{C}_1$, because $\mathcal{C}$ is a $\overline{t}$-SSC(n, M, q). So, $\mathcal{F}_0 \subseteq \mathcal{F}_1$.

This completes the proof. □

3.2 Relationships between strong separable codes and other codes

In this section, we investigate the relationships between strong separable codes and other fingerprinting codes, and derive several infinite series of optimal q-ary $\overline{2}$-SSCs of length 2.

Recall that, in any $\overline{t}$-SSC(n, M, q) $\mathcal{C}$, for any $\mathcal{C}_0 \subseteq \mathcal{C}$, $1 \leq |\mathcal{C}_0| \leq t$, and any $\mathcal{C}' \in S(\mathcal{C}_0)$, $\mathcal{C}' \neq \mathcal{C}_0$, we have $\mathcal{C}_0 \subseteq \mathcal{C}'$ and $|\mathcal{C}'| \geq t+1$. In other words, there are no distinct subsets $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$ with $1 \leq |\mathcal{C}_1| \leq t$, $1 \leq |\mathcal{C}_2| \leq t$, such that $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$. This implies the following lemma.

Lemma 3.2.1 *Any $\overline{t}$-SSC(n, M, q) is a $\overline{t}$-SC(n, M, q).*

The following example shows that the converse of Lemma 3.2.1 does not always hold.

Example 3.2.2 *Consider the following* $(3,5,2)$ *code* $\mathcal{C}$*:*

$$\mathcal{C} = \begin{array}{c} \begin{array}{ccccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 \end{array} \\ \left(\begin{array}{ccccc} 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 1 \end{array} \right) \end{array}$$

We can directly check that $\mathcal{C}$ *is a* $\overline{2}$*-SC*$(3,5,2)$*. Now, we show that* $\mathcal{C}$ *is not a* $\overline{2}$*-SSC. Let* $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_5\}$ *and* $\mathcal{C}^{'} = \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$*, then* $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(\mathcal{C}^{'})$*, while* $\mathcal{C}_0 \nsubseteq \mathcal{C}^{'}$*. This implies that* $\mathcal{C}$ *is not a* $\overline{2}$*-SSC*$(3,5,2)$*.*

However, the following result shows that a $\overline{2}$-SSC$(2,M,q)$ is always a $\overline{2}$-SC$(2,M,q)$.

Theorem 3.2.3 *Let* $\mathcal{C}$ *be a* $(2,M,q)$ *code. Then* $\mathcal{C}$ *is a* $\overline{2}$*-SSC*$(2,M,q)$ *if and only if it is a* $\overline{2}$*-SC*$(2,M,q)$*.*

Proof: By Lemma 3.2.1, it suffices to consider the sufficiency. Let $\mathcal{C}$ be a $\overline{2}$-SC$(2,M,q)$. Assume that $\mathcal{C}$ is not a $\overline{2}$-SSC$(2,M,q)$. Then there exist $\mathcal{C}_0, \mathcal{C}^{'} \subseteq \mathcal{C}$, $|\mathcal{C}_0| \leq 2$, such that $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(\mathcal{C}^{'})$ but $\mathcal{C}_0 \nsubseteq \mathcal{C}^{'}$. If $|\mathcal{C}_0| = 1$, then it is clear that $\mathcal{C}_0 = \mathcal{C}^{'}$, a contradiction. So $|\mathcal{C}_0| = 2$. Let $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\}$, $\mathbf{c}_i = (a_i, b_i)^T$, where $i = 1, 2$. Since $\mathcal{C}$ is a $\overline{2}$-SC$(2,M,q)$ and $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(\mathcal{C}^{'})$, we have $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ and $|\mathcal{C}^{'}| \geq 3$. We now consider the Hamming distance $d(\mathbf{c}_1, \mathbf{c}_2)$ of $\mathbf{c}_1$ and $\mathbf{c}_2$, where the Hamming distance of $\mathbf{c}_1$ and $\mathbf{c}_2$ is the number of positions where $\mathbf{c}_1$ and $\mathbf{c}_2$ have different symbols.

(1) If $d(\mathbf{c}_1, \mathbf{c}_2) = 1$, without loss of generality, we may assume $a_1 = a_2$, $b_1 \neq b_2$. Then $|\mathsf{desc}(\mathcal{C}_0)| = 2$. So $|\mathcal{C}^{'}| \leq |\mathsf{desc}(\mathcal{C}_0)| = 2$, a contradiction.

(2) If $d(\mathbf{c}_1, \mathbf{c}_2) = 2$, then $a_1 \neq a_2$, $b_1 \neq b_2$, and $\mathsf{desc}(\mathcal{C}_0) = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, where $\mathbf{c}_3 = (a_1, b_2)^T$ and $\mathbf{c}_4 = (a_2, b_1)^T$. Then $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| \leq 3$. Otherwise, if $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| = 4$, i.e., $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, then $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_4\})$, a contradiction to the definition of a $\overline{2}$-SC. Since $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ and $|\mathcal{C}^{'}| \geq 3$, we have $|\mathcal{C}^{'}| = 3$. So we may assume, without loss of generality, that $\mathcal{C}^{'} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, which implies $\mathcal{C}_0 \subseteq \mathcal{C}^{'}$, a contradiction.

This completes the proof. □

Therefore, the optimal SCs in Theorem 2.2.22 are, in fact, optimal SSCs from the equivalence stated in Theorem 3.2.3.

Corollary 3.2.4 *Let* $k \geq 2$ *be a prime power. Then there is an optimal* $\overline{2}$*-SSC*$(2, M,$ $q)$ *for any* $q \in \{k^2-1, k^2+k-2, k^2+k-1, k^2+k, k^2+k+1\}$*.*

Finally, we consider the relationship between strong separable codes and frameproof codes defined below.

Definition 3.2.5 *Let $\mathcal{C}$ be an (n, M, q) code and $t \geq 2$ be an integer. $\mathcal{C}$ is a t-frameproof code, or t-FPC(n, M, q), if for any $\mathcal{C}' \subseteq \mathcal{C}$ such that $|\mathcal{C}'| \leq t$, we have $\mathsf{desc}(\mathcal{C}') \bigcap \mathcal{C} = \mathcal{C}'$, that is, for any $\mathbf{c} = (\mathbf{c}(1), \ldots, \mathbf{c}(n))^T \in \mathcal{C} \setminus \mathcal{C}'$, there is at least one coordinate i, $1 \leq i \leq n$, such that $\mathbf{c}(i) \notin \mathcal{C}'(i)$.*

Intuitively, an (n, M, q) code is a t-FPC if no coalition of size at most t can frame another user not in the coalition in generic digital fingerprinting. Frameproof codes were first introduced to prevent a coalition from framing a user not in the coalition in [12], but were widely considered as having no traceability for generic digital data (see for example [48]). However, Cheng and Miao [17] showed that frameproof codes actually have traceability for multimedia contents. This greatly strengthens the importance of frameproof codes in fingerprinting.

Lemma 3.2.6 ([17]) *Under the assumption that the number of colluders in the averaging attack is at most t, any t-FPC$(n, M, 2)$ can be used to identify all the colluders with computational complexity $O(nM)$ by using Algorithm 3.2 described in* [17].

Lemma 3.2.7 *Any t-FPC(n, M, q) is a $\overline{t}$-SSC(n, M, q).*

Proof: Let $\mathcal{C}$ be a t-FPC(n, M, q). We are going to show that for any $\mathcal{C}_0 \subseteq \mathcal{C}$, $|\mathcal{C}_0| \leq t$, $S(\mathcal{C}_0) = \{\mathcal{C}^{'} \subseteq \mathcal{C} \mid \mathsf{desc}(\mathcal{C}^{'}) = \mathsf{desc}(\mathcal{C}_0)\} = \{\mathcal{C}_0\}$. Assume that there exists $\mathcal{C}^{'} \in S(\mathcal{C}_0)$ such that $\mathcal{C}^{'} \neq \mathcal{C}_0$.

(1) If $|\mathcal{C}^{'}| \geq |\mathcal{C}_0|$, then there exists $\mathbf{c} \in \mathcal{C}^{'} \subseteq \mathcal{C}$ such that $\mathbf{c} \notin \mathcal{C}_0$. Since $\mathsf{desc}(\mathcal{C}^{'}) = \mathsf{desc}(\mathcal{C}_0)$, we have $\mathbf{c} \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, while $|\mathcal{C}_0| \leq t$, a contradiction to the definition of a t-FPC.

(2) If $|\mathcal{C}^{'}| < |\mathcal{C}_0| \leq t$, then there exists $\mathbf{c} \in \mathcal{C}_0 \subseteq \mathcal{C}$ such that $\mathbf{c} \notin \mathcal{C}^{'}$. Since $\mathsf{desc}(\mathcal{C}^{'}) = \mathsf{desc}(\mathcal{C}_0)$, we have $\mathbf{c} \in \mathsf{desc}(\mathcal{C}^{'}) \bigcap \mathcal{C}$, while $|\mathcal{C}^{'}| < t$, a contradiction to the definition of a t-FPC.

According to the discussions above, we have $S(\mathcal{C}_0) = \{\mathcal{C}_0\}$. This implies that $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} = \mathcal{C}_0$. □

The following example shows that the converse of Lemma 3.2.7 does not always hold.

Example 3.2.8 Consider the following $(3, 4, 2)$ code $\mathcal{C}$:

$$\begin{array}{cc} & \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \mathcal{C} = & \left(\begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right) \end{array}$$

From Example 3.1.2, we know that $\mathcal{C}$ is a $\overline{2}$-SSC$(3, 4, 2)$. Now, we show that $\mathcal{C}$ is not a 2-FPC. For $\mathcal{C}^{'} = \{\mathbf{c}_2, \mathbf{c}_3\}$, $\mathsf{desc}(\mathcal{C}') \bigcap \mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\} \neq \mathcal{C}'$. This is a contradiction to the definition of a 2-FPC.

Algorithm 3.2: `FPCIdenAlg`(R)

```
Define $J_a$, $J_o$ to be the sets of indices where $R(j) = \{1\}$, $R(j) = \{0\}$, respectively, and $\mathbf{J_a} = (\mathbf{J_a}(1), \ldots, \mathbf{J_a}(|J_a|))^T$, $\mathbf{J_o} = (\mathbf{J_o}(1), \ldots, \mathbf{J_o}(|J_o|))^T$ to be the vector representing $R$'s coordinates where $R(j) = \{1\}$ and $R(j) = \{0\}$, respectively;
$\mathbf{\Phi} = \mathbf{1}$;
$U_1 = \emptyset$;
for $k = 1$ to $|J_a|$ do
    $j = \mathbf{J_a}(k)$;
    define $\mathbf{e}_j$ to be the $j$th row of $\mathcal{C}$;
    $\mathbf{\Phi} = \mathbf{\Phi} \cdot \mathbf{e}_j$;
for $i = 1$ to $M$ do
    if $\mathbf{\Phi}(i) = 1$ then
        $U_1 = \{i\} \bigcup U_1$;
$\mathbf{\Phi} = \mathbf{1}$;
$U_2 = \emptyset$;
for $k = 1$ to $|J_o|$ do
    $j = \mathbf{J_o}(k)$;
    $\mathbf{\Phi} = \mathbf{\Phi} \cdot \bar{\mathbf{e}}_j$;
for $i = 1$ to $M$ do
    if $\mathbf{\Phi}(i) = 1$ then
        $U_2 = \{i\} \bigcup U_2$;
$U = U_1 \bigcap U_2$;
if $|U| \leq t$ then
    output $U$;
else
    output "The set of colluders has size at least $t + 1$."
```

We would like to make some remarks here. The multimedia fingerprinting scheme based on a t-FPC$(n, M, 2)$ can have at most $r \cdot 2^{\lceil \frac{n}{t} \rceil} + O(2^{\lceil \frac{n}{t} \rceil - 1})$ authorized users, where r is the unique integer such that $r \in \{1, 2, \ldots, t\}$ and $r = n \pmod t$ [10]. In the case of large t, this number of users is too small to be of practical use. We can use $\overline{t}$-SSCs to overcome this shortcoming. On one hand, we know that $\overline{t}$-SSC$(n, M, 2)$s have the same traceability as t-FPC$(n, M, 2)$s from Theorem 3.1.3 and Lemma 3.2.6. On the other hand, $\overline{t}$-SSC$(n, M, 2)$s have weaker requirements than t-FPC$(n, M, 2)$s from Lemma 3.2.7. Therefore, we can say that in some sense, the significance of $\overline{t}$-SSC$(n, M, 2)$s relies on their maximum size.

3.3 Constructions for $\overline{2}$-SSCs of length 3

In this section, we investigate combinatorial properties of q-ary $\overline{2}$-SSCs of length 3, and construct an infinite series of such codes.

From Lemma 3.2.1, we know that any $\overline{2}$-SSC$(3, M, q)$ is a $\overline{2}$-SC$(3, M, q)$. Therefore, we can start from $\overline{2}$-SC$(3, M, q)$s to investigate $\overline{2}$-SSC$(3, M, q)$s. At first, we derive forbidden configurations of a $\overline{2}$-SSC$(3, M, q)$.

Lemma 3.3.1 *Let $\mathcal{C}$ be a $\overline{2}$-SC$(3, M, q)$. If there exist $\mathcal{C}_0, \mathcal{C}' \subseteq \mathcal{C}$, $|\mathcal{C}_0| \leq 2$ such that $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(\mathcal{C}')$ and $\mathcal{C}_0 \nsubseteq \mathcal{C}'$, then $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\}$ and the Hamming distance $d(\mathbf{c}_1, \mathbf{c}_2) \notin \{0, 1, 2\}$.*

Proof: If $|\mathcal{C}_0| = 1$, then it is clear that $\mathcal{C}_0 = \mathcal{C}'$, a contradiction. So $|\mathcal{C}_0| = 2$. Let $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\}$, $\mathbf{c}_i = (a_i, b_i, e_i)$, $\mathbf{c}_1 \neq \mathbf{c_2}$. Since $\mathcal{C}$ is a $\overline{2}$-SC$(3, M, q)$ and $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(\mathcal{C}')$, we have $\mathcal{C}' \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ and $|\mathcal{C}'| \geq 3$.

(1) If $d(\mathbf{c}_1, \mathbf{c}_2) = 1$, we may assume, without loss of generality, that $a_1 = a_2$, $b_1 = b_2$, $e_1 \neq e_2$. Then $|\mathsf{desc}(\mathcal{C}_0)| = 2$. So $|\mathcal{C}'| \leq |\mathsf{desc}(\mathcal{C}_0)| = 2$, a contradiction.

(2) If $d(\mathbf{c}_1, \mathbf{c}_2) = 2$, we may assume, without loss of generality, $a_1 = a_2$, $b_1 \neq b_2$, $e_1 \neq e_2$. Then $\mathsf{desc}(\mathcal{C}_0) = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, where $\mathbf{c}_3 = (a_1, b_1, e_2)^T$ and $\mathbf{c}_4 = (a_1, b_2, e_1)^T$. Then $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| \leq 3$. Otherwise, if $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| = 4$, i.e., $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, then $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_4\})$, a contradiction to the definition of a $\overline{2}$-SC. Since $\mathcal{C}' \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ and $|\mathcal{C}'| \geq 3$, we have $|\mathcal{C}'| = 3$. So, we may assume, without loss of generality, that $\mathcal{C}' = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$. This implies $\mathcal{C}_0 \subseteq \mathcal{C}'$, a contradiction.

This completes the proof. □

Lemma 3.3.2 *Let $\mathcal{C}$ be a $\overline{2}$-SC$(3, M, q)$. If there exist $\mathcal{C}_0, \mathcal{C}' \subseteq \mathcal{C}$, $|\mathcal{C}_0| \leq 2$, such that $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(\mathcal{C}')$ and $\mathcal{C}_0 \nsubseteq \mathcal{C}'$, then $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of one of the following* *four types:*

$$\begin{array}{cc} \textit{Type } \mathbf{I}\text{:} & \textit{Type } \mathbf{II}\text{:} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_1 \\ b_1 & b_2 & b_1 & b_2 \\ e_1 & e_2 & e_2 & e_1 \end{array}\right), & \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_1 \\ e_1 & e_2 & e_2 & e_1 \end{array}\right), \end{array}$$

$$\begin{array}{cc} \textit{Type } \mathbf{III}\text{:} & \textit{Type } \mathbf{IV}\text{:} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_2 \\ b_1 & b_2 & b_2 & b_1 \\ e_1 & e_2 & e_1 & e_1 \end{array}\right), & \left(\begin{array}{cc|ccc} a_1 & a_2 & a_1 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 & b_1 \\ e_1 & e_2 & e_2 & e_1 & e_1 \end{array}\right), \end{array}$$

where $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\}$*,* $\mathbf{c}_i = (a_i, b_i, e_i)$*,* $i = 1, 2$*, and* $a_1 \neq a_2$*,* $b_1 \neq b_2$*,* $e_1 \neq e_2$*.*

Proof: According to Lemma 3.3.1, we can only have $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\}$, $\mathbf{c}_i = (a_i, b_i, e_i)^T$, where $i = 1, 2$, $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$. Then $\mathsf{desc}(\mathcal{C}_0) = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6, \mathbf{c}_7, \mathbf{c}_8\}$, where $\mathbf{c}_3 = (a_1, b_1, e_2)^T$, $\mathbf{c}_4 = (a_1, b_2, e_1)^T$, $\mathbf{c}_5 = (a_2, b_1, e_1)^T$, $\mathbf{c}_6 = (a_2, b_2, e_1)^T$, $\mathbf{c}_7 = (a_2, b_1, e_2)^T$, $\mathbf{c}_8 = (a_1, b_2, e_2)^T$.

$$\mathsf{desc}(\mathcal{C}_0) = \begin{array}{c} \begin{array}{cccccccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 & \mathbf{c}_7 & \mathbf{c}_8 \end{array} \\ \left(\begin{array}{cc|cccccc} a_1 & a_2 & a_1 & a_1 & a_2 & a_2 & a_2 & a_1 \\ b_1 & b_2 & b_1 & b_2 & b_1 & b_2 & b_1 & b_2 \\ e_1 & e_2 & e_2 & e_1 & e_1 & e_1 & e_2 & e_2 \end{array}\right) \end{array}$$

Let $B_i = \{\mathbf{c}_{i+2}, \mathbf{c}_{i+5}\}$, where $1 \leq i \leq 3$. Then for any $1 \leq i \leq 3$, we have $B_i \nsubseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. Otherwise, $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(B_i)$, a contradiction to the definition of a $\overline{2}$-SC. Since $\mathcal{C}$ is a $\overline{2}$-SC$(3, M, q)$ and $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(\mathcal{C}^{'})$, we have $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ and $|\mathcal{C}^{'}| \geq 3$.

If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \mathcal{C}_0$, then $\mathcal{C}^{'} \subseteq \mathcal{C}_0$, and thus $|\mathcal{C}^{'}| \leq |\mathcal{C}_0| = 2$, a contradiction. So $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ contains at least one of the words $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6, \mathbf{c}_7, \mathbf{c}_8$. Without loss of generality, we may assume $\mathbf{c}_3 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. Then $\mathbf{c}_6 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, since $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ and $|\mathcal{C}^{'}| \geq 3$, we have $\mathcal{C}^{'} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, which implies $\mathcal{C}_0 \subseteq \mathcal{C}^{'}$, a contradiction. So $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ should contain at least one of the words $\mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_7, \mathbf{c}_8$.

(1) If $\mathbf{c}_4 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, then $\mathbf{c}_7 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. We also have $\mathbf{c}_8 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, otherwise, $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_8\}) = \mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_4\})$, a contradiction. So, if $\mathbf{c}_5 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, then $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of Type **I**, and if $\mathbf{c}_5 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, then $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of Type **IV**.

(2) If $\mathbf{c}_5 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, then $\mathbf{c}_8 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. We also have $\mathbf{c}_7 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, otherwise, $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_7\}) = \mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_5\})$, a contradiction. So, if $\mathbf{c}_4 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, then $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of Type **II**, and if $\mathbf{c}_4 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, then $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of Type **IV**.

(3) If $\mathbf{c}_7 \in \mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$, then $\mathbf{c}_4 \notin \mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$. Also, $\mathbf{c}_5 \notin \mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$, otherwise, $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_7\}) = \mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_5\})$, a contradiction. We further have $\mathbf{c}_8 \notin \mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$, otherwise, $\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3\}) = \mathsf{desc}(\{\mathbf{c}_7, \mathbf{c}_8\})$, a contradiction. So, in this case, $\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_7\}$.

$$\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C} = \begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_7 \end{array} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_1 \\ e_1 & e_2 & e_2 & e_2 \end{array}\right) \end{array}$$

If $\mathbf{c}_1 \notin \mathcal{C}^{'}$ (or $\mathbf{c}_2 \notin \mathcal{C}^{'}$), then $e_1 \notin \mathcal{C}^{'}(3)$ (or $b_2 \notin \mathcal{C}^{'}(2)$), which implies $\mathsf{desc}(\mathcal{C}^{'}) \neq \mathsf{desc}(\mathcal{C}_0)$. Hence $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}^{'}$, which implies $\mathcal{C}_0 \subseteq \mathcal{C}^{'}$, a contradiction. So this case is impossible.

(4) If $\mathbf{c}_8 \in \mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$, then $\mathbf{c}_5 \notin \mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$. Also, $\mathbf{c}_4 \notin \mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$, otherwise, $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_8\}) = \mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_4\})$, a contradiction. We further have $\mathbf{c}_7 \notin \mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$, otherwise, $\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3\}) = \mathsf{desc}(\{\mathbf{c}_7, \mathbf{c}_8\})$, a contradiction. So, in this case, $\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_8\}$.

$$\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C} = \begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_8 \end{array} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_1 \\ b_1 & b_2 & b_1 & b_2 \\ e_1 & e_2 & e_2 & e_2 \end{array}\right) \end{array}$$

If $\mathbf{c}_1 \notin \mathcal{C}^{'}$ (or $\mathbf{c}_2 \notin \mathcal{C}^{'}$), then $e_1 \notin \mathcal{C}^{'}(3)$ (or $a_2 \notin \mathcal{C}^{'}(1)$), which implies $\mathsf{desc}(\mathcal{C}^{'}) \neq \mathsf{desc}(\mathcal{C}_0)$. Hence $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}^{'}$, which implies $\mathcal{C}_0 \subseteq \mathcal{C}^{'}$, a contradiction. So this case is impossible.

This completes the proof. □

Theorem 3.3.3 *Let $\mathcal{C}$ be a $\overline{2}$-SC$(3, M, q)$. Then $\mathcal{C}$ is a $\overline{2}$-SSC$(3, M, q)$ if and only if for any $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}$, where $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$, we have that $\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$ is not of one of the following four types:*

$$\begin{array}{c} \textit{Type } \mathbf{I}\textit{:} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_1 \\ b_1 & b_2 & b_1 & b_2 \\ e_1 & e_2 & e_2 & e_1 \end{array}\right), \end{array} \quad \begin{array}{c} \textit{Type } \mathbf{II}\textit{:} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_1 \\ e_1 & e_2 & e_2 & e_1 \end{array}\right), \end{array}$$

$$\begin{array}{c} \textit{Type } \mathbf{III:} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_2 \\ b_1 & b_2 & b_2 & b_1 \\ e_1 & e_2 & e_1 & e_1 \end{array}\right), \end{array} \quad \begin{array}{c} \textit{Type } \mathbf{IV:} \\ \left(\begin{array}{cc|ccc} a_1 & a_2 & a_1 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 & b_1 \\ e_1 & e_2 & e_2 & e_1 & e_1 \end{array}\right). \end{array}$$

Proof: Suppose that $\mathcal{C}$ is a $\overline{2}$-SSC$(3, M, q)$. Assume that there exists $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}$, where $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$, such that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of one of the four types. For convenience, let $\mathbf{c}_3 = (a_1, b_1, e_2)^T$, $\mathbf{c}_4 = (a_1, b_2, e_1)^T$, $\mathbf{c}_5 = (a_2, b_1, e_1)^T$.

(1) If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of type **I**, then $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\})$, while $\{\mathbf{c}_1, \mathbf{c}_2\} \nsubseteq \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, a contradiction to the definition of a $\overline{2}$-SSC. So this case is impossible.

(2) If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of type **II**, then $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_5\})$, while $\{\mathbf{c}_1, \mathbf{c}_2\} \nsubseteq \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_5\}$, a contradiction to the definition of a $\overline{2}$-SSC. So this case is impossible.

(3) If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of type **III**, then $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_4, \mathbf{c}_5\})$, while $\{\mathbf{c}_1, \mathbf{c}_2\} \nsubseteq \{\mathbf{c}_2, \mathbf{c}_4, \mathbf{c}_5\}$, a contradiction to the definition of a $\overline{2}$-SSC. So this case is impossible.

(4) If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of type **IV**, then $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5\})$, while $\{\mathbf{c}_1, \mathbf{c}_2\} \nsubseteq \{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5\}$, a contradiction to the definition of a $\overline{2}$-SSC. So this case is impossible.

So, $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is not of one of the four types described above.

Conversely, suppose that $\mathcal{C}$ is a $\overline{2}$-SC$(3, M, q)$, and for any $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}$, where $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$, we have that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is not of one of the four types. If $\mathcal{C}$ is not a $\overline{2}$-SSC$(3, M, q)$, then there exist $\mathcal{C}_1 \subseteq \mathcal{C}$, $|\mathcal{C}_1| \leq 2$, and $\mathcal{C}' \in S(\mathcal{C}_1) = \{\mathcal{C}' \subseteq \mathcal{C} \mid \mathsf{desc}(\mathcal{C}') = \mathsf{desc}(\mathcal{C}_1)\}$, such that $\mathcal{C}_1 \nsubseteq \mathcal{C}'$. According to Lemma 3.3.2, $\mathcal{C}_1 = \{\mathbf{c}'_1, \mathbf{c}'_2\} = \{(a'_1, b'_1, e'_1)^T, (a'_2, b'_2, e'_2)^T\} \subseteq \mathcal{C}$, where $a'_1 \neq a'_2$, $b'_1 \neq b'_2$, and $e'_1 \neq e'_2$, such that $\mathsf{desc}(\mathcal{C}_1) \bigcap \mathcal{C}$ is of one of the four types, a contradiction. So $\mathcal{C}$ is a $\overline{2}$-SSC$(3, M, q)$. □

Now, we pay our attention to the construction of $\overline{2}$-SSCs of length 3 via the discussion above. In order to describe our construction, we need s new elements $\infty_i \notin Z_{q-s}$, $i \in \{0, 1, \ldots, s-1\} \subseteq Z_{q-s}$, such that for any $g \in Z_{q-s}$ and any $i \in \{0, 1, \ldots, s-1\}$,

$$g + \infty_i = \infty_i + g = g \cdot \infty_i = \infty_i \cdot g = \infty_i.$$

Lemma 3.3.4 ([16]) *A* $(3, M, q)$ *code is a* $\overline{2}$-*SC*$(3, M, q)$ *on* Q *if and only if* $|\mathcal{A}^j_{g_1} \bigcap \mathcal{A}^j_{g_2}| \leq 1$ *holds for any* $1 \leq j \leq 3$, *and any distinct* $g_1, g_2 \in Q$.

Lemma 3.3.5 *Let* $\mathcal{C}$ *be a* $(3, M, q)$ *code on* Q. *If for any* $\mathcal{C}_0 \subseteq \mathcal{C}$, $|\mathcal{C}_0| \leq 2$, *we have* $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| \leq 3$, *then* $\mathcal{C}$ *is a* $\overline{2}$-*SSC*$(3, M, q)$.

Proof: We first show that $\mathcal{C}$ is a $\overline{2}$-SC$(3, M, q)$. Assume not. According to Lemma 3.3.4, we may assume, without loss of generality, that there exist two distinct $g_1, g_2 \in Q$ such that $|\mathcal{A}^1_{g_1} \bigcap \mathcal{A}^1_{g_2}| \geq 2$. Suppose $(b_1, e_1)^T, (b_2, e_2)^T \in \mathcal{A}^1_{g_1} \bigcap \mathcal{A}^1_{g_2}$, where $(b_1, e_1)^T \neq (b_2, e_2)^T$. Then $(g_1, b_1, e_1)^T, (g_2, b_1, e_1)^T, (g_1, b_2, e_2)^T, (g_2, b_2, e_2)^T \in \mathcal{C}$, which imply $|\mathsf{desc}(\{(g_1,b_1,e_1)^T,(g_2,b_2,e_2)^T\})\bigcap\mathcal{C}|\geq 4$, a contradiction to the hypothesis. So $\mathcal{C}$ is a $\overline{2}$-SC$(3,M,q)$. Next, we prove it is in fact a $\overline{2}$-SSC. Since for any $\mathcal{C}_0\subseteq\mathcal{C}$, $|\mathcal{C}_0|\leq 2$, $|\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}|\leq 3$ always holds, we know that $\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}$ can not be of any of the four types mentioned in Theorem 3.3.3. So $\mathcal{C}$ is a $\overline{2}$-SSC$(3,M,q)$ from Theorem 3.3.3. □

Based on Lemma 3.3.5, we can construct $\overline{2}$-SSCs as follows.

Lemma 3.3.6 *Suppose that q is a positive integer, s is a non-negative integer, where $0\leq s\leq\frac{q}{2}$ and $q-s$ is odd. Then there exists a $\overline{2}$-SSC$(3,q^2+sq-2s^2,q)$.*

Proof: Since $q-s$ is odd and $0\leq s\leq\frac{q}{2}$, we can construct a code $\mathcal{C}$ on $Q=\{\infty_0,\infty_1,\ldots,\infty_{s-1}\}\bigcup Z_{q-s}$ as follows. Let

$$M_s=\begin{pmatrix}0&0&\cdots&0\\0&1&\cdots&q-s-1\\0&2&\cdots&2(q-s-1)\end{pmatrix},\qquad M_i=\begin{pmatrix}\infty_i&i&0\\0&\infty_i&i\\i&0&\infty_i\end{pmatrix},$$

$i\in\{0,1,\ldots,s-1\}$. Define $\mathcal{D}_j=\{\mathbf{c}+g\mid \mathbf{c}\in M_j, g\in Z_{q-s}\}$, where $0\leq j\leq s$, and $\mathcal{C}=\bigcup_{j=0}^{s}\mathcal{D}_j$. Then $\mathcal{C}$ is a $(3,q^2+sq-2s^2,q)$ code on Q.

According to Lemma 3.3.5, in order to prove that $\mathcal{C}$ is a $\overline{2}$-SSC$(3,q^2+sq-2s^2,q)$, it suffices to check that $|\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}|\leq 3$ always holds for any $\mathcal{C}_0\subseteq\mathcal{C}$, $|\mathcal{C}_0|\leq 2$. We prove this lemma in two steps.

(1) At first, we will prove that for any distinct $g_1,g_2\in Q$, $(g_1,g_2)\in\{\infty_0,\infty_1,\ldots,\infty_{s-1}\}^2\bigcup Z_{q-s}^2$, $|\mathcal{A}_{g_1}^i\bigcap\mathcal{A}_{g_2}^i|=0$ always holds for any $1\leq i\leq 3$. We only need to consider the case $|\mathcal{A}_{g_1}^1\bigcap\mathcal{A}_{g_2}^1|=0$, because we can consider the other two cases in a similar way.

(1.1) For any $0\leq i<j\leq s-1$, we have $\mathcal{A}_{\infty_i}^1\bigcap\mathcal{A}_{\infty_j}^1=\emptyset$. Assume that $(b,e)^T\in\mathcal{A}_{\infty_i}^1\bigcap\mathcal{A}_{\infty_j}^1$. Then there exist $b_1,b_2\in Z_{q-s}$, such that $(b,e)^T=(b_1,b_1+i)^T=(b_2,b_2+j)^T$, which implies $b_1=b_2=b$, and $i=j$, a contradiction.

(1.2) For any distinct $i,j\in Z_{q-s}$, we have $\mathcal{A}_i^1\bigcap\mathcal{A}_j^1=\emptyset$. Assume that $(b,e)^T\in\mathcal{A}_i^1\bigcap\mathcal{A}_j^1$.

(1.2.A) If there exists $0\leq k\leq s-1$ such that $b=\infty_k$, then $(b,e)^T=(\infty_k,i-k)^T=(\infty_k,j-k)^T$, which implies $i=j$, a contradiction.

(1.2.B) If there exists $0\leq k\leq s-1$ such that $e=\infty_k$, then $(b,e)^T=(i+k,\infty_k)^T=(j+k,\infty_k)^T$, which implies $i=j$, a contradiction.

(1.2.C) If $b,e\notin\{\infty_0,\infty_1,\ldots,\infty_{s-1}\}$, then there exist $b_1,b_2\in Z_{q-s}$, such that $(b,e)^T=(i+b_1,i+2b_1)^T=(j+b_2,j+2b_2)^T$. Hence $i+b_1=j+b_2$ and $i+2b_1=j+2b_2$, which imply $b_1=b_2$ and $i=j$, a contradiction.

(2) According to (1), we know that for any distinct $g_1,g_2\in Q$ and any $1\leq i\leq 3$, $|\mathcal{A}_{g_1}^i\bigcap\mathcal{A}_{g_2}^i|\geq 1$ implies $(g_1,g_2)\in Z_{q-s}\times\{\infty_0,\infty_1,\ldots,\infty_{s-1}\}$. We are going to show that $|\mathsf{desc}(\mathcal{C}_0)\bigcap\mathcal{C}|\leq 3$ always holds for any $\mathcal{C}_0\subseteq\mathcal{C}$, $|\mathcal{C}_0|\leq 2$. If $|\mathcal{C}_0|=1$, then it is

clear that $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| = |\mathcal{C}_0| = 1$. Now, we consider the case $|\mathcal{C}_0| = 2$. Suppose $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}$, where $\mathbf{c}_1 \neq \mathbf{c}_2$. Consider the Hamming distance of $\mathbf{c}_1$ and $\mathbf{c}_2$.

(2.1) If $d(\mathbf{c}_1, \mathbf{c}_2) = 1$, then it is clear that $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| = |\mathcal{C}_0| = 2$.

(2.2) If $d(\mathbf{c}_1, \mathbf{c}_2) = 2$, without loss of generality, we may assume that $a_1 = a_2$, $b_1 \neq b_2$, $e_1 \neq e_2$. Then $\mathsf{desc}(\mathcal{C}_0) = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, where $\mathbf{c}_3 = (a_1, b_1, e_2)^T$ and $\mathbf{c}_4 = (a_1, b_2, e_1)^T$.

$$\mathsf{desc}(\mathcal{C}_0) = \begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \left(\begin{array}{cc|cc} a_1 & a_1 & a_1 & a_1 \\ b_1 & b_2 & b_1 & b_2 \\ e_1 & e_2 & e_2 & e_1 \end{array}\right) \end{array}$$

Assume that $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| = 4$, i.e. $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$. Then $|\mathcal{A}^3_{e_1} \bigcap \mathcal{A}^3_{e_2}| \geq 1$, which implies that exactly one of e_1 and e_2 is ∞_i for some $0 \leq i \leq s-1$.

(2.2.A) If $e_1 = \infty_i$, then $\mathbf{c}_1 = \mathbf{c}_4$, which implies $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| \leq 3$, a contradiction.

(2.2.B) If $e_2 = \infty_i$, then $\mathbf{c}_2 = \mathbf{c}_3$, which implies $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| \leq 3$, a contradiction.

So, if $d(\mathbf{c}_1, \mathbf{c}_2) = 2$, $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| \leq 3$ always holds.

(2.3) If $d(\mathbf{c}_1, \mathbf{c}_2) = 3$, then $a_1 \neq a_2$, $b_1 \neq b_2$, $e_1 \neq e_2$, and $\mathsf{desc}(\mathcal{C}_0) = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6, \mathbf{c}_7, \mathbf{c}_8\}$, where $\mathbf{c}_3 = (a_1, b_1, e_2)^T$, $\mathbf{c}_4 = (a_1, b_2, e_1)^T$, $\mathbf{c}_5 = (a_2, b_1, e_1)^T$, $\mathbf{c}_6 = (a_2, b_2, e_1)^T$, $\mathbf{c}_7 = (a_2, b_1, e_2)^T$, $\mathbf{c}_8 = (a_1, b_2, e_2)^T$.

$$\mathsf{desc}(\mathcal{C}_0) = \begin{array}{c} \begin{array}{cccccccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 & \mathbf{c}_7 & \mathbf{c}_8 \end{array} \\ \left(\begin{array}{cc|cccccc} a_1 & a_2 & a_1 & a_1 & a_2 & a_2 & a_2 & a_1 \\ b_1 & b_2 & b_1 & b_2 & b_1 & b_2 & b_1 & b_2 \\ e_1 & e_2 & e_2 & e_1 & e_1 & e_1 & e_2 & e_2 \end{array}\right) \end{array}$$

We are going to show that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ contains at most one element of the set $B = \{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6, \mathbf{c}_7, \mathbf{c}_8\}$. Assume not. Then there exist two elements $\mathbf{c}', \mathbf{c}''$ of B contained in $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, where $\{\mathbf{c}', \mathbf{c}''\} \in \{\{\mathbf{c}_3, \mathbf{c}_4\}, \{\mathbf{c}_3, \mathbf{c}_5\}, \{\mathbf{c}_3, \mathbf{c}_6\}, \{\mathbf{c}_3, \mathbf{c}_7\}, \{\mathbf{c}_3, \mathbf{c}_8\}, \{\mathbf{c}_4, \mathbf{c}_5\}, \{\mathbf{c}_4, \mathbf{c}_6\}, \{\mathbf{c}_4, \mathbf{c}_7\}, \{\mathbf{c}_4, \mathbf{c}_8\}, \{\mathbf{c}_5, \mathbf{c}_6\}, \{\mathbf{c}_5, \mathbf{c}_7\}, \{\mathbf{c}_5, \mathbf{c}_8\}, \{\mathbf{c}_6, \mathbf{c}_7\}, \{\mathbf{c}_6, \mathbf{c}_8\}, \{\mathbf{c}_7, \mathbf{c}_8\}\}$. However, we can prove none of them is possible.

(2.3.A) If $\{\mathbf{c}', \mathbf{c}''\} = \{\mathbf{c}_3, \mathbf{c}_4\}$, then we have $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$.

$$\begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_1 \\ b_1 & b_2 & b_1 & b_2 \\ e_1 & e_2 & e_2 & e_1 \end{array}\right) \end{array}$$

Then $|\mathcal{A}^3_{e_1} \bigcap \mathcal{A}^3_{e_2}| \geq 1$ (from $\mathbf{c}_1$ and $\mathbf{c}_3$) and $|\mathcal{A}^2_{b_1} \bigcap \mathcal{A}^2_{b_2}| \geq 1$ (from $\mathbf{c}_1$ and $\mathbf{c}_4$). Hence there exist $0 \leq i, j \leq s-1$ such that exactly one of e_1 and e_2 is ∞_i, and exactly one of b_1 and b_2 is ∞_j.

(2.3.A.a) If $e_1 = \infty_i$, then $\infty_j \notin \{b_1, b_2\}$ from $\mathbf{c}_1$ and $\mathbf{c}_4$, a contradiction. So, this case is impossible.

(2.3.A.b) If $e_2 = \infty_i$, then $\infty_j \notin \{b_1, b_2\}$ from $\mathbf{c}_2$ and $\mathbf{c}_3$, a contradiction. So, this case is impossible.

Similarly, we can know that it is impossible for $\{\mathbf{c}', \mathbf{c}''\} \in \{\{\mathbf{c}_3, \mathbf{c}_5\}, \{\mathbf{c}_4, \mathbf{c}_5\}, \{\mathbf{c}_6, \mathbf{c}_7\}, \{\mathbf{c}_6, \mathbf{c}_8\}, \{\mathbf{c}_7, \mathbf{c}_8\}\}$.

(2.3.B) If $\{\mathbf{c}', \mathbf{c}''\} = \{\mathbf{c}_3, \mathbf{c}_6\}$, then we have $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_6\} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$.

$$\begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_6 \end{array} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 \\ e_1 & e_2 & e_2 & e_1 \end{array}\right) \end{array}$$

Then $|\mathcal{A}^3_{e_1} \bigcap \mathcal{A}^3_{e_2}| \geq 1$ (from $\mathbf{c}_1$ and $\mathbf{c}_3$). Hence, without loss of generality, we may assume that $e_1 \in Z_{q-s}$ and there exists $0 \leq i \leq s-1$ such that $e_2 = \infty_i$. Then we can derive that $a_1, a_2, b_1 = a_1 + i, b_2 = a_2 + i \in Z_{q-s}$, which imply $\mathbf{c}_1, \mathbf{c}_6 \in \mathcal{D}_s$. So we can derive $e_1 = a_1 + 2i = a_2 + 2i$, which implies $a_1 = a_2$, a contradiction. So this case is impossible.

Similarly, it is impossible that $\{\mathbf{c}', \mathbf{c}''\} \in \{\{\mathbf{c}_4, \mathbf{c}_7\}, \{\mathbf{c}_5, \mathbf{c}_8\}\}$.

(2.3.C) If $\{\mathbf{c}', \mathbf{c}''\} = \{\mathbf{c}_3, \mathbf{c}_7\}$, then we have $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_7\} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$.

$$\begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_7 \end{array} \\ \left(\begin{array}{cc|cc} a_1 & a_2 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_1 \\ e_1 & e_2 & e_2 & e_2 \end{array}\right) \end{array}$$

Then $|\mathcal{A}^3_{e_1} \bigcap \mathcal{A}^3_{e_2}| \geq 1$ (from $\mathbf{c}_1$ and $\mathbf{c}_3$), $|\mathcal{A}^2_{b_1} \bigcap \mathcal{A}^2_{b_2}| \geq 1$ (from $\mathbf{c}_2$ and $\mathbf{c}_7$), and $|\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}| \geq 1$ (from $\mathbf{c}_3$ and $\mathbf{c}_7$). Hence there exists $0 \leq i, j, k \leq s-1$ such that exactly one of e_1 and e_2 is ∞_i, and $\infty_j \in \{b_1, b_2\}$, $\infty_k \in \{a_1, a_2\}$. Then at least one of $(a_1, b_1, e_1)^T$ and $(a_2, b_2, e_2)^T$ contains at least two components from $\{\infty_0, \infty_1, \ldots, \infty_{s-1}\}$, a contradiction. So this case is impossible.

Similarly, it is impossible that $\{\mathbf{c}', \mathbf{c}''\} \in \{\{\mathbf{c}_3, \mathbf{c}_8\}, \{\mathbf{c}_4, \mathbf{c}_6\}, \{\mathbf{c}_4, \mathbf{c}_8\}, \{\mathbf{c}_5, \mathbf{c}_6\}, \{\mathbf{c}_5, \mathbf{c}_7\}\}$.

The conclusion then comes from Lemma 3.3.5. □

Theorem 3.3.7 *There exists a* $\overline{2}$*-SSC*$(3, \frac{1}{8}(9q^2 - w^2), q)$ *for any positive integer* q*, with* m *being the residue of* q *modulo* 8*, and*

$$w = \begin{cases} 4 - m, & \textit{if} \ \ m \equiv 0 \pmod 4, \\ \min\{m, 8-m\}, & \textit{otherwise.} \end{cases}$$

Proof: According to Lemma 3.3.6, there exists a $\overline{2}$-SSC$(3, q^2 + sq - 2s^2, q)$ for any positive integer q, where $0 \leq s \leq \frac{q}{2}$, and $q - s$ is odd. Let $q = 8r + m$, where r is a non-negative integer, and $f(s) = q^2 + sq - 2s^2 = -2(s - \frac{q}{4})^2 + \frac{9}{8}q^2$. Now, we are going to find the maximum value of $f(s)$, where $0 \le s \le \frac{q}{2}$ and $q - s$ is odd.

(1) If $m = 0$, then q is even. Since $\frac{q}{4} = 2r$ is even, $s = 2r - 1 = \frac{q-4}{4}$ is odd, we can know $q - s$ is odd, and $f(\frac{q-4}{4}) = \frac{1}{8}(9q^2 - 4^2)$ is the maximum value of $f(s)$.

(2) If $m = 1$, then q is odd and $\frac{q}{4} = 2r + \frac{1}{4}$. Since $s = 2r = \frac{q-1}{4}$ is even, we can know $q - s$ is odd, and $f(\frac{q-1}{4}) = \frac{1}{8}(9q^2 - 1)$ is the maximum value of $f(s)$.

(3) If $m = 2$, then q is even and $\frac{q}{4} = 2r + \frac{2}{4}$. Since $s = 2r + 1 = \frac{q+2}{4}$ is odd, we can know $q - s$ is odd, and $f(\frac{q+2}{4}) = \frac{1}{8}(9q^2 - 2^2)$ is the maximum value of $f(s)$.

(4) If $m = 3$, then q is odd and $\frac{q}{4} = 2r + \frac{3}{4}$. Since $s = 2r = \frac{q-3}{4}$ is even, we can know $q - s$ is odd, and $f(\frac{q-3}{4}) = \frac{1}{8}(9q^2 - 3^2)$ is the maximum value of $f(s)$.

(5) If $m = 4$, then q is even. Since $s = 2r + 1 = \frac{q}{4}$ is odd, we can know $q - s$ is odd, and $f(\frac{q}{4}) = \frac{9}{8}q^2$ is the maximum value of $f(s)$.

(6) If $m = 5$, then q is odd and $\frac{q}{4} = 2r + \frac{5}{4}$. Since $s = 2r + 2 = \frac{q+3}{4}$ is even, we can know $q - s$ is odd, and $f(\frac{q+3}{4}) = \frac{1}{8}(9q^2 - 3^2)$ is the maximum value of $f(s)$.

(7) If $m = 6$, then q is even and $\frac{q}{4} = 2r + \frac{6}{4}$. Since $s = 2r + 1 = \frac{q-2}{4}$ is odd, we can know $q - s$ is odd, and $f(\frac{q-2}{4}) = \frac{1}{8}(9q^2 - 2^2)$ is the maximum value of $f(s)$.

(8) If $m = 7$, then q is odd and $\frac{q}{4} = 2r + \frac{7}{4}$. Since $s = 2r + 2 = \frac{q+1}{4}$ is even, we can know $q - s$ is odd, and $f(\frac{q+1}{4}) = \frac{1}{8}(9q^2 - 1)$ is the maximum value of $f(s)$.

We can summarize the results obtained in (1)-(8) into the following table, from which the conclusion comes.

m	w	s	$f(s)$
0	4	$\frac{1}{4}(q-4)$	$\frac{1}{8}(9q^2 - 4^2)$
1	1	$\frac{1}{4}(q-1)$	$\frac{1}{8}(9q^2 - 1^2)$
2	2	$\frac{1}{4}(q+2)$	$\frac{1}{8}(9q^2 - 2^2)$
3	3	$\frac{1}{4}(q-3)$	$\frac{1}{8}(9q^2 - 3^2)$
4	0	$\frac{q}{4}$	$\frac{9}{8}q^2$
5	3	$\frac{1}{4}(q+3)$	$\frac{1}{8}(9q^2 - 3^2)$
6	2	$\frac{1}{4}(q-2)$	$\frac{1}{8}(9q^2 - 2^2)$
7	1	$\frac{1}{4}(q+1)$	$\frac{1}{8}(9q^2 - 1^2)$

□

As is well-known, for any 2-FPC$(3, M, q)$, we have $M \le q^2$ (see for example [6]). Theorem 3.3.7 shows that there is an infinite series of $\overline{2}$-SSC$(3, M', q)$s which have more than 12.5% codewords than 2-FPC$(3, M, q)$s could have.

Chapter 4

Multimedia Identifiable Parent Property Codes

In Chapter 2, we know that any binary $\bar{t}$-SC can be used to identify all colluders when the number of colluders in the averaging attack is at most t. However, in most cases, the number of codewords in a $\bar{t}$-SC which is corresponding to the number of authorized users is still too small to be of practical use. Meanwhile, guaranteeing exact identification of at least one member of the pirate coalition of size at most t would bring enough pressure to bear on malicious authorized users to give up their attempts at collusion.

In this chapter, we introduce a new anti-collusion code called multimedia identifiable parent property code (t-MIPPC) to resist the averaging attack on multimedia contents in a fingerprinting system with number of users beyond a $\bar{t}$-SC could provide. Although t-MIPPCs can not be used to identify all the colluders when the size of the coalition is at most t, nevertheless they can be used to identify at least one colluder, thereby helping stop the proliferation of the fraudulent content in digital marketplace.

In Section 4.1, we introduce the notion of an MIPPC, describe a colluder tracing algorithm based on a binary MIPPC, and show a concatenation construction for binary MIPPCs from q-ary MIPPCs. In Section 4.2, some upper bounds on the size of an MIPPC are derived. We also investigate combinatorial properties of a 3-MIPPC of length 2, characterize such a code in terms of a bipartite graph, and derive a tight upper bound on a 3-MIPPC of length 2 in Section 4.2. In Section 4.3, we characterize a 3-MIPPC of length 2 in terms of a generalized packing, and construct several infinite series of (asymptotically) optimal 3-MIPPCs of length 2.

4.1 Tracing algorithm for multimedia identifiable parent property codes

In this section, we first introduce the notion of a multimedia identifiable parent property code (MIPPC). We then show a tracing algorithm based on this new code, and present a concatenation construction for binary MIPPCs from q-ary MIPPCs.

Definition 4.1.1 *Let $\mathcal{C}$ be an (n, M, q) code, and for any $R \subseteq \mathcal{C}(1) \times \mathcal{C}(2) \times \cdots \times \mathcal{C}(n)$, define the set of parent sets of R as*

$$\mathcal{P}_t(R) = \{\mathcal{C}' \subseteq \mathcal{C} \mid |\mathcal{C}'| \leq t, R = \mathsf{desc}(\mathcal{C}')\}.$$

We say that $\mathcal{C}$ is a code with the identifiable parent property (IPP) for multimedia fingerprinting, or a multimedia IPP code, denoted t-MIPPC(n, M, q), if

$$\bigcap_{\mathcal{C}' \in \mathcal{P}_t(R)} \mathcal{C}' \neq \emptyset$$

is satisfied for any $R \subseteq \mathcal{C}(1) \times \mathcal{C}(2) \times \cdots \times \mathcal{C}(n)$ with $\mathcal{P}_t(R) \neq \emptyset$.

Intuitively, $\mathcal{P}_t(R)$ consists of all the sub-codes of $\mathcal{C}$ with size at most t that could have produced all the words in R, and an (n, M, q) code $\mathcal{C}$ is a t-MIPPC(n, M, q) if the following condition is satisfied: even if there are distinct sub-codes of $\mathcal{C}$, each of size at most t, could produce the same set R of words, we can track down at least one parent of R which is contained in each parent set of R. In fact, any codeword in $\bigcap_{\mathcal{C}' \in \mathcal{P}_t(R)} \mathcal{C}'$ is a parent of R.

Example 4.1.2 Consider the following $(3, 4, 2)$ code $\mathcal{C}$:

$$\mathcal{C} = \begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \begin{pmatrix} 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix} \end{array}$$

Obviously

$$\mathcal{C}(1) \times \mathcal{C}(2) \times \mathcal{C}(3) = \{0, 1\} \times \{0, 1\} \times \{0, 1\}.$$

There are exactly two cases satisfying $|\mathcal{P}_3(R)| \geq 2$, that is, $R = \{1\} \times \{0, 1\} \times \{0, 1\}, \{0, 1\} \times \{0, 1\} \times \{0, 1\}$. In the first case,

$$\mathcal{P}_3(\{1\} \times \{0, 1\} \times \{0, 1\}) = \{\{\mathbf{c}_3, \mathbf{c}_4\}, \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}\},$$

and

$$\{\mathbf{c}_3, \mathbf{c}_4\} \bigcap \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\} = \{\mathbf{c}_3, \mathbf{c}_4\} \neq \emptyset.$$

In the second case,

$$\mathcal{P}_3(\{0, 1\} \times \{0, 1\} \times \{0, 1\}) = \{\{\mathbf{c}_1, \mathbf{c}_2\}, \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}, \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4\}, \{\mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4\}\},$$

and

$$\{\mathbf{c}_1, \mathbf{c}_2\} \bigcap \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\} \bigcap \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4\} \bigcap \{\mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4\} = \{\mathbf{c}_1\} \neq \emptyset.$$

So the code $\mathcal{C}$ is a 3-MIPPC$(3, 4, 2)$

MIPPCs are a variation of IPP codes, which were introduced for the purpose of protecting copyrighted digital contents, and a generalization of separable codes. The notion of an IPP code was first introduced in a special case in [32], investigated in full generality in [2, 4, 5, 8, 46, 53], and surveyed in [9].

In Definition 4.1.1, if R is set to be a singleton set $\{\mathbf{d}\}$, and the set of parent sets be modified as

$$\mathcal{P}_t(R) = \{\mathcal{C}^{'} \subseteq \mathcal{C} \mid |\mathcal{C}^{'}| \leq t, \mathbf{d} \in \mathsf{desc}(\mathcal{C}^{'})\},$$

then we obtain a t-IPP code, while if we require that $|\mathcal{P}_t(R)| = 1$ for any $R \subseteq \mathcal{C}(1) \times \mathcal{C}(2) \times \cdots \times \mathcal{C}(n)$ with $\mathcal{P}_t(R) \neq \emptyset$, then we obtain a $\overline{t}$-separable code.

Lemma 4.1.3 *Any $\overline{t}$-SC(n, M, q) is a $\overline{t}$-MIPPC(n, M, q).*

Using the tracing algorithm `MIPPCTraceAlg`(R) described in Theorem 4.1.5, we know that by means of a binary MIPPC, we can capture a set $R \subseteq \mathcal{C}(1) \times \cdots \times \mathcal{C}(n)$ in the multimedia scenario instead of an element $\mathbf{d} \in R$ in the generic digital scenario, and although binary t-MIPPCs can not identify all malicious users as binary $\overline{t}$-separable codes do when the size of the coalition is at most t, they can identify, as IPP codes do in the generic digital scenario [3, 32], at least one such malicious authorized user, thereby helping stop the proliferation of the fraudulent content in digital marketplace.

Therefore, we can say that in some sense, the significance of t-MIPPCs relies on their maximum sizes. For $t = 2$, we will show in Lemma 4.1.4 that a t-MIPPC(n, M, q) is in fact a $\overline{t}$-SC(n, M, q), so they have the same maximum size. For $t > 2$, the maximum size of a $\overline{t}$-SC(n, M, q) is $O(q^{\lceil n/(t-1) \rceil})$ (see [16]), while the maximum size of a t-MIPPC(n, M, q) will be shown in Theorem 4.2.2 to be $O(q^{(t+1)n/(2t)})$, except for the case that t is even and n is odd, where the value is $O(q^{((t+1)n+1)/(2t)})$. This is a significant improvement on the number of codewords, which makes the notion of MIPPCs useful.

Lemma 4.1.4 *Let $\mathcal{C}$ be an (n, M, q) code. Then $\mathcal{C}$ is a 2-MIPPC(n, M, q) if and only if it is a $\overline{2}$-SC(n, M, q).*

Proof: From Lemma 4.1.3, we only need to consider its necessity. Assume that $\mathcal{C}$ is a 2-MIPPC(n, M, q) such that $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$, $|\mathcal{C}_1| \leq 2$, $|\mathcal{C}_2| \leq 2$, $\mathcal{C}_1 \neq \mathcal{C}_2$, and $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$. Then $\mathcal{C}_1 \bigcap \mathcal{C}_2 \neq \emptyset$. Let $\mathbf{a} \in \mathcal{C}_1 \bigcap \mathcal{C}_2$. There are two cases to be considered.

(1) $\mathcal{C}_1 = \{\mathbf{a}\}$, $\mathcal{C}_2 = \{\mathbf{a}, \mathbf{b}\}$: Since $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$, we have $\mathbf{a} = \mathbf{b}$, which implies $\mathcal{C}_1 = \mathcal{C}_2$.

(2) $\mathcal{C}_1 = \{\mathbf{a}, \mathbf{b}\}$, $\mathcal{C}_2 = \{\mathbf{a}, \mathbf{c}\}$: Let $\mathbf{a} = (\mathbf{a}(1), \ldots, \mathbf{a}(n))^T$, $\mathbf{b} = (\mathbf{b}(1), \ldots, \mathbf{b}(n))^T$ and $\mathbf{c} = (\mathbf{c}(1), \ldots, \mathbf{c}(n))^T$. Since $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$, we have $\{\mathbf{a}(i), \mathbf{b}(i)\} = \{\mathbf{a}(i), \mathbf{c}(i)\}$ for any $1 \le i \le n$. Now, if $\mathbf{b}(i) = \mathbf{a}(i)$, then $\mathbf{c}(i) = \mathbf{b}(i)$. On the other hand, if $\mathbf{b}(i) \ne \mathbf{a}(i)$, then $\mathbf{c}(i) = \mathbf{b}(i)$ since $\{\mathbf{a}(i), \mathbf{b}(i)\} = \{\mathbf{a}(i), \mathbf{c}(i)\}$. Hence, $\mathbf{c}(i) = \mathbf{b}(i)$ holds for any $1 \le i \le n$. This implies $\mathbf{b} = \mathbf{c}$ and thus $\mathcal{C}_1 = \mathcal{C}_2$.

So for any distinct $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$ such that $1 \le |\mathcal{C}_1| \le 2$, $1 \le |\mathcal{C}_2| \le 2$, it always holds that $\mathsf{desc}(\mathcal{C}_1) \ne \mathsf{desc}(\mathcal{C}_2)$. This means that $\mathcal{C}$ is a $\overline{2}$-SC(n, M, q). □

Now we describe a tracing algorithm based on a binary MIPPC. The following theorem shows that binary t-MIPPCs can be used to identify at least one colluder in the averaging attack.

Theorem 4.1.5 *Under the assumption that the number of colluders in the averaging attack is at most t, any t-MIPPC$(n, M, 2)$ can be used to identify at least one colluder with computational complexity $O(nM^t)$ by applying Algorithm 4.1 described below.*

Proof: Let $\mathcal{C}$ be the t-MIPPC$(n, M, 2)$, and $R \subseteq \mathcal{C}(1) \times \cdots \times \mathcal{C}(n)$ be the captured descendant code derived from the detection statistics $\mathbf{T}$. Then by applying the following tracing algorithm, Algorithm 4.1, we can identify at least one colluder.

Algorithm 4.1: `MIPPCTraceAlg`(R)

```
Given $R$;
Find $\mathcal{P}_t(R) = \{\mathcal{C}' \subseteq \mathcal{C} \mid |\mathcal{C}'| \le t, R = \mathsf{desc}(\mathcal{C}')\}$;
Compute $\mathcal{C}_0 = \bigcap_{\mathcal{C}' \in \mathcal{P}_t(R)} \mathcal{C}'$;
if $|\mathcal{C}_0| \le t$ then
    output $\mathcal{C}_0$ as the set of colluders;
else
    output "the set of colluders has size at least $t+1$";
```

The computational complexity is obvious. We need only to show that any user u assigned with a codeword $\mathbf{c} \in \mathcal{C}_0$ is a colluder. Since R is the captured descendant code derived from the detection statistics $\mathbf{T}$, it is clear that $\mathcal{P}_t(R) \ne \emptyset$. Therefore,

$$\mathcal{C}_0 = \bigcap_{\mathcal{C}' \in \mathcal{P}_t(R)} \mathcal{C}' \ne \emptyset$$

by the definition of a t-MIPPC. Assume that u is not a colluder. Then for any $\mathcal{C}' \in \mathcal{P}_t(R)$, we have $\mathcal{C}' \setminus \{\mathbf{c}\} \in \mathcal{P}_t(R)$, which implies $\mathbf{c} \notin \mathcal{C}_0$, a contradiction. □

The following theorem is a simple concatenation construction for binary t-MIPPCs from q-ary t-MIPPCs, which stimulates us to investigate q-ary t-MIPPCs with short length.

Lemma 4.1.6 *If there exists a t-MIPPC(n, M, q), then there exists a t-MIPPC$(nq, M, 2)$.*

Proof: Let $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \dots, \mathbf{c}_M\}$ be the t-MIPPC(n, M, q) defined on $Q = \{0, 1, \dots, q-1\}$, and $\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2, \dots, \mathbf{e}_q\}$, where $\mathbf{e}_i$ is the i-th column identity vector, i.e., all its coordinates are 0 except the i-th one being 1. Let $f : Q \longrightarrow \mathcal{E}$ be the bijective mapping such that $f(i) = \mathbf{e}_{i+1}$. For any codeword $\mathbf{c} = (\mathbf{c}(1), \mathbf{c}(2), \dots, \mathbf{c}(n))^T \in \mathcal{C}$, we define $f(\mathbf{c}) = (f(\mathbf{c}(1)), f(\mathbf{c}(2)), \dots, f(\mathbf{c}(n)))^T$. Obviously, $f(\mathbf{c})$ is a binary column vector of length nq. We define a new $(nq, M, 2)$ code $\mathcal{F} = \{f(\mathbf{c}_1), f(\mathbf{c}_2), \dots, f(\mathbf{c}_M)\}$. We are going to show that $\mathcal{F}$ is in fact a t-MIPPC.

Consider any $S \subseteq \mathcal{F}(1) \times \cdots \times \mathcal{F}(nq)$ with $\mathcal{P}_t(S) = \{\mathcal{F}_1, \dots, \mathcal{F}_r\} \neq \emptyset$. Each $\mathcal{F}_i$ corresponds to a subcode $\mathcal{C}_i \subseteq \mathcal{C}$ such that $|\mathcal{C}_i| \leq t$, where $\mathcal{F}_i = \{f(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_i\}$. Since $\mathsf{desc}(\mathcal{F}_1) = \mathsf{desc}(\mathcal{F}_2) = \cdots = \mathsf{desc}(\mathcal{F}_r)$, we immediately have $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2) = \cdots = \mathsf{desc}(\mathcal{C}_r)$. Since $\mathcal{C}$ is a t-MIPPC(n, M, q), we have $\bigcap_{i=1}^r \mathcal{C}_i \neq \emptyset$. Let $\mathbf{c} \in \bigcap_{i=1}^r \mathcal{C}_i$, then $\mathbf{c} \in \mathcal{C}_i$ for any $1 \leq i \leq r$, which implies $f(\mathbf{c}) \in \mathcal{F}_i$ for any $1 \leq i \leq r$, and thus $f(\mathbf{c}) \in \bigcap_{i=1}^r \mathcal{F}_i$. Therefore, $\bigcap_{i=1}^r \mathcal{F}_i \neq \emptyset$. This completes the proof. □

4.2 Upper bounds

In this section, we discuss the upper bound on the size of an MIPPC. We first derive a general upper bound on the size of a t-MIPPC(n, M, q), and then investigate 3-MIPPCs in more detail. By investigating the combinatorial properties of 3-MIPPCs of length 2, we further derive a tight upper bound for 3-MIPPCs of length 2.

4.2.1 A general upper bound

Let $M_{MIPPC}(t, n, q) = \max\{M \mid \text{there exists a } t\text{-MIPPC}(n, M, q)\}$. A t-MIPPC(n, M, q) is said to be optimal if $M = M_{MIPPC}(t, n, q)$, and asymptotically optimal if $\lim\limits_{q \to \infty} \frac{M}{M_{MIPPC}(t,n,q)} = 1$. Let $G_{X,Y} = G(u, v)$ be a bipartite graph on u vertices in the class X and v vertices in the class Y. Without loss of generality, we may assume that $u \geq v$. Let $e(G)$ denote the number of edges of G, that is, the size of G.

Lemma 4.2.1 ([37, 36]) *If a bipartite graph $G(u, v)$ contains no cycle of length less than or equal to $2l$, where $u \geq v$, then*

$$e(G) \leq \begin{cases} (uv)^{\frac{l+1}{2l}} + c(u+v), & l \text{ is odd}, \\ v^{\frac{1}{2}} u^{\frac{l+2}{2l}} + c(u+v), & l \text{ is even}, \end{cases}$$

where c is a constant depending only on l.

An application of Lemma 4.2.1 is the following theorem.

Theorem 4.2.2 *$M_{MIPPC}(t,n,q) \le q^{\frac{n}{2}}(q^{\frac{n}{2t}}+2c)$ if n is even, and*

$$M_{MIPPC}(t,n,q) \le \begin{cases} q^{\frac{n}{2}}(q^{\frac{n+1}{2t}}+c(q^{\frac{1}{2}}+q^{-\frac{1}{2}})), & t \text{ is even,} \\ q^{\frac{n}{2}}(q^{\frac{n}{2t}}+c(q^{\frac{1}{2}}+q^{-\frac{1}{2}})), & t \text{ is odd} \end{cases}$$

if n is odd, where c is a constant depending only on t.

Proof: Let $\mathcal{C}$ be a t-MIPPC(n,M,q) defined on Q. We prove this theorem in two cases.

If n is even, we construct a bipartite graph $G(q^{\frac{n}{2}},q^{\frac{n}{2}})$ as follows. Let $X=Y=Q^{\frac{n}{2}}$. An edge connects $\mathbf{a}\in X$ and $\mathbf{b}\in Y$ if and only if $(\mathbf{a},\mathbf{b})^T\in\mathcal{C}$. Obviously, $M=e(G)$. Suppose that there exists a $2t_0$-cycle in G, where $2\le t_0\le t$. Let $(\mathbf{a}_1,\mathbf{b}_1,\mathbf{a}_2,\mathbf{b}_2,\ldots,\mathbf{a}_{t_0},\mathbf{b}_{t_0})$ be the $2t_0$-cycle, where $\mathbf{a}_i$, $1\le i\le t_0$, are distinct vertices in X, and $\mathbf{b}_i$, $1\le i\le t_0$, are distinct vertices in Y. Then $(\mathbf{a}_i,\mathbf{b}_i)^T\in\mathcal{C}$ for $1\le i\le t_0$, and $(\mathbf{a}_1,\mathbf{b}_{t_0})^T,(\mathbf{a}_i,\mathbf{b}_{i-1})^T\in\mathcal{C}$ for $2\le i\le t_0$. Let $\mathcal{C}_1=\{(\mathbf{a}_i,\mathbf{b}_i)^T\mid 1\le i\le t_0\}$, $\mathcal{C}_2=\{(\mathbf{a}_1,\mathbf{b}_{t_0})^T\}\bigcup\{(\mathbf{a}_i,\mathbf{b}_{i-1})^T\mid 2\le i\le t_0\}$. Then $\mathsf{desc}(\mathcal{C}_1)=\mathsf{desc}(\mathcal{C}_2)$, but $\mathcal{C}_1\bigcap\mathcal{C}_2=\emptyset$, a contradiction to the fact that $\mathcal{C}$ is a t-MIPPC(n,M,q). So G contains no cycle of length less than or equal to $2t$. The conclusion then comes from Lemma 4.2.1.

If n is odd, we construct a bipartite graph $G(q^{\frac{n+1}{2}},q^{\frac{n-1}{2}})$ with $X=Q^{\frac{n+1}{2}},Y=Q^{\frac{n-1}{2}}$. Similarly, we can show that G contains no cycle of length less than or equal to $2t$, and the conclusion follows by Lemma 4.2.1. □

4.2.2 An upper bound for 3-MIPPCs of length 2

In order to derive a tight upper bound on the size of a 3-MIPPC of length 2, we present a combinatorial characterization of 3-MIPPCs. We first prove the following lemma on $\overline{2}$-separable codes.

Lemma 4.2.3 *Let $\mathcal{C}$ be a $(2,M,q)$ code on Q. Then $\mathcal{C}$ is a $\overline{2}$-SC$(2,M,q)$ if and only if $|\mathcal{A}^1_{a_1}\bigcap\mathcal{A}^1_{a_2}|\le 1$ holds in $\mathcal{C}$ for any distinct elements $a_1,a_2\in Q$.*

Proof: Let $\mathcal{C}$ be a $\overline{2}$-SC$(2,M,q)$. Assume that there exist distinct elements $a_1,a_2\in Q$ satisfying $|\mathcal{A}^1_{a_1}\bigcap\mathcal{A}^1_{a_2}|\ge 2$. Suppose $b_1,b_2\in\mathcal{A}^1_{a_1}\bigcap\mathcal{A}^1_{a_2}$, $b_1\ne b_2$. Then $(a_1,b_1)^T$, $(a_1,b_2)^T$, $(a_2,b_1)^T$, $(a_2,b_2)^T\in\mathcal{C}$. Let $\mathcal{C}_1=\{(a_1,b_1)^T,(a_2,b_2)^T\}$ and $\mathcal{C}_2=\{(a_1,b_2)^T,(a_2,b_1)^T\}$. Then $\mathcal{C}_1\ne\mathcal{C}_2$ and $\mathsf{desc}(\mathcal{C}_1)=\mathsf{desc}(\mathcal{C}_2)$, a contradiction to the definition of a $\overline{2}$-SC$(2,M,q)$.

Now we consider its sufficiency. Suppose that $|\mathcal{A}^1_{a_1}\bigcap\mathcal{A}^1_{a_2}|\le 1$ holds in $\mathcal{C}$ for any distinct elements $a_1,a_2\in Q$, but $\mathcal{C}$ is not a $\overline{2}$-SC$(2,M,q)$. This implies that there exist $\mathcal{C}_1,\mathcal{C}_2\subseteq\mathcal{C}$, $\mathcal{C}_1\ne\mathcal{C}_2$, $1\le|\mathcal{C}_1|\le 2$ and $1\le|\mathcal{C}_2|\le 2$, such that $\mathsf{desc}(\mathcal{C}_1)=\mathsf{desc}(\mathcal{C}_2)$.

Let $\mathcal{C}_1 = \{\mathbf{c}_1, \mathbf{c}_2\}$, $\mathcal{C}_2 = \{\mathbf{c}_3, \mathbf{c}_4\}$, $\mathcal{C}_1 \neq \mathcal{C}_2$, and $\mathbf{c}_i = (a_i, b_i)^T$ for $1 \leq i \leq 4$. We remark here that we allow $\mathbf{c}_1 = \mathbf{c}_2$ or $\mathbf{c}_3 = \mathbf{c}_4$. Since $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$, then $\mathcal{C}_1(1) = \mathcal{C}_2(1)$ and $\mathcal{C}_1(2) = \mathcal{C}_2(2)$. This implies that $a_1 = a_2$ (or $a_3 = a_4$) if and only if $a_1 = a_2 = a_3 = a_4$, and $b_1 = b_2$ (or $b_3 = b_4$) if and only if $b_1 = b_2 = b_3 = b_4$.

Now, if $a_1 = a_2$, then $a_1 = a_2 = a_3 = a_4$. Since $\mathcal{C}_1 \neq \mathcal{C}_2$, we have $b_1 \neq b_2$. By the fact that $\mathcal{C}_1(2) = \mathcal{C}_2(2)$, we have $\{b_1, b_2\} = \{b_3, b_4\}$, and therefore $\mathcal{C}_1 = \mathcal{C}_2$, a contradiction. On the other hand, if $a_1 \neq a_2$, then $a_3 \neq a_4$. Clearly, $b_1 \neq b_2$, otherwise we can use a similar argument to conclude that $\mathcal{C}_1 = \mathcal{C}_2$. Now, we have $\{a_1, a_2\} = \{a_3, a_4\}$ and $\{b_1, b_2\} = \{b_3, b_4\}$ as set equalities. Without loss of generality, we may assume $a_1 = a_3$ and $a_2 = a_4$. In this case, if $b_1 = b_3$, then $b_2 = b_4$, and thus $\mathcal{C}_1 = \mathcal{C}_2$, a contradiction. Therefore, $b_1 = b_4$ and $b_2 = b_3$, which implies that $\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2} = \{b_1, b_2\}$, a contradiction. This completes the proof. $\square$

Now we turn our attention to 3-MIPPCs.

Lemma 4.2.4 *Let $\mathcal{C}$ be a 3-MIPPC(n, M, q) defined on Q. Then*

(I) $|\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}| \leq 1$ *always holds for any distinct elements $a_1, a_2 \in Q$;*

(II) *There do not exist distinct elements $a_1, a_2, a_3 \in Q$ and distinct vectors $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \in Q^{n-1}$ such that $\mathbf{b}_1, \mathbf{b}_2 \in \mathcal{A}^1_{a_1}$, $\mathbf{b}_2, \mathbf{b}_3 \in \mathcal{A}^1_{a_2}$, $\mathbf{b}_1, \mathbf{b}_3 \in \mathcal{A}^1_{a_3}$.*

Proof: (I) If there exist distinct elements $a_1, a_2 \in Q$ satisfying that $|\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}| \geq 2$, say $\mathbf{b}_1 \neq \mathbf{b}_2 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}$, then $(a_1, \mathbf{b}_1)^T, (a_1, \mathbf{b}_2)^T, (a_2, \mathbf{b}_1)^T, (a_2, \mathbf{b}_2)^T \in \mathcal{C}$. Let $\mathcal{C}_1 = \{(a_1, \mathbf{b}_1)^T, (a_2, \mathbf{b}_2)^T\}$ and $\mathcal{C}_2 = \{(a_1, \mathbf{b}_2)^T, (a_2, \mathbf{b}_1)^T\}$. Then $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$, but $\mathcal{C}_1 \bigcap \mathcal{C}_2 = \emptyset$, a contradiction to the definition of a 3-MIPPC(n, M, q).

(II) If there exist distinct elements $a_1, a_2, a_3 \in Q$ and distinct vectors $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3 \in Q^{n-1}$ such that $\mathbf{b}_1, \mathbf{b}_2 \in \mathcal{A}^1_{a_1}$, $\mathbf{b}_2, \mathbf{b}_3 \in \mathcal{A}^1_{a_2}$, $\mathbf{b}_1, \mathbf{b}_3 \in \mathcal{A}^1_{a_3}$, then $(a_1, \mathbf{b}_1)^T$, $(a_1, \mathbf{b}_2)^T$, $(a_2, \mathbf{b}_2)^T$, $(a_2, \mathbf{b}_3)^T$, $(a_3, \mathbf{b}_1)^T$, $(a_3, \mathbf{b}_3)^T \in \mathcal{C}$. Let $\mathcal{C}_1 = \{(a_1, \mathbf{b}_1)^T, (a_2, \mathbf{b}_2)^T, (a_3, \mathbf{b}_3)^T\}$, $\mathcal{C}_2 = \{(a_1, \mathbf{b}_2)^T, (a_2, \mathbf{b}_3)^T, (a_3, \mathbf{b}_1)^T\}$. Then $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$, but $\mathcal{C}_1 \bigcap \mathcal{C}_2 = \emptyset$, a contradiction to the definition of a 3-MIPPC(n, M, q). $\square$

It is of interest to see that the converse of Lemma 4.2.4 is true when $n = 2$.

Lemma 4.2.5 *Let $\mathcal{C}$ be a $(2, M, q)$ code defined on Q. If $\mathcal{C}$ satisfies the following two conditions:*

(I) $|\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}| \leq 1$ *always holds for any distinct elements $a_1, a_2 \in Q$;*

(II) *There do not exist distinct elements $a_1, a_2, a_3 \in Q$ and distinct elements $b_1, b_2, b_3 \in Q$, such that $b_1, b_2 \in \mathcal{A}^1_{a_1}$, $b_2, b_3 \in \mathcal{A}^1_{a_2}$, $b_1, b_3 \in \mathcal{A}^1_{a_3}$.*

Then $\mathcal{C}$ is a 3-MIPPC$(2, M, q)$.

Proof: Suppose $\mathcal{C}$ satisfies conditions (I) and (II). We prove this lemma in three steps.

(1) At first, we prove that if there exist $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathcal{C}$, $\mathcal{C}_1 \neq \mathcal{C}_2$, $|\mathcal{C}_1| \leq 3$, $|\mathcal{C}_2| \leq 3$, satisfying $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$, then $\mathcal{C}_1$ and $\mathcal{C}_2$ should be of one of the following three types:

$$\text{Type } \mathbf{I}: \qquad \begin{array}{c} \begin{array}{ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 \end{array} \\ \begin{pmatrix} a_1 & a_2 & a_1 \\ b_1 & b_2 & b_2 \end{pmatrix} \end{array},$$

where $\mathcal{C}_1 = \{\mathbf{c}_1, \mathbf{c}_2\}$, $\mathcal{C}_2 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, $a_1 \neq a_2$, $b_1 \neq b_2$;

$$\text{Type } \mathbf{II}: \qquad \begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \begin{pmatrix} a_1 & a_2 & a_3 & a_1 \\ b_1 & b_1 & b_3 & b_3 \end{pmatrix} \end{array},$$

where $\mathcal{C}_1 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, $\mathcal{C}_2 = \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, $a_{k_1} \neq a_{k_2}$, $1 \leq k_1 < k_2 \leq 3$, $b_1 \neq b_3$;

$$\text{Type } \mathbf{III}: \qquad \begin{array}{c} \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \begin{pmatrix} a_1 & a_1 & a_3 & a_3 \\ b_1 & b_2 & b_3 & b_1 \end{pmatrix} \end{array},$$

where $\mathcal{C}_1 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, $\mathcal{C}_2 = \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, $a_1 \neq a_3$, $b_{k_1} \neq b_{k_2}$, $1 \leq k_1 < k_2 \leq 3$.

(1.1) If $|\mathcal{C}_1| \leq 2$, $|\mathcal{C}_2| \leq 2$, then $\mathcal{C}$ is not a $\overline{2}$-SC$(2, M, q)$. However, according to condition (I) and Lemma 4.2.3, $\mathcal{C}$ is a $\overline{2}$-SC$(2, M, q)$, a contradiction. So this case is impossible.

(1.2) If $|\mathcal{C}_1| = 1$, $|\mathcal{C}_2| = 3$, let $\mathcal{C}_1 = \{\mathbf{c}_1\}$, $\mathcal{C}_2 = \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, where $\mathbf{c}_i = (a_i, b_i)^T$, $1 \leq i \leq 4$. Then $a_1 = a_2 = a_3 = a_4$ and $b_1 = b_2 = b_3 = b_4$ according to $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$, which implies $\mathbf{c}_1 = \mathbf{c}_2 = \mathbf{c}_3 = \mathbf{c}_4$, a contradiction. So this case is not possible either.

(1.3) Consider the case $|\mathcal{C}_1| = 2$, $|\mathcal{C}_2| = 3$. Let $|\mathcal{C}_1| = \{\mathbf{c}_1, \mathbf{c}_2\}$, $|\mathcal{C}_2| = \{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5\}$, where $\mathbf{c}_i = (a_i, b_i)^T$, $1 \leq i \leq 5$.

(1.3.A) If $a_1 = a_2$, then $a_3 = a_4 = a_5 = a_1$. Since $\{b_1, b_2\} = \{b_3, b_4, b_5\}$, there must be two identical elements in $\{b_3, b_4, b_5\}$. We may assume $b_3 = b_4$. Then $\mathbf{c}_3 = \mathbf{c}_4$, a contradiction. So this case is impossible.

(1.3.B) If $a_1 \neq a_2$, since $\mathsf{desc}(\mathcal{C}_1) = \mathsf{desc}(\mathcal{C}_2)$, then $a_3, a_4, a_5 \in \{a_1, a_2\}$ and $b_3, b_4, b_5 \in \{b_1, b_2\}$. Without loss of generality, we may assume that $a_3 = a_4 = a_1$ and $a_5 = a_2$. Then $b_3 \neq b_4$, otherwise, $\mathbf{c}_3 = \mathbf{c}_4$, a contradiction. Since $b_3, b_4 \in \{b_1, b_2\}$, then $b_1 \neq b_2$ and we may assume that $b_3 = b_1$ and $b_4 = b_2$.

$$\begin{array}{c} \begin{array}{cc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 \end{array} \\ \left(\begin{array}{cc|ccc} a_1 & a_2 & a_1 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 & \end{array}\right) \end{array}$$

If $b_5 = b_1$, then $b_1, b_2 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}$, that is, $|\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}| \geq 2$, a contradiction to condition (I). So this case is impossible.

If $b_5 = b_2$, then

$$\begin{array}{cc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 \\ a_1 & a_2 & a_1 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 & b_2 \end{array} ,$$

that is,

$$\begin{array}{ccc} \mathbf{c}_1(\mathbf{c}_3) & \mathbf{c}_2(\mathbf{c}_5) & \mathbf{c}_4 \\ a_1 & a_2 & a_1 \\ b_1 & b_2 & b_2 \end{array} .$$

So $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **I**.

(1.4) Consider the case $|\mathcal{C}_1| = 3$, $|\mathcal{C}_2| = 3$. Let $\mathcal{C}_1 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, $\mathcal{C}_2 = \{\mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6\}$, where $\mathbf{c}_i = (a_i, b_i)^T$, $1 \leq i \leq 6$.

(1.4.A) If $a_1 = a_2 = a_3$ or $b_1 = b_2 = b_3$, then $\mathcal{C}_1 = \mathcal{C}_2$, a contradiction. So this case is impossible.

(1.4.B) Consider the case $a_1 = a_2$ and $a_3 \neq a_1$. Then $b_1 \neq b_2$, otherwise, $\mathbf{c}_1 = \mathbf{c}_2$, a contradiction.

(1.4.B.a) Suppose $b_1 = b_3$. Since $a_3 \in \{a_4, a_5, a_6\}$, we may assume $a_4 = a_3$. Then $b_4 = b_1$, otherwise, $b_4 = b_2$, which implies $b_1, b_2 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_3}$, a contradiction to condition (I).

$$\begin{array}{ccc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 \\ a_1 & a_1 & a_3 & a_3 & & \\ b_1 & b_2 & b_1 & b_1 & & \end{array}$$

Now we consider $\mathbf{c}_5$ and $\mathbf{c}_6$. If $a_5 = a_3$ or $a_6 = a_3$, similarly, we can show that $b_5 = b_1$ or $b_6 = b_1$, respectively, which implies $\mathbf{c}_5 = \mathbf{c}_4$ or $\mathbf{c}_6 = \mathbf{c}_4$, respectively, a contradiction. So $a_5 = a_6 = a_1$. Then $b_5 \neq b_6$, otherwise, $\mathbf{c}_5 = \mathbf{c}_6$, a contradiction. Since $b_5, b_6 \in \{b_1, b_2\}$, we may assume that $b_5 = b_1$, $b_6 = b_2$.

$$\begin{array}{ccc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 \\ a_1 & a_1 & a_3 & a_3 & a_1 & a_1 \\ b_1 & b_2 & b_1 & b_1 & b_1 & b_2 \end{array}$$

Then $\mathcal{C}_1 = \mathcal{C}_2$, a contradiction. So this case is impossible.

(1.4.B.b) Suppose $b_i \neq b_j$, $1 \leq i < j \leq 3$. Since $\{b_1, b_2, b_3\} = \{b_4, b_5, b_6\}$, we may assume that $b_4 = b_1, b_5 = b_2, b_6 = b_3$.

$$\begin{array}{ccc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 \\ a_1 & a_1 & a_3 & & & \\ b_1 & b_2 & b_3 & b_1 & b_2 & b_3 \end{array}$$

It is impossible that $(a_4, a_5) = (a_1, a_1)$. Otherwise, $a_6 = a_3$, which implies $\mathcal{C}_1 = \mathcal{C}_2$, a contradiction.

It is not possible either that $(a_4, a_5) = (a_3, a_3)$. Otherwise, $b_1, b_2 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_3}$, a contradiction to condition (I).

If $(a_4, a_5) = (a_1, a_3)$, then

$$\begin{array}{c} \begin{array}{ccc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 \end{array} \\ \left(\begin{array}{ccc|ccc} a_1 & a_1 & a_3 & a_1 & a_3 & \\ b_1 & b_2 & b_3 & b_1 & b_2 & b_3 \end{array}\right) \end{array}.$$

We should have $a_6 = a_3$. Otherwise, $a_6 = a_1$, then $b_2, b_3 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_3}$, a contradiction to condition (I). So

$$\begin{array}{c} \begin{array}{cccc} \mathbf{c}_2 & \mathbf{c}_1(\mathbf{c}_4) & \mathbf{c}_3(\mathbf{c}_6) & \mathbf{c}_5 \end{array} \\ \left(\begin{array}{cccc} a_1 & a_1 & a_3 & a_3 \\ b_2 & b_1 & b_3 & b_2 \end{array}\right) \end{array},$$

and therefore, $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **III**.

Similarly, if $(a_4, a_5) = (a_3, a_1)$, we can show that $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **III**.

(1.4.C) Consider the case $a_i \neq a_j$, $1 \leq i < j \leq 3$. Since $\{a_1, a_2, a_3\} = \{a_4, a_5, a_6\}$, we may assume that $a_4 = a_1, a_5 = a_2, a_6 = a_3$.

(1.4.C.a) Suppose $b_1 = b_2$ and $b_3 \neq b_1$.

$$\begin{array}{c} \begin{array}{ccc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 \end{array} \\ \left(\begin{array}{ccc|ccc} a_1 & a_2 & a_3 & a_1 & a_2 & a_3 \\ b_1 & b_1 & b_3 & & & \end{array}\right) \end{array}$$

It is impossible that $(b_4, b_5) = (b_1, b_1)$. Otherwise, $b_6 = b_3$, which implies $\mathcal{C}_1 = \mathcal{C}_2$, a contradiction.

It is not possible either that $(b_4, b_5) = (b_3, b_3)$. Otherwise, $b_1, b_3 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}$, a contradiction to condition (I).

Suppose $(b_4, b_5) = (b_1, b_3)$.

$$\begin{array}{c} \begin{array}{ccc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 \end{array} \\ \left(\begin{array}{ccc|ccc} a_1 & a_2 & a_3 & a_1 & a_2 & a_3 \\ b_1 & b_1 & b_3 & b_1 & b_3 & \end{array}\right) \end{array}$$

Then $b_6 = b_3$. Otherwise, $b_6 = b_1$, then $b_1, b_3 \in \mathcal{A}^1_{a_2} \bigcap \mathcal{A}^1_{a_3}$, a contradiction to condition (I). So

$$\begin{array}{c} \begin{array}{cccc} \mathbf{c}_2 & \mathbf{c}_1(\mathbf{c}_4) & \mathbf{c}_3(\mathbf{c}_6) & \mathbf{c}_5 \end{array} \\ \left(\begin{array}{cccc} a_2 & a_1 & a_3 & a_2 \\ b_1 & b_1 & b_3 & b_3 \end{array}\right) \end{array}$$

and thus $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **II**.

Similarly, if $(b_4, b_5) = (b_3, b_1)$, we can derive that $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **II**.

(1.4.C.b) Suppose $b_i \neq b_j$, $1 \leq i < j \leq 3$.

$$\begin{array}{c}
\begin{array}{ccc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 \end{array} \\
\left(\begin{array}{ccc|ccc} a_1 & a_2 & a_3 & a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 & & & \end{array}\right)
\end{array}$$

It is impossible that $(b_4, b_5, b_6) = (b_1, b_2, b_3)$. Otherwise, $\mathcal{C}_1 = \mathcal{C}_2$, a contradiction.

It is impossible that $(b_4, b_5, b_6) = (b_1, b_3, b_2)$. Otherwise, $b_2, b_3 \in \mathcal{A}^1_{a_2} \bigcap \mathcal{A}^1_{a_3}$, a contradiction to condition (I).

It is impossible that $(b_4, b_5, b_6) = (b_2, b_1, b_3)$. Otherwise, $b_1, b_2 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}$, a contradiction to condition (I).

It is impossible that $(b_4, b_5, b_6) = (b_2, b_3, b_1)$. Otherwise, $b_1, b_2 \in \mathcal{A}^1_{a_1}$, $b_2, b_3 \in \mathcal{A}^1_{a_2}$, $b_1, b_3 \in \mathcal{A}^1_{a_3}$, a contradiction to condition (II).

It is impossible that $(b_4, b_5, b_6) = (b_3, b_1, b_2)$. Otherwise, $b_1, b_3 \in \mathcal{A}^1_{a_1}$, $b_1, b_2 \in \mathcal{A}^1_{a_2}$, $b_2, b_3 \in \mathcal{A}^1_{a_3}$, a contradiction to condition (II).

Finally, it is not possible either that $(b_4, b_5, b_6) = (b_3, b_2, b_1)$. Otherwise, $b_1, b_3 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_3}$, a contradiction to condition (I).

(2) Now we prove that $|\mathcal{P}_3(R)| \leq 2$ for any $R \subseteq \mathcal{C}(1) \times \mathcal{C}(2)$. Assume that there exists $R \subseteq \mathcal{C}(1) \times \mathcal{C}(2)$ such that $|\mathcal{P}_3(R)| \geq 3$. Let $\mathcal{C}_1, \mathcal{C}_2, \mathcal{C}_3 \in \mathcal{P}_3(R)$ be three distinct sub-codes of $\mathcal{C}$. According to (1), $\mathsf{desc}(\mathcal{C}_i) = \mathsf{desc}(\mathcal{C}_j)$ implies $\mathcal{C}_i$ and $\mathcal{C}_j$ are of one of the three types described in (1), where $1 \leq i < j \leq 3$.

(2.1) If there exists an index i, $1 \leq i \leq 3$, such that $|\mathcal{C}_i| = 2$, without loss of generality, we may assume $|\mathcal{C}_1| = 2$. Then $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **I**, $\mathcal{C}_1$ and $\mathcal{C}_3$ are of type **I**. We may assume that $\mathcal{C}_1 = \{\mathbf{c}_1, \mathbf{c}_2\}$, $\mathcal{C}_2 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, and $\mathcal{C}_3 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4\}$, where $\mathbf{c}_i = (a_i, b_i)^T$, $1 \leq i \leq 4$. According to type I, $\mathbf{c}_3, \mathbf{c}_4 \in \{(a_1, b_2)^T, (a_2, b_1)^T\}$. Clearly $\mathbf{c}_3 \neq \mathbf{c}_4$, otherwise $\mathcal{C}_2 = \mathcal{C}_3$, a contradiction. Therefore, $b_1, b_2 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}$, which implies $|\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}| \geq 2$, a contradiction to condition (I). So this case is impossible.

(2.2) Consider the case $|\mathcal{C}_i| = 3$ for all $1 \leq i \leq 3$.

(2.2.A) Suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **II**, $\mathcal{C}_1$ and $\mathcal{C}_3$ are of type **II**. Let $\mathcal{C}_1 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, $\mathcal{C}_2 = \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, and $\mathcal{C}_3 = \{\mathbf{c}_5, \mathbf{c}_6, \mathbf{c}_7\}$, where $\mathbf{c}_i = (a_i, b_i)^T$, $1 \leq i \leq 7$. According to type **II**, $a_{k_1} \neq a_{k_2}$, $1 \leq k_1 < k_2 \leq 3$, $b_1 \neq b_3$.

$$\begin{array}{c}
\begin{array}{ccccccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 & \mathbf{c}_7 \end{array} \\
\left(\begin{array}{ccccccc} a_1 & a_2 & a_3 & a_1 & & & \\ b_1 & b_1 & b_3 & b_3 & & & \end{array}\right)
\end{array}$$

Since $\mathcal{C}_1$ and $\mathcal{C}_3$ are of type **II**, we have $|\mathcal{C}_1 \bigcap \mathcal{C}_3| = 2$. Furthermore, because we require $b_1 \neq b_3$, we know $\mathcal{C}_1 \bigcap \mathcal{C}_3 \neq \{\mathbf{c}_1, \mathbf{c}_2\}$.

If $\mathcal{C}_1 \bigcap \mathcal{C}_3 = \{\mathbf{c}_1, \mathbf{c}_3\}$, we may assume $\mathbf{c}_5 = \mathbf{c}_1, \mathbf{c}_6 = \mathbf{c}_3$. Then we should have $\mathbf{c}_7 = (a_2, b_3)^T$, and

$$\begin{array}{ccccc} \mathbf{c}_2 & \mathbf{c}_1(\mathbf{c}_5) & \mathbf{c}_3(\mathbf{c}_6) & \mathbf{c}_7 & \mathbf{c}_4 \\ \end{array}$$
$$\left(\begin{array}{ccccc} a_2 & a_1 & a_3 & a_2 & a_1 \\ b_1 & b_1 & b_3 & b_3 & b_3 \end{array}\right),$$

which implies $b_1, b_3 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}$, i.e., $|\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}| \geq 2$, a contradiction to condition (I). So this case is impossible.

If $\mathcal{C}_1 \bigcap \mathcal{C}_3 = \{\mathbf{c}_2, \mathbf{c}_3\}$, we may assume $\mathbf{c}_5 = \mathbf{c}_2, \mathbf{c}_6 = \mathbf{c}_3$. Then $\mathbf{c}_7 = (a_1, b_3)^T = \mathbf{c}_4$, which implies $\mathcal{C}_2 = \mathcal{C}_3$, a contradiction. So this case is not possible either.

(2.2.B) Suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **III**, $\mathcal{C}_1$ and $\mathcal{C}_3$ are of type **III**. Similar to (2.2.A), we can prove this case is impossible.

(2.2.C) Suppose $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **II**, $\mathcal{C}_1$ and $\mathcal{C}_3$ are of type **III**. Let $\mathcal{C}_1 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, $\mathcal{C}_2 = \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$.

$$\begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array}$$
$$\left(\begin{array}{cccc} a_1 & a_2 & a_3 & a_1 \\ b_1 & b_1 & b_3 & b_3 \end{array}\right)$$

Since $a_{k_1} \neq a_{k_2}$, $1 \leq k_1 < k_2 \leq 3$, it is impossible that $\mathcal{C}_1$ and $\mathcal{C}_3$ are of type **III**. So this case is not possible either.

Therefore, as we claimed earlier, $|\mathcal{P}_3(R)| \leq 2$ for any $R \subseteq \mathcal{C}(1) \times \mathcal{C}(2)$.

(3) Finally, the conclusion comes from (1), (2), and the fact that $\mathcal{C}_1 \bigcap \mathcal{C}_2 \neq \emptyset$ whenever $\mathcal{C}_1$ and $\mathcal{C}_2$ are of type **I**, **II**, or **III**. □

Combining Lemma 4.2.4 with Lemma 4.2.5, we derive an important result as follows.

Theorem 4.2.6 *Let $\mathcal{C}$ be a $(2, M, q)$ code defined on Q. Then $\mathcal{C}$ is a 3-MIPPC$(2, M, q)$ if and only if it satisfies the following two conditions:*

(I) $|\mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}| \leq 1$ *always holds for any distinct elements $a_1, a_2 \in Q$;*

(II) *There do not exist distinct elements $a_1, a_2, a_3 \in Q$ and distinct elements $b_1, b_2, b_3 \in Q$ such that $b_1, b_2 \in \mathcal{A}^1_{a_1}$, $b_2, b_3 \in \mathcal{A}^1_{a_2}$, $b_1, b_3 \in \mathcal{A}^1_{a_3}$.*

Now, we are going to derive a tight upper bound on the size of a 3-MIPPC$(2, M, q)$ based on Theorem 4.2.6.

Lemma 4.2.7 *There exists a 3-MIPPC$(2, M, q)$ if and only if there exists a bipartite graph $G(q, q)$ of girth at least 8 with $e(G) = M$.*

Proof: Suppose that there exists a 3-MIPPC$(2, M, q)$, $\mathcal{C}$, defined on Q. We construct a bipartite graph $G(q, q)$ as follows. Let $X = Q \times \{1\}$ and $Y = Q \times \{2\}$. An edge is incident to $(a, 1) \in X$ and $(b, 2) \in Y$ if and only if $(a, b)^T \in \mathcal{C}$. Then $e(G) = M$. We are going to show that G has girth at least 8.

Assume $G(q, q)$ contains a 4-cycle, say $((a_1, 1), (b_1, 2), (a_2, 1), (b_2, 2))$, where $(a_i, 1)$, $1 \leq i \leq 2$, are distinct elements of X, and $(b_i, 2)$, $1 \leq i \leq 2$, are distinct elements of Y. Then $(a_1, b_1)^T, (a_2, b_1)^T, (a_2, b_2)^T, (a_1, b_2)^T \in \mathcal{C}$, and thus $b_1, b_2 \in \mathcal{A}^1_{a_1} \bigcap \mathcal{A}^1_{a_2}$, a contradiction to Theorem 4.2.6. So this case is impossible.

Assume $G(q, q)$ contains a 6-cycle, say $((a_1, 1), (b_1, 2), (a_2, 1), (b_2, 2), (a_3, 1), (b_3, 2))$, where $(a_i, 1)$, $1 \leq i \leq 3$, are distinct elements of X, and $(b_i, 2)$, $1 \leq i \leq 3$, are distinct elements of Y. Then $(a_1, b_1)^T$, $(a_2, b_1)^T$, $(a_2, b_2)^T$, $(a_3, b_2)^T$, $(a_3, b_3)^T$, $(a_1, b_3)^T \in \mathcal{C}$, and thus $b_1, b_3 \in \mathcal{A}^1_{a_1}$, $b_1, b_1 \in \mathcal{A}^1_{a_2}$, $b_2, b_3 \in \mathcal{A}^1_{a_3}$, a contradiction to Theorem 4.2.6. So this case is not possible either.

Therefore, the bipartite graph $G(q, q)$ constructed above has girth at least 8, with $e(G) = M$.

Conversely, for any bipartite graph $G(q, q) = G_{X,Y}$ with girth at least 8, we construct a $(2, M, q)$ code $\mathcal{C}$. Let $Q = X$ and $f : Y \longrightarrow X$ be a bijective mapping. A vector $(x, f(y))^T \in \mathcal{C}$ if and only if $\{x, y\}$ is an edge of G, where $x \in X$ and $y \in Y$. Obviously, $\mathcal{C}$ is a $(2, M, q)$ code defined on Q and $M = e(G)$. Suppose that $\mathcal{C}$ is not a 3-MIPPC$(2, M, q)$. Then by Theorem 4.2.6, at least one of the following cases should happen.

(1) There exist distinct elements $x_1, x_2 \in Q$ such that $|\mathcal{A}^1_{x_1} \bigcap \mathcal{A}^1_{x_2}| \geq 2$. In this case, we may assume $f(y_1) \neq f(y_2) \in \mathcal{A}^1_{x_1} \bigcap \mathcal{A}^1_{x_2}$. Then $y_1 \neq y_2$, and $(x_1, f(y_1))^T$, $(x_1, f(y_2))^T$, $(x_2, f(y_1))^T$, $(x_2, f(y_2))^T \in \mathcal{C}$. Hence $\{x_1, y_1\}$, $\{x_1, y_2\}$, $\{x_2, y_1\}$, $\{x_2, y_2\}$ are edges of G forming a 4-cycle, a contradiction. So this case is impossible.

(2) There exist distinct elements $x_1, x_2, x_3 \in Q$ and distinct elements $f(y_1), f(y_2)$, $f(y_3) \in Q$ such that $f(y_1)$, $f(y_2) \in \mathcal{A}^1_{x_1}$, $f(y_2)$, $f(y_3) \in \mathcal{A}^1_{x_2}$, $f(y_1), f(y_3) \in \mathcal{A}^1_{x_3}$. In this case, y_i, $1 \leq i \leq 3$, are all distinct, and $(x_1, f(y_1))^T$, $(x_1, f(y_2))^T$, $(x_2, f(y_2))^T$, $(x_2, f(y_3))^T$, $(x_3, f(y_3))^T$, $(x_3, f(y_1))^T \in \mathcal{C}$. Hence $\{x_1, y_1\}$, $\{x_1, y_2\}$, $\{x_2, y_2\}$, $\{x_2, y_3\}$, $\{x_3, y_3\}$, $\{x_3, y_1\}$ are edges of G forming a 6-cycle, a contradiction. So this case is not possible either.

Therefore, the $(2, M, q)$ code $\mathcal{C}$ constructed above is a 3-MIPPC$(2, M, q)$ with $M = e(G)$.

This completes the proof. □

García-Vázquez *et al.* [28] stated that any maximum bipartite graph $G(q, q)$ with size $M_{MIPPC}(3, 2, q)$ must have girth 8, for $q \geq 6$ or $q = 4$. Therefore, we have the following corollary.

Corollary 4.2.8 *Let $q \geq 6$ or $q = 4$. There exists a 3-MIPPC$(2, M, q)$ if and only if there exists a bipartite graph $G(q, q)$ of girth 8 with $e(G) = M$.*

Lemma 4.2.9 ([42]) *If $G(u,v)$ contains no cycle of length 4 and 6, then its size e satisfies the following inequality*

$$e^3 - (u+v)e^2 + 2uve - u^2v^2 \leq 0.$$

Then the size of a 3-MIPPC$(2, M, q)$ can be derived from Lemmas 4.2.7 and 4.2.9.

Corollary 4.2.10 *For any* 3-*MIPPC*$(2, M, q)$, $M^3 - 2qM^2 + 2q^2M - q^4 \leq 0$.

4.3 Constructions for 3-MIPPC$(2, M, q)$s

In this section, an infinite series of optimal 3-MIPPCs of length 2 are derived by generalized quadrangles. Several infinite series of asymptotically optimal 3-MIPPCs of length 2 are also constructed by deleting suitable points and lines from generalized quadrangles.

4.3.1 Optimal 3-MIPPC$(2, M, q)$s

MIPPCs are also closely related with generalized packings defined in Definition 2.2.1. A generalized packing $(X, \mathcal{B})$ is called $\triangle$-free if for any three distinct elements $P_1, P_2, P_3 \in X$, if there are two blocks containing P_1, P_2 and P_1, P_3 respectively, then there is no block containing P_2, P_3.

Theorem 4.3.1 *There exists a* 3-*MIPPC*$(2, M, q)$ *defined on* $Q = \{0, 1, \ldots, q-1\}$ *if and only if there exists a $\triangle$-free generalized* $(q, q, K, 1)$ *packing* $(Q, \{\mathcal{A}_0^1, \ldots, \mathcal{A}_{q-1}^1\})$ *with* $K = \{|\mathcal{A}_0^1|, \ldots, |\mathcal{A}_{q-1}^1|\}$, *and* $M = |\mathcal{A}_0^1| + \cdots + |\mathcal{A}_{q-1}^1|$.

Proof: Suppose $\mathcal{C}$ is a 3-MIPPC$(2, M, q)$ defined on Q, and $\mathcal{A}_i^1 = \{b \in Q \mid (i, b)^T \in \mathcal{C}\}$ for any $i \in Q$. Then by Theorem 4.2.6, we know that $(Q, \{\mathcal{A}_0^1, \ldots, \mathcal{A}_{q-1}^1\})$ is a $\triangle$-free generalized $(q, q, \{|\mathcal{A}_0^1|, \ldots, |\mathcal{A}_{q-1}^1|\}, 1)$ packing, and $M = |\mathcal{A}_0^1| + \cdots + |\mathcal{A}_{q-1}^1|$.

Conversely, for any $\triangle$-free generalized $(q, q, K, 1)$ packing $(Q, \mathcal{B})$ with $\mathcal{B} = \{B_0, \ldots, B_{q-1}\}$ and $M = |B_0| + \cdots + |B_{q-1}|$, we define a set of vectors $\mathcal{B}^1 = \{B_0^1, \ldots, B_{q-1}^1\}$, with $B_i^1 = \{(i, b)^T \mid b \in B_i\}$ if $B_i \neq \emptyset$ and $B_i^1 = \emptyset$ if $B_i = \emptyset$, $0 \leq i \leq q-1$. By Theorem 4.2.6, it is readily checked that $\mathcal{B}^1$ is a 3-MIPPC$(2, M, q)$ defined on Q and $\mathcal{A}_i^1 = B_i$ for any $i \in Q$.

This completes the proof. □

Corollary 4.3.2 *There exists an optimal* 3-*MIPPC*$(2, M, q)$ *on* $Q = \{0, 1, \ldots, q-1\}$ *if and only if there exists a $\triangle$-free generalized* $(q, q, K, 1)$ *packing with maximum* $M = |\mathcal{A}_0^1| + \cdots + |\mathcal{A}_{q-1}^1|$, *where* $K = \{|\mathcal{A}_0^1|, \ldots, |\mathcal{A}_{q-1}^1|\}$, Now we show that some optimal 3-MIPPC$(2, M, q)$s can be constructed by means of generalized quadrangles.

Definition 4.3.3 *A finite generalized quadrangle (GQ) is an incidence structure $\mathcal{S} = (X, \mathcal{B}, I)$ with point-set X and line-set $\mathcal{B}$ satisfying the following conditions:*

(1) *Each point is incident with $1 + t$ lines ($t \geq 1$) and two distinct points are incident with at most one line;*

(2) *Each line is incident with $1 + s$ points ($s \geq 1$) and two distinct lines are incident with at most one point;*

(3) *If x is a point and L is a line not incident with x, then there is a unique pair $(y, N) \in X \times \mathcal{B}$ for which $xINIyIL$.*

The integers s and t are the parameters of the GQ and $\mathcal{S}$ has order (s, t); if $s = t$, $\mathcal{S}$ has order s.

From the definition, any generalized quadrangle has no triangles. It is known (see [19]) that in a generalized quadrangle, $|X| = (1+s)(1+st)$, $|\mathcal{B}| = (1+t)(1+st)$, and $s + t$ divides $st(1 + s)(1 + t)$.

Lemma 4.3.4 *If there exits a GQ(s, t), then there exists a $\triangle$-free generalized $(v, b, \{1 + s\}, 1)$ packing, where $v = (1 + s)(1 + st), b = (1 + t)(1 + st)$.*

Proof: Suppose $\mathcal{S} = (X, \mathcal{B}, I)$ is a GQ(s, t). By regarding the lines of $\mathcal{S}$ as blocks and the points of $\mathcal{S}$ as elements, we easily obtain a $\triangle$-free generalized $(v, b, \{1+s\}, 1)$ packing $(X, \mathcal{B})$. □

Lemma 4.3.5 ([19]) *Let k be a prime power and $s \leq t$ be two positive integers. Then there exist GQ(s, t)s for $(s, t) \in \{(k - 1, k + 1), (k, k), (k, k^2), (k^2, k^3)\}$.*

If there exists a GQ(s, t) with $s \leq t$, then Lemma 4.3.4 gives a $\triangle$-free generalized $(v, b, \{1 + s\}, 1)$ packing with $v = (1 + s)(1 + st) \leq (1 + t)(1 + st) = b$. Deleting $b - v$ blocks, we obtain a $\triangle$-free generalized $(v, v, \{1 + s\}, 1)$ packing.

Corollary 4.3.6 *For any prime power k, there exist 3-MIPPC$(2, M, q)$s for $(M, q) \in \{(k^4, k^3), ((k^2+1)(k+1)^2, (k^2+1)(k+1)), ((k^3+1)(k+1)^2, (k^3+1)(k+1)), ((k^5 + 1)(k^2 + 1)^2, (k^5 + 1)(k^2 + 1))\}$.*

Proof: Apply Theorem 4.3.1 with Lemmas 4.3.4, 4.3.5. □

Lemma 4.3.7 *Let a, d be two positive integers with $d^2 - 2d + 2 - a = 0$. Then for any 3-MIPPC$(2, M, ad)$, we have $M \leq ad^2$.*

Proof: For any 3-MIPPC$(2, M, q)$, by Corollary 4.2.10, we know that $M^3 - 2qM^2 + 2q^2M - q^4 \leq 0$. Let $f(M) = M^3 - 2qM^2 + 2q^2M - q^4$, then the derivative of $f(M)$ is

$$\frac{df}{dM}(M) = 3M^2 - 4qM + 2q^2 = 3(M - \frac{2q}{3})^2 + \frac{2q^2}{3} > 0.$$

Therefore, f is a strictly increasing function on M. Let $q = ad$, where a and d are positive integers such that $d^2 - 2d + 2 - a = 0$. Then

$$\begin{aligned} f(ad^2) &= (ad^2)^3 - 2(ad)(ad^2)^2 + 2(ad)^2(ad^2) - (ad)^4 \\ &= a^3d^6 - 2a^3d^5 + 2a^3d^4 - a^4d^4 \\ &= a^3d^4(d^2 - 2d + 2 - a) \\ &= 0. \end{aligned}$$

For any $M' > ad^2$, we have $f(M') > 0$. So ad^2 is the greatest integer which satisfies the inequality $M^3 - 2qM^2 + 2q^2M - q^4 \leq 0$. This completes the proof. □

Therefore, we can derive optimal 3-MIPPCs.

Theorem 4.3.8 *There exists an optimal* 3-*MIPPC*$(2, (k^2+1)(k+1)^2, (k^2+1)(k+1))$ *for any prime power* k.

Proof: A 3-MIPPC$(2, (k^2+1)(k+1)^2, (k^2+1)(k+1))$ exists from Corollary 4.3.6. Let $a = k^2 + 1, d = k + 1$, then $d^2 - 2d + 2 - a = 0$. Apply Lemma 4.3.7. □

4.3.2 Asymptotically optimal 3-MIPPC$(2, M, q)$s

Corollaries 4.2.8 and 4.3.2 inspire us to construct optimal 3-MIPPC$(2, M, q)s$ via bipartite graphs with girth 8 or maximum $\triangle$-free generalized $(q, q, K, 1)$ packings. Unfortunately, except for the result in Theorem 4.3.8, we do not know other infinite families of optimal 3-MIPPC$(2, M, q)$s. However, we can construct several infinite families of asymptotically optimal 3-MIPPC$(2, M, q)$s by deleting points and lines from generalized quadrangles.

Theorem 4.3.9 *There exists a* 3-*MIPPC*$(2, k^4 + 2k^3 + 2k^2 + 2k - 2sk, k^3 + k^2 + k + 1 - s)$ *for every prime power* k*, where* $1 \leq s \leq k^2 + k + 1$.

Proof: If we can construct a $\triangle$-free generalized $(k^3 + k^2 + k + 1 - s, k^3 + k^2 + k + 1 - s, \{k, k+1\}, 1)$ packing with $k^3 + k^2 + k - sk$ blocks of size $k + 1$ and $sk - s + 1$ blocks of size k, then the conclusion would follow from Theorem 4.3.1. According to Lemma 4.3.5, there exists a GQ(k, k), say $\mathcal{S} = (X, \mathcal{B}, I)$, for every prime power k. Choose an arbitrary point $x_{0,0} \in X$. Let $L_{0,j} = \{x_{0,0}, x_{1,j}, \ldots, x_{k,j}\}$, $0 \leq j \leq k$, be the $k+1$ distinct lines incident with $x_{0,0}$, and $L_{i,1}, \ldots, L_{i,k}$, $1 \leq i \leq k$, be the other k distinct lines incident with $x_{i,0} \in X$. Let $s_1 = \lfloor \frac{s-1}{k} \rfloor$ and $s_2 = s - 1 - ks_1$. Then the desired $\triangle$-free generalized packing can be constructed by deleting s points $x_{0,0}$, $x_{1,0}$, $\ldots$, $x_{k,0}$, $x_{1,1}$, $\ldots$, $x_{k,1}$, $\ldots$, x_{1,s_1-1}, $\ldots$, x_{k,s_1-1}, x_{1,s_1}, $\ldots$, x_{s_2,s_1} and s lines $L_{0,0}, L_{0,1}, \ldots, L_{0,k}$, $L_{1,1}$, $\ldots$, $L_{1,k}$, $\ldots$, $L_{s_1-1,1}$, $\ldots$, $L_{s_1-1,k}$, $L_{s_1,1}$, $\ldots$, L_{s_1,s_2}, where the size of each line after deletion is $k+1$ or k because of the $\triangle$-freeness of the GQ. □

Theorem 4.3.10 *There exists a* 3*-MIPPC*$(2, k^4 - sk, k^3 - s)$ *for every prime power* k*, where* $0 \leq s \leq 2k-1$.

Proof: Similar to Theorem 4.3.9, we want to construct a $\triangle$-free generalized $(k^3 - s, k^3 - s, \{k\}, 1)$ packing. According to Lemma 4.3.5, there exists a GQ$(k-1, k+1)$, say $\mathcal{S} = (X, \mathcal{B}, I)$, for any prime power k. Then $|X| = k^3$ and $|\mathcal{B}| = k^3 + 2k^2$. Let $x_0 \in X$ and $X_0 = \{x \in X \setminus \{x_0\} \mid x_0$ and x are incident with a line$\}$. Then $|X_0| = k^2 + k - 2$. Let $X_s = \{x_0, x_1, \ldots, x_{s-1}\} \subseteq \{x_0\} \cup X_0$ and $\mathcal{B}_s = \{L \in \mathcal{B} \mid L$ is incident with a point $x \in X_s\}$. By a simple counting argument, we know that $|\mathcal{B}_s| = (k+2) + (s-1)(k+1) = s + sk + 1$. Then we can obtain a $\triangle$-free generalized $(v, b, k, 1)$ packing by deleting the s points in X_s and the $s + sk + 1$ lines in $\mathcal{B}_s$ from the GQ$(k-1, k+1)$, $\mathcal{S}$, where $v = k^3 - s$ and $b = k^3 - s + (2k^2 - sk - 1)$. Since $0 \leq s \leq 2k - 1$, we have $b \geq v$. Therefore the desired $\triangle$-free generalized packing exists by further deleting $b - v$ blocks of the $\triangle$-free generalized $(v, b, k, 1)$ packing. □

Theorem 4.3.11 *There exists a* 3*-MIPPC*$(2, k^4 + 2k^3 + 2k^2 - sk - s + \lfloor \frac{s-1}{k+1} \rfloor, k^3 + 2k^2 - s)$ *for every prime power* k*, where* $1 \leq s \leq k^2 + k + 1$.

Proof: According to Lemma 4.3.5 and the point-line duality of GQs (see, for example, [19]), there exists a GQ$(k+1, k-1)$ for any prime power k. Suppose that $\mathcal{S}$ is a GQ$(k+1, k-1)$. Then $|X| = k^3 + 2k^2$ and $|\mathcal{B}| = k^3$. Pick an arbitrary point $x \in X$. Suppose $L_i = \{x, x_{i,1}, \ldots, x_{i,k+1}\}$, $1 \leq i \leq k$, are k distinct lines containing x, and each P_i is the point-set of L_i. Let $s_1 = \lfloor \frac{s-1}{k+1} \rfloor$, $s_2 = s - 1 - s_1(k+1)$, and

$$\mathcal{P}_s = \begin{cases} \{x\}, & \text{if } \ s = 1, \\ \{x\} \bigcup (\bigcup_{i=1}^{s_1} P_i), \text{if } \ s \neq 1 \text{ and } s \equiv 1 \pmod{k+1}, \\ \{x\} \bigcup (\bigcup_{i=1}^{s_1} P_i) \bigcup \{x_{s_1+1,1}, \cdots, x_{s_1+1,s_2}\}, \text{otherwise}. \end{cases}$$

For a given s, we can delete the point-set $\mathcal{P}_s$ and derive a $\triangle$-free generalized $(v, b, \{k+1-s_2, k+1, k+2\}, 1)$ packing with $(s-1)(k-1) + k - s_1 - h(s_2)$ blocks of size $k+1$, $k^3 - k - (s-1)(k-1)$ blocks of size $k+2$, and $h(s_2)$ block of size $k + 1 - s_2$, where $v = k^3 + 2k^2 - s$, $b = k^3 - s_1$, and

$$h(s_2) = \begin{cases} 0, & \text{if } s_2 = 0, \\ 1, & \text{otherwise}. \end{cases}$$

Then $v-b=2k^2-s+s_1>0$. So, the desired generalized packing can be constructed by adding $v-b$ blocks containing exactly one point belonging to $X \setminus \mathcal{P}_s$. Now we compute the value M.

$$\begin{aligned} M &= [(s-1)(k-1)+k-s_1-h(s_2)](k+1) \\ &\quad + [k^3-k-(s-1)(k-1)](k+2) \\ &\quad + h(s_2)(k+1-s_2)+2k^2-s+s_1 \\ &= k^4+2k^3+2k^2-sk-s_1k-1-h(s_2)s_2. \end{aligned}$$

If $s_2 \neq 0$, then $h(s_2)s_2 = s_2$; if $s_2=0$, then $h(s_2)s_2 = 0 = s_2$. So

$$\begin{aligned} M = &\ k^4+2k^3+2k^2-sk-s_1k-1-s_2 \\ = &\ k^4+2k^3+2k^2-sk-s_1k-1-(s-1-s_1(k+1)) \\ = &\ k^4+2k^3+2k^2-sk-s-s_1 \\ = &\ k^4+2k^3+2k^2-sk-s-\lfloor\frac{s-1}{k+1}\rfloor. \end{aligned}$$

This completes the proof. □

Theorem 4.3.12 *The* 3-*MIPPC*$(2,M,q)$*s constructed in Theorems* 4.3.9, 4.3.10 and 4.3.11 *are asymptotically optimal.*

Proof: Here, we only prove that the 3-MIPPC$(2,M,q)$s constructed in Theorem 4.3.10 are asymptotically optimal. The other two cases can be proved in a similar way. Note that in Theorem 4.3.10, $q=k^3-s$, $M=k^4-sk$, where k is a prime power and $0 \leq s \leq 2k-1$.

Just as in the proof of Lemma 4.3.7, we consider the strictly increasing function $f(M)=M^3-2qM^2+2q^2M-q^4$, and also the cubic equation $f(M)=0$. Let $a=1, b=-2q, c=2q^2, d=-q^4$. Then the discriminant of the above-mentioned cubic equation is $D=18abcd-4b^3d+b^2c^2-4ac^3-27a^2d^2=q^6(40q-16-27q^2)<0$, which implies that this cubic equation has one real root M_0 and two complex conjugate roots (see, for example, [34], and also [42]), where

$$\begin{aligned} M_0 = &-\frac{b}{3a}-\frac{1}{3a}\sqrt[3]{\frac{1}{2}[2b^3-9abc+27a^2d+\sqrt{-27a^2D}]} \\ &-\frac{1}{3a}\sqrt[3]{\frac{1}{2}[2b^3-9abc+27a^2d-\sqrt{-27a^2D}]} \\ = &\ \frac{2q}{3}-\frac{q}{3}\sqrt[3]{\frac{1}{2}[20-27q+\sqrt{27(27q^2-40q+16)}]} \\ &-\frac{q}{3}\sqrt[3]{\frac{1}{2}[20-27q-\sqrt{27(27q^2-40q+16)}]}. \end{aligned}$$

Noting that $f(0) = -q^4 < 0$, we have $M_0 > 0$. By Corollary 4.2.10, $M_{MIPPC}(3,2,q) \leq M_0$, and then $0 < \frac{M}{M_0} \leq \frac{M}{M_{MIPPC}(3,2,q)} \leq 1$. Therefore it is sufficient to prove that $\lim\limits_{q\to\infty} \frac{M}{M_0} = 1$ holds.

Since $q = k^3 - s$, we have

$$\begin{aligned}
\lim_{q\to\infty} \frac{M_0}{k^4} &= \lim_{k\to\infty} \frac{M_0}{k^4} \\
&= \lim_{k\to\infty} \frac{2q}{3k^4} - \lim_{k\to\infty} \frac{q}{3k^4} \sqrt[3]{\frac{1}{2}[20 - 27q + \sqrt{27(27q^2 - 40q + 16)}]} \\
&\quad - \lim_{k\to\infty} \frac{q}{3k^4} \sqrt[3]{\frac{1}{2}[20 - 27q - \sqrt{27(27q^2 - 40q + 16)}]} \\
&= 0 - 0 - (-1) \\
&= 1,
\end{aligned}$$

then

$$\lim_{q\to\infty} \frac{M}{M_0} = \lim_{k\to\infty} \frac{M}{M_0} = \frac{\lim\limits_{k\to\infty} \frac{M}{k^4}}{\lim\limits_{k\to\infty} \frac{M_0}{k^4}} = \frac{1}{1} = 1.$$

This completes the proof. □

CHAPTER 5

Strong Multimedia Identifiable Parent Property Codes

From what has been discussed in Chapter 4, we know that any binary t-MIPPC can capture at least one colluder by applying Algorithm 4.1 if the number of colluders is less than or equal to t with computational complexity $O(nM^t)$, where n is the length of the code and M is the number of authorized users. Obviously, the computational complexity $O(nM^t)$ is not efficient for practical use. Therefore, we introduce the notion of a strong multimedia identifiable parent property code (t-SMIPPC) in this chapter. We show that any binary t-SMIPPC can be used to identify at least one colluder in the averaging attack by applying Algorithm 3.1 with computational complexity $O(nM)$, which is clearly more efficient than that of a t-MIPPC.

In Section 5.1, we introduce the notion of an SMIPPC, describe a colluder tracing algorithm based on a binary SMIPPC, and present a concatenation construction for binary SMIPPCs from q-ary SMIPPCs. In Section 5.2, we discuss the relationships between t-SMIPPCs and other fingerprinting codes, and derive several infinite series of optimal q-ary t-SMIPPCs of length 2 with $t = 2, 3$. In Section 5.3, we investigate combinatorial properties of q-ary 2-SMIPPCs of length 3, and optimal q-ary 2-SMIPPCs of length 3 with $q \equiv 0, 1, 2, 5 \pmod 6$ are constructed by means of difference matrices.

5.1 Tracing algorithm for strong multimedia identifiable parent property codes

In this section, we introduce a notion of an SMIPPC, describe a tracing algorithm based on a binary SMIPPC, and show a concatenation construction for binary SMIPPCs from q-ary SMIPPCs.

Definition 5.1.1 *Let $\mathcal{C}$ be an (n, M, q) code, and $t \geq 2$ be an integer. $\mathcal{C}$ is a strong multimedia identifiable parent property code, or t-SMIPPC(n, M, q), if for any $\mathcal{C}_0 \subseteq \mathcal{C}$, $1 \leq |\mathcal{C}_0| \leq t$, we have $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}' \neq \emptyset$, where $S(\mathcal{C}_0) = \{\mathcal{C}' \subseteq \mathcal{C} \mid \mathsf{desc}(\mathcal{C}') = \mathsf{desc}(\mathcal{C}_0)\}$.*

Example 5.1.2 Consider the following $(3, 4, 2)$ code $\mathcal{C}$:

$$\begin{array}{cc} & \begin{array}{cccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 \end{array} \\ \mathcal{C} = & \left(\begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array}\right) \end{array}$$

Then

$$\begin{aligned}
\mathsf{desc}(\{\mathbf{c}_1\}) &= \{1\} \times \{0\} \times \{0\},\\
\mathsf{desc}(\{\mathbf{c}_2\}) &= \{0\} \times \{1\} \times \{1\},\\
\mathsf{desc}(\{\mathbf{c}_3\}) &= \{0\} \times \{0\} \times \{1\},\\
\mathsf{desc}(\{\mathbf{c}_4\}) &= \{0\} \times \{1\} \times \{0\},\\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) &= \{0, 1\} \times \{0, 1\} \times \{0, 1\},\\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_3\}) &= \{0, 1\} \times \{0\} \times \{0, 1\},\\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_4\}) &= \{0, 1\} \times \{0, 1\} \times \{0\},\\
\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3\}) &= \{0\} \times \{0, 1\} \times \{1\},\\
\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_4\}) &= \{0\} \times \{1\} \times \{0, 1\},\\
\mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_4\}) &= \{0\} \times \{0, 1\} \times \{0, 1\},\\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}) &= \{0, 1\} \times \{0, 1\} \times \{0, 1\},\\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4\}) &= \{0, 1\} \times \{0, 1\} \times \{0, 1\},\\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4\}) &= \{0, 1\} \times \{0, 1\} \times \{0, 1\},\\
\mathsf{desc}(\{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}) &= \{0\} \times \{0, 1\} \times \{0, 1\},\\
\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}) &= \{0, 1\} \times \{0, 1\} \times \{0, 1\}.
\end{aligned}$$

It is easy to check that

$S(\{\mathbf{c}_1\}) = \{\{\mathbf{c}_1\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_1\})} \mathcal{C}' = \{\mathbf{c}_1\} \neq \emptyset$,

$S(\{\mathbf{c}_2\}) = \{\{\mathbf{c}_2\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_2\})} \mathcal{C}' = \{\mathbf{c}_2\} \neq \emptyset$,

$S(\{\mathbf{c}_3\}) = \{\{\mathbf{c}_3\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_3\})} \mathcal{C}' = \{\mathbf{c}_3\} \neq \emptyset$,

$S(\{\mathbf{c}_4\}) = \{\{\mathbf{c}_4\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_4\})} \mathcal{C}' = \{\mathbf{c}_4\} \neq \emptyset$,

$S(\{\mathbf{c}_1, \mathbf{c}_2\}) = \{\{\mathbf{c}_1, \mathbf{c}_2\}, \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}, \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_4\}, \{\mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4\}, \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_1, \mathbf{c}_2\})} \mathcal{C}' = \{\mathbf{c}_1\} \neq \emptyset$,

$S(\{\mathbf{c}_1, \mathbf{c}_3\}) = \{\{\mathbf{c}_1, \mathbf{c}_3\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_1, \mathbf{c}_3\})} \mathcal{C}' = \{\mathbf{c}_1, \mathbf{c}_3\} \neq \emptyset$,

$S(\{\mathbf{c}_1, \mathbf{c}_4\}) = \{\{\mathbf{c}_1, \mathbf{c}_4\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_1, \mathbf{c}_4\})} \mathcal{C}' = \{\mathbf{c}_1, \mathbf{c}_4\} \neq \emptyset$,

$S(\{\mathbf{c}_2, \mathbf{c}_3\}) = \{\{\mathbf{c}_2, \mathbf{c}_3\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_2, \mathbf{c}_3\})} \mathcal{C}' = \{\mathbf{c}_2, \mathbf{c}_3\} \neq \emptyset$,

$S(\{\mathbf{c}_2, \mathbf{c}_4\}) = \{\{\mathbf{c}_2, \mathbf{c}_4\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_2, \mathbf{c}_4\})} \mathcal{C}' = \{\mathbf{c}_2, \mathbf{c}_4\} \neq \emptyset$,

$S(\{\mathbf{c}_3, \mathbf{c}_4\}) = \{\{\mathbf{c}_3, \mathbf{c}_4\}, \{\mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}\}$ and $\bigcap_{\mathcal{C}' \in S(\{\mathbf{c}_3, \mathbf{c}_4\})} \mathcal{C}' = \{\mathbf{c}_3, \mathbf{c}_4\} \neq \emptyset$.

So the code $\mathcal{C}$ is a 2-SMIPPC$(3,4,2)$.

The following relationship immediately comes from Definitions 3.1.1 and 5.1.1.

Lemma 5.1.3 *Any $\bar{t}$-SSC(n,M,q) is a t-SMIPPC(n,M,q).*

The following is an equivalent definition of an SMIPPC.

Definition 5.1.4 *Let $\mathcal{C}$ be an (n,M,q) code, and $t \geq 2$ be an integer. For any $R \subseteq \mathcal{C}(1) \times \cdots \times \mathcal{C}(n)$, define the set of parent sets of R as*

$$\mathcal{P}(R) = \{\mathcal{C}^{'} \subseteq \mathcal{C} \mid \mathsf{desc}(\mathcal{C}^{'}) = R\}.$$

We say $\mathcal{C}$ is a strong multimedia identifiable parent property code, or t-SMIPPC$(n,M,$ $q)$, if $\bigcap_{\mathcal{C}' \in \mathcal{P}(R)} \mathcal{C}^{'} \neq \emptyset$ is satisfied for all $R \subseteq \mathcal{C}(1) \times \cdots \times \mathcal{C}(n)$ with $\mathcal{P}_t(R) \neq \emptyset$, where $\mathcal{P}_t(R) = \{\mathcal{C}^{'} \subseteq \mathcal{C} \mid |\mathcal{C}^{'}| \leq t, \mathsf{desc}(\mathcal{C}^{'}) = R\}$.

We can also derive the following relationship from Definitions 4.1.1 and 5.1.4.

Lemma 5.1.5 *Any t-SMIPPC(n,M,q) is a t-MIPPC(n,M,q).*

The following theorem shows that a t-SMIPPC$(n,M,2)$ can be used to identify at least one colluder in the averaging attack with computational complexity $O(nM)$, which is more efficient than that of a t-MIPPC$(n,M,2)$. We in fact use Algorithm 3.1 in Section 3.1.

Theorem 5.1.6 *Under the assumption that the number of colluders in the averaging attack is at most t, any t-SMIPPC$(n,M,2)$ can be used to identify at least one colluder with computational complexity $O(nM)$ by applying Algorithm 3.1.*

Proof: Let $\mathcal{C}$ be the t-SMIPPC$(n,M,2)$, and R be the descendant code derived from the detection statistics $\mathbf{T}$. Then by applying Algorithm 3.1, one can identify at least one colluder. The computational complexity is clearly $O(nM)$.

According to Algorithm 3.1, by deleting all columns $\{\mathbf{c} \in \mathcal{C} \mid \exists\, 1 \leq i \leq n, R(i) = \{1\}, \mathbf{c}(i) = 0,\ \text{or}\ R(i) = \{0\}, \mathbf{c}(i) = 1\}$, we obtain a sub-matrix $\mathcal{C}_L$ of $\mathcal{C}$. Suppose that $C_0 = \{u_1, u_2, \ldots, u_r\}$, $1 \leq r \leq t$, is the set of colluders, the codeword $\mathbf{c}_i$ is assigned to the colluder u_i, $1 \leq i \leq r$, and $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_r\}$. It is not difficult to see that $\mathcal{C}_0 \subseteq \mathcal{C}_L$. According to the definition of a t-SMIPPC, we have $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$, where $S(\mathcal{C}_0) = \{\mathcal{C}^{'} \subseteq \mathcal{C} \mid \mathsf{desc}(\mathcal{C}^{'}) = \mathsf{desc}(\mathcal{C}_0) = R\}$. We prove this theorem in three steps.

(1) $\mathcal{C}_L \in S(\mathcal{C}_0)$, that is $\mathsf{desc}(\mathcal{C}_L) = R$. For any $1 \leq j \leq n$, we consider the following cases.

(1.1) $R(j) = \{1\}$. For any $\mathbf{c} \in \mathcal{C}_L$, $\mathbf{c}(j) = 1$ according to the processes deriving $\mathcal{C}_L$. So, $\mathcal{C}_L(j) = \{1\} = R(j)$.

(1.2) $R(j) = \{0\}$. For any $\mathbf{c} \in \mathcal{C}_L$, $\mathbf{c}(j) = 0$ according to the processes deriving $\mathcal{C}_L$. So, $\mathcal{C}_L(j) = \{0\} = R(j)$.

(1.3) $R(j) = \{0, 1\}$. Since $\mathsf{desc}(\mathcal{C}_0) = R$, we know that there exist $\mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}_0 \subseteq \mathcal{C}_L$ such that $\mathbf{c}_1(j) = 0$ and $\mathbf{c}_2(j) = 1$, respectively. This implies $\mathcal{C}_L(j) = \{0, 1\} = R(j)$.

According to (1.1)-(1.3) above, for any $1 \leq j \leq n$, we have $\mathcal{C}_L(j) = R(j)$, which implies $\mathsf{desc}(\mathcal{C}_L) = R$.

(2) We want to show that for any $\mathbf{x} \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$, there exists $1 \leq j \leq n$, such that $\mathbf{x}(j) = 1$ and $\mathbf{c}(j) = 0$ for any $\mathbf{c} \in \mathcal{C}_L \setminus \{\mathbf{x}\}$, or $\mathbf{x}(j) = 0$ and $\mathbf{c}(j) = 1$ for any $\mathbf{c} \in \mathcal{C}_L \setminus \{\mathbf{x}\}$. Assume not. Then for any $1 \leq j \leq n$, $\mathbf{x}(j) = 1$ implies that there exists $\mathbf{c}_1 \in \mathcal{C}_L \setminus \{\mathbf{x}\}$ such that $\mathbf{c}_1(j) = 1$, and $\mathbf{x}(j) = 0$ implies that there exists $\mathbf{c}_2 \in \mathcal{C}_L \setminus \{\mathbf{x}\}$ such that $\mathbf{c}_2(j) = 0$. Then we have $\mathsf{desc}(\mathcal{C}_L) = \mathsf{desc}(\mathcal{C}_L \setminus \{\mathbf{x}\})$. Since $\mathcal{C}_L \in S(\mathcal{C}_0)$ by (1), we can have $\mathcal{C}_L \setminus \{\mathbf{x}\} \in S(\mathcal{C}_0)$, and $\mathbf{x} \notin \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$, a contradiction.

(3) At last, according to Algorithm 3.1 and (2), it suffices to show that any user u assigned with a codeword $\mathbf{x} \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$ is a colluder. Assume that u is not a colluder. Then for any $\mathcal{C}^{'} \in S(\mathcal{C}_0)$, we have $\mathcal{C}^{'} \setminus \{\mathbf{x}\} \in S(\mathcal{C}_0)$, which implies $\mathbf{x} \notin \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$, a contradiction.

This completes the proof. □

The following is a concatenation construction for binary t-SMIPPCs from q-ary t-SMIPPCs, which makes the research of q-ary t-SMIPPCs interesting.

Lemma 5.1.7 *If there exists a t-SMIPPC(n, M, q), then there exists a t-SMIPPC$(nq, M, 2)$.*

Proof: Let $\mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \ldots, \mathbf{c}_M\}$ be a t-SMIPPC(n, M, q) defined on $Q = \{0, 1, \ldots, q-1\}$, and $\mathcal{E} = \{\mathbf{e}_1, \mathbf{e}_2, \ldots, \mathbf{e}_q\}$, where $\mathbf{e}_i$ is the i-th column identity vector, i.e., all its coordinates are 0 except the i-th one being 1. Let $f : Q \longrightarrow \mathcal{E}$ be the bijective mapping such that $f(i) = \mathbf{e}_{i+1}$. For any codeword $\mathbf{c} = (\mathbf{c}(1), \mathbf{c}(2), \ldots, \mathbf{c}(n))^T \in \mathcal{C}$, we define $f(\mathbf{c}) = (f(\mathbf{c}(1)), f(\mathbf{c}(2)), \ldots, f(\mathbf{c}(n)))^T$. Obviously, $f(\mathbf{c})$ is a binary column vector of length nq. We define a new $(nq, M, 2)$ code $\mathcal{F} = \{f(\mathbf{c}_1), f(\mathbf{c}_2), \ldots, f(\mathbf{c}_M)\}$. We are going to show that $\mathcal{F}$ is in fact a t-SMIPPC.

Consider any $\mathcal{F}_0 \subseteq \mathcal{F}$ with $|\mathcal{F}_0| \leq t$, and $S(\mathcal{F}_0) = \{\mathcal{F}^{'} \subseteq \mathcal{F} \mid \mathsf{desc}(\mathcal{F}^{'}) = \mathsf{desc}(\mathcal{F}_0)\} = \{\mathcal{F}_0, \mathcal{F}_1, \ldots, \mathcal{F}_r\}$. Each $\mathcal{F}_i$ corresponds to a subcode $\mathcal{C}_i \subseteq \mathcal{C}$ such that $|\mathcal{C}_i| = |\mathcal{F}_i|$, where $\mathcal{F}_i = \{f(\mathbf{c}) \mid \mathbf{c} \in \mathcal{C}_i\}$. Since $\mathsf{desc}(\mathcal{F}_0) = \mathsf{desc}(\mathcal{F}_1) = \cdots = \mathsf{desc}(\mathcal{F}_r)$, we immediately have $\mathsf{desc}(\mathcal{C}_0) = \mathsf{desc}(\mathcal{C}_1) = \cdots = \mathsf{desc}(\mathcal{C}_r)$. Since $\mathcal{C}$ is a t-SMIPPC(n, M, q) and $|\mathcal{C}_0| = |\mathcal{F}_0| \leq t$, we have $\bigcap_{i=0}^r \mathcal{C}_i \neq \emptyset$. Let $\mathbf{c} \in \bigcap_{i=0}^r \mathcal{C}_i$, then $\mathbf{c} \in \mathcal{C}_i$ for any $0 \leq i \leq r$, which implies $f(\mathbf{c}) \in \mathcal{F}_i$ for any $0 \leq i \leq r$, and thus $f(\mathbf{c}) \in \bigcap_{i=0}^r \mathcal{F}_i$. Therefore, $\bigcap_{i=0}^r \mathcal{F}_i \neq \emptyset$. This completes the proof. □

5.2 Optimal t-SMIPPC$(2, M, q)$s with small t

Similar to the definition of optimal SCs, we can define optimal t-SMIPPCs. Let $M_{SMIPPC}(t, n, q) = \max\{M \mid \text{there exists a } t\text{-SMIPPC}(n, M, q)\}$. A t-SMIPPC(n, M, q) is said to be optimal if $M = M_{SMIPPC}(t, n, q)$. In this section, we establish two equivalences in Corollary 5.2.2 and Theorem 5.2.4, respectively. Based on these two relationships and the known results in Theorems 2.2.22 and 4.3.8, several infinite series of optimal t-SMIPPC$(2, M, q)$s with $t = 2, 3$ are derived.

Theorem 5.2.1 *Let $\mathcal{C}$ be a $(2, M, q)$ code. Then $\mathcal{C}$ is a 2-SMIPPC$(2, M, q)$ if and only if it is a 2-MIPPC$(2, M, q)$.*

Proof: According to Lemma 5.1.5, it suffices to consider the sufficiency. Let $\mathcal{C}$ be a 2-MIPPC$(2, M, q)$, which implies that $\mathcal{C}$ is a $\overline{2}$-SC$(2, M, q)$ from Lemma 4.1.4. Assume that $\mathcal{C}$ is not a 2-SMIPPC$(2, M, q)$. Then there exists $\mathcal{C}_0 \subseteq \mathcal{C}$, $1 \leq |\mathcal{C}_0| \leq 2$, such that $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}' = \emptyset$, where $S(\mathcal{C}_0) = \{\mathcal{C}' \subseteq \mathcal{C} \mid \mathsf{desc}(\mathcal{C}') = \mathsf{desc}(\mathcal{C}_0)\}$. If $|\mathcal{C}_0| = 1$, then it is clear that $S(\mathcal{C}_0) = \{\mathcal{C}_0\}$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}' = \mathcal{C}_0 \neq \emptyset$, a contradiction. So $|\mathcal{C}_0| = 2$. Let $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\}$, $\mathbf{c}_i = (a_i, b_i)^T$, where $i = 1, 2$. Obviously, for any $\mathcal{C}' \in S(\mathcal{C}_0)$, we have $\mathcal{C}' \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. We now consider the Hamming distance $d(\mathbf{c}_1, \mathbf{c}_2)$ of $\mathbf{c}_1$ and $\mathbf{c}_2$.

(1) If $d(\mathbf{c}_1, \mathbf{c}_2) = 1$, we may assume $a_1 = a_2$, $b_1 \neq b_2$. We can easily see that $S(\mathcal{C}_0) = \{\mathcal{C}_0\}$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}' = \mathcal{C}_0 \neq \emptyset$, a contradiction. So this case is impossible.

(2) If $d(\mathbf{c}_1, \mathbf{c}_2) = 2$, then $a_1 \neq a_2$, $b_1 \neq b_2$, and $\mathsf{desc}(\mathcal{C}_0) = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, where $\mathbf{c}_3 = (a_1, b_2)^T$ and $\mathbf{c}_4 = (a_2, b_1)^T$. Then $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| \leq 3$. Otherwise, if $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| = 4$, i.e., $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3, \mathbf{c}_4\}$, then $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{\mathbf{c}_3, \mathbf{c}_4\})$, a contradiction to the fact that $\mathcal{C}$ is a $\overline{2}$-SC. Since $\mathcal{C}$ is a $\overline{2}$-SC$(2, M, q)$, for any $\mathcal{C}' \in S(\mathcal{C}_0)$, $\mathcal{C}' \neq \mathcal{C}_0$, we have $|\mathcal{C}'| \geq 3$. Together with the facts $\mathcal{C}' \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ and $|\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}| \leq 3$, one can derive $\mathcal{C}' = \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. Hence $\mathcal{C}_0 \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \mathcal{C}'$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}' = \mathcal{C}_0 \neq \emptyset$, a contradiction. So this case is impossible.

This completes the proof. □

The following result comes from Lemma 4.1.4 and Theorem 5.2.1.

Corollary 5.2.2 *Let $\mathcal{C}$ be an (n, M, q) code. Then $\mathcal{C}$ is a 2-SMIPPC$(2, M, q)$ if and only if it is a $\overline{2}$-SC$(2, M, q)$.*

Thus, according to Theorem 2.2.22 and Corollary 5.2.2, one can obtain optimal 2-SMIPPC$(2, M, q)$s.

Corollary 5.2.3 *Let $k \geq 2$ be a prime power. Then there is an optimal 2-SMIPPC$(2, M, q)$ for any $q \in \{k^2 - 1, k^2 + k - 2, k^2 + k - 1, k^2 + k, k^2 + k + 1\}$.*

Similarly, we also find an equivalence between a 3-SMIPPC$(2, M, q)$ and a 3-MIPPC$(2, M, q)$ as follows.

Theorem 5.2.4 *Let $\mathcal{C}$ be an $(2, M, q)$ code. Then $\mathcal{C}$ is a 3-SMIPPC$(2, M, q)$ if and only if it is a 3-MIPPC$(2, M, q)$.*

Proof: By Lemma 5.1.5, it suffices to consider the sufficiency. Suppose that $\mathcal{C}$ is a 3-MIPPC$(2, M, q)$. Then $\mathcal{C}$ is also a 2-MIPPC$(2, M, q)$, which implies that $\mathcal{C}$ is a 2-SMIPPC$(2, M, q)$ from Theorem 5.2.1. Assume that $\mathcal{C}$ is not a 3-SMIPPC$(2, M, q)$. Then there exists $\mathcal{C}_0 \subseteq \mathcal{C}$, $1 \le |\mathcal{C}_0| \le 3$, such that $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} = \emptyset$, where $S(\mathcal{C}_0) = \{\mathcal{C}^{'} \subseteq \mathcal{C} \mid \mathsf{desc}(\mathcal{C}^{'}) = \mathsf{desc}(\mathcal{C}_0)\}$. Obviously, for any $\mathcal{C}^{'} \in S(\mathcal{C}_0)$, we have $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. Then, at least one of the following cases should occur. However, we can prove none of them is possible.

(1) $1 \le |\mathcal{C}_0| \le 2$. Since $\mathcal{C}$ is a 2-SMIPPC$(2, M, q)$, $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$, a contradiction. So this case is impossible.

(2) If $|\mathcal{C}_0| = 3$, then let $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}$, where $\mathbf{c}_i = (a_i, b_i)^T$, $1 \le i \le 3$.

(2.1) If $a_1 = a_2 = a_3$, then $b_i \neq b_j$, $1 \le i < j \le 3$. We can easily see that $S(\mathcal{C}_0) = \{\mathcal{C}_0\}$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} = \mathcal{C}_0 \neq \emptyset$, a contradiction. So this case is impossible.

(2.2) If $a_1 = a_2 \neq a_3$, then $b_1 \neq b_2$. Let $\mathcal{C}_1 = (\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}) \backslash \mathcal{C}_0$. Then $b_1 \notin \mathcal{C}_1(2)$ or $b_2 \notin \mathcal{C}_1(2)$. Otherwise, $b_1, b_2 \in \mathcal{C}_1(2)$, which implies that $(a_3, b_1)^T, (a_3, b_2)^T \in \mathcal{C}$. Then we have $\mathsf{desc}(\{\mathbf{c}_1, (a_3, b_2)^T\}) = \mathsf{desc}(\{\mathbf{c}_2, (a_3, b_1)^T\})$, and $\{\mathbf{c}_1, (a_3, b_2)^T\} \bigcap \{\mathbf{c}_2, (a_3, b_1)^T\} = \emptyset$, a contradiction to the definition of a 3-MIPPC.

(2.2.A) If $b_1 \notin \mathcal{C}_1(2)$, then $\mathbf{c}_1$ is the only codeword such that $\mathbf{c}_1 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ and $\mathbf{c}_1(2) = b_1$. Since $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, we should have $\mathbf{c}_1 \in \mathcal{C}^{'}$ for any $\mathcal{C}^{'} \in S(\mathcal{C}_0)$. Otherwise, if $\mathbf{c}_1 \notin \mathcal{C}^{'}$, then $b_1 \notin \mathcal{C}^{'}(2)$, which implies $\mathsf{desc}(\mathcal{C}^{'}) \neq \mathsf{desc}(\mathcal{C}_0)$ as $b_1 \in \mathcal{C}_0(2)$, a contradiction. So, in this case, $\mathbf{c}_1 \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$, a contradiction to the assumption. So this case is impossible.

(2.2.B) If $b_2 \notin \mathcal{C}_1(2)$, similar to (2.2.A), we can have $\mathbf{c}_2 \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$, a contradiction to the assumption. So this case is impossible.

(2.3) If $a_i \neq a_j$, $1 \le i < j \le 3$, we only need to consider the case $b_i \neq b_j$, $1 \le i < j \le 3$, because we can consider the other two cases in a similar way with (2.1) and (2.2). In this case, we have

$$\mathsf{desc}(\mathcal{C}_0) = \begin{array}{ccc|cccccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 & \mathbf{c}_6 & \mathbf{c}_7 & \mathbf{c}_8 & \mathbf{c}_9 \\ a_1 & a_2 & a_3 & a_1 & a_1 & a_2 & a_2 & a_3 & a_3 \\ b_1 & b_2 & b_3 & b_2 & b_3 & b_1 & b_3 & b_1 & b_2 \end{array}$$

If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \mathcal{C}_0$, we can check that for any $\mathcal{C}^{'} \in S(\mathcal{C}_0)$, $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}^{'}) \bigcap \mathcal{C} = \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \mathcal{C}_0$, then $|\mathcal{C}^{'}| \le |\mathcal{C}_0| = 3$, and hence $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$ as $\mathcal{C}$ is a 3-MIPPC, a contradiction to the assumption. So $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ contains at least one of the words $\mathbf{c}_4, \mathbf{c}_5, \mathbf{c}_6, \mathbf{c}_7, \mathbf{c}_8, \mathbf{c}_9$. Without loss of generality, we only need to consider the case $\mathbf{c}_4 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. Then $\mathbf{c}_6 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, otherwise, $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{\mathbf{c}_4, \mathbf{c}_6\})$, and $\{\mathbf{c}_1, \mathbf{c}_2\} \bigcap \{\mathbf{c}_4, \mathbf{c}_6\} = \emptyset$, a contradiction to the definition of a 3-MIPPC. We are going to show that $\mathbf{c}_7, \mathbf{c}_8 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. If $\mathbf{c}_7 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ (or $\mathbf{c}_8 \notin \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$), then for any $\mathcal{C}' \in S(\mathcal{C}_0)$, we have $\mathbf{c}_2 \in \mathcal{C}'$ (or $\mathbf{c}_1 \in \mathcal{C}'$), otherwise, $a_2 \notin \mathcal{C}'(1)$ (or $b_1 \notin \mathcal{C}'(2)$), which implies $\mathsf{desc}(\mathcal{C}') \neq \mathsf{desc}(\mathcal{C}_0)$ as $a_2 \in \mathcal{C}_0(1)$ (or $b_1 \in \mathcal{C}_0(2)$). Hence $\mathbf{c}_2 \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}'$ (or $\mathbf{c}_1 \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}'$), which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}' \neq \emptyset$, a contradiction to the assumption. So, $\mathbf{c}_4, \mathbf{c}_7, \mathbf{c}_8 \in \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$. Then $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\}) = \mathsf{desc}(\{\mathbf{c}_4, \mathbf{c}_7, \mathbf{c}_8\})$, while $\{\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3\} \bigcap \{\mathbf{c}_4, \mathbf{c}_7, \mathbf{c}_8\} = \emptyset$, a contradiction to the definition of a 3-MIPPC. So this case is impossible.

This completes the proof. □

The above theorem shows that the optimal 3-MIPPCs of length 2 in Theorem 4.3.8 are in fact optimal 3-SMIPPCs of length 2.

Corollary 5.2.5 *There exists an optimal* 3-*SMIPPC*$(2, (k^2+1)(k+1)^2, (k^2+1)(k+1))$ *for any prime power* k.

5.3 Optimal 2-SMIPPC$(3, M, q)$s

In this section, we will investigate combinatorial properties of a 2-SMIPPC$(3, M, q)$, and then derive forbidden configurations of a 2-SMIPPC$(3, M, q)$. Optimal 2-SMIPPC$(3, M, q)$s are also constructed for each $q \equiv 0, 1, 2, 5 \pmod 6$.

5.3.1 General idea

At first, one can easily derive the following result from Lemmas 5.1.5 and 4.1.4.

Corollary 5.3.1 *Any* 2-*SMIPPC*(n, M, q) *is a* $\overline{2}$-*SC*(n, M, q).

Lemma 5.3.2 ([16]) *For any* $\overline{2}$-*SC*$(3, M, q)$, *we have* $M \leq q^2 + \frac{q(q-1)}{2}$.

Then an upper bound on the size of a 2-SMIPPC$(3, M, q)$ can be derived by Corollary 5.3.1 and Lemma 5.3.2.

Theorem 5.3.3 *For any* 2-*SMIPPC*$(3, M, q)$, *we have* $M \leq q^2 + \frac{q(q-1)}{2}$.

Next, we try to find out forbidden configurations of a 2-SMIPPC$(3, M, q)$.

Theorem 5.3.4 *Let* $\mathcal{C}$ *be a* $\overline{2}$-*SC*$(3, M, q)$. *Then* $\mathcal{C}$ *is a* 2-*SMIPPC*$(3, M, q)$ *if and only if for any* $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}$, *where* $a_1 \neq a_2$,

$b_1 \neq b_2$, and $e_1 \neq e_2$, we have $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is not of type **IV** *mentioned in Lemma* 3.3.2:

$$\left(\begin{array}{cc|ccc} a_1 & a_2 & a_1 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 & b_1 \\ e_1 & e_2 & e_2 & e_1 & e_1 \end{array}\right)$$

Proof: Suppose that $\mathcal{C}$ is a 2-SMIPPC$(3, M, q)$. If there exists $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}$, where $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$, such that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of type **IV**, then we can derive that $\mathsf{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \mathsf{desc}(\{(a_1, b_1, e_2)^T, (a_1, b_2, e_1)^T, (a_2, b_1, e_1)^T\})$, while $\{\mathbf{c}_1, \mathbf{c}_2\} \bigcap \{(a_1, b_1, e_2)^T, (a_1, b_2, e_1)^T, (a_2, b_1, e_1)^T\} = \emptyset$, a contradiction to the definition of a 2-SMIPPC.

Conversely, suppose that $\mathcal{C}$ is a $\overline{2}$-SC$(3, M, q)$, and for any $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}$, where $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$, we have $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is not of type **IV**. We will show $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$.

(1) If for any $\mathcal{C}^{'} \in S(\mathcal{C}_0)$, we have $\mathcal{C}_0 \subseteq \mathcal{C}^{'}$, then $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} = \mathcal{C}_0 \neq \emptyset$.

(2) If there exists $\mathcal{C}^{''} \in S(\mathcal{C}_0)$ such that $\mathcal{C}_0 \nsubseteq \mathcal{C}^{''}$, then by Lemma 3.3.2, we know that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of one of the four types mentioned in Lemma 3.3.2. Since $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is not type **IV**, we know that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of one of the types **I**, **II**, **III**.

(2.1) If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of type **I**, then for any $\mathcal{C}^{'} \in S(\mathcal{C}_0)$, we have $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, and thus $\mathbf{c}_2 \in \mathcal{C}^{'}$, otherwise, $a_2 \notin \mathcal{C}^{'}(1)$, which implies $\mathsf{desc}(\mathcal{C}^{'}) \neq \mathsf{desc}(\mathcal{C}_0)$, that is $\mathcal{C}^{'} \notin S(\mathcal{C}_0)$, a contradiction. So we have $\mathbf{c}_2 \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$.

(2.2) If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of type **II**, then for any $\mathcal{C}^{'} \in S(\mathcal{C}_0)$, we have $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, and thus $\mathbf{c}_2 \in \mathcal{C}^{'}$, otherwise, $b_2 \notin \mathcal{C}^{'}(2)$, which implies $\mathsf{desc}(\mathcal{C}^{'}) \neq \mathsf{desc}(\mathcal{C}_0)$, that is $\mathcal{C}^{'} \notin S(\mathcal{C}_0)$, a contradiction. So we have $\mathbf{c}_2 \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$.

(2.3) If $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of type **III**, then for any $\mathcal{C}^{'} \in S(\mathcal{C}_0)$, we have $\mathcal{C}^{'} \subseteq \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$, and thus $\mathbf{c}_2 \in \mathcal{C}^{'}$, otherwise, $e_2 \notin \mathcal{C}^{'}(3)$, which implies $\mathsf{desc}(\mathcal{C}^{'}) \neq \mathsf{desc}(\mathcal{C}_0)$, that is $\mathcal{C}^{'} \notin S(\mathcal{C}_0)$, a contradiction. So we have $\mathbf{c}_2 \in \bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'}$, which implies $\bigcap_{\mathcal{C}' \in S(\mathcal{C}_0)} \mathcal{C}^{'} \neq \emptyset$.

Therefore, $\mathcal{C}$ is a 2-SMIPPC$(3, M, q)$. □

Now we turn our attention to the constructions of 2-SMIPPC$(3, M, q)$s. Let us start from the definition of a difference matrix.

Definition 5.3.5 *A cyclic difference matrix $(q, k, 1)$-CDM is a $k \times q$ matrix $D = (d_{ij})$ with $d_{ij} \in Z_q$ such that for any $1 \leq i_1 \neq i_2 \leq k$, the differences $d_{i_1 j} - d_{i_2 j}$, $1 \leq j \leq q$, comprise all the elements of Z_q.*

Similar to [16], suppose that there exists a $(q, 3, 1)$-CDM D. Without loss of generality, we may assume that

$$D = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & q-1 \\ x_0 & x_1 & \cdots & x_{q-1} \end{pmatrix}. \tag{5.1}$$

Let S be a $3 \times w$ matrix on Z_q as follows.

$$S = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ s_1 & s_2 & \cdots & s_w \\ t_1 & t_2 & \cdots & t_w \end{pmatrix}. \tag{5.2}$$

Let

$$\mathcal{C}_D = \{\mathbf{c} + g \mid \mathbf{c} \in D, g \in Z_q\}, \mathcal{C}_S = \{\mathbf{c} + g \mid \mathbf{c} \in S, g \in Z_q\}, \mathcal{C} = \mathcal{C}_D \bigcup \mathcal{C}_S. \tag{5.3}$$

Theorem 5.3.6 ([16]) *Suppose that D is a $(q,3,1)$-CDM in the form (5.1) and S is a $3 \times w$ matrix in the form (5.2), where $|\{s_1, s_2, \ldots, s_w\}| = |\{t_1, t_2, \ldots, t_w\}| = |\{t_1 - s_1, t_2 - s_2, \ldots, t_w - s_w\}| = w$. Then, the following two statements are equivalent:*

(1) *$\mathcal{C}$ in the form (5.3) is a $\overline{2}$-SC$(3, q(q+w), q)$;*

(2) *For any two columns $(0, s_i, t_i)^T$ and $(0, s_j, t_j)^T$ in S, $1 \le i \ne j \le w$, suppose $(0, y, x_y)^T$, $(0, z, x_z)^T$, $(0, y_i, x_{y_i})^T$, $(0, y_j, x_{y_j})^T$, $(0, z_i, x_{z_i})^T$, $(0, z_j, x_{z_j})^T \in D$, where $y, z, y_i, y_j, z_i, z_j \in Z_q$, such that*

$$\begin{cases} t_i - s_i = x_y - y, \\ t_j - s_j = x_z - z, \\ t_i = x_{y_i}, \\ t_j = x_{y_j}, \\ s_i = z_i, \\ s_j = z_j. \end{cases}$$

Then we have $0 \notin \{t_i - x_y, t_j - x_z, (t_i - x_y) \pm (t_j - x_z), s_i - y_i, s_j - y_j, (s_i - y_i) \pm (s_j - y_j), t_i - x_{z_i}, t_j - x_{z_j}, (t_i - x_{z_i}) \pm (t_j - x_{z_j})\}$.

Theorem 5.3.7 *Suppose that $\mathcal{C}$ is a $\overline{2}$-SC$(3, q(q+w), q)$ in the form (5.3) on Z_q, and $E = \{(y, x_y) \mid y \in Z_q\} \bigcup \{(s_i, t_i) \mid 1 \le i \le w\}$. Then $\mathcal{C}$ is a 2-SMIPPC$(3, q(q+w), q)$ provided that the following hold:*

(I) *There do not exist distinct $1 \le i_1, i_2, i_3 \le w$ and $y \in Z_q$, such that*

$$\begin{cases} y = s_{i_1}, \\ x_y = t_{i_2}, \\ x_y - y = t_{i_3} - s_{i_3}, \\ (s_{i_2} + t_{i_3} - x_y, t_{i_1} + t_{i_3} - x_y) \in E. \end{cases}$$

(II) *There do not exist distinct* $y_1, y_2, y_3 \in Z_q$ *and* $1 \leq i \leq w$*, such that*

$$\begin{cases} s_i = y_1, \\ t_i = x_{y_2}, \\ t_i - s_i = x_{y_3} - y_3, \\ (y_2 + x_{y_3} - t_i, x_{y_1} + x_{y_3} - t_i) \in E. \end{cases}$$

Proof: It is not difficult to check that $\mathcal{C}_D$ and $\mathcal{C}_S$ are codes with minimum distance 2, where the minimum distance of a code is the smallest Hamming distance between two distinct codewords. Assume that $\mathcal{C}$ is not a 2-SMIPPC. According to Theorem 5.3.4, there exists $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}$, where $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$, such that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}$ is of the following type:

$$\begin{array}{c} \begin{array}{ccccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 \end{array} \\ \mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C} = \left(\begin{array}{cc|ccc} a_1 & a_2 & a_1 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 & b_1 \\ e_1 & e_2 & e_2 & e_1 & e_1 \end{array} \right) \end{array}$$

For convenience, suppose that $\mathbf{c}_3 = (a_1, b_1, e_2)^T$, $\mathbf{c}_4 = (a_1, b_2, e_1)^T$, $\mathbf{c}_5 = (a_2, b_1, e_1)^T$.

(1) If $\mathbf{c}_1 \in \mathcal{C}_D$, then $\mathbf{c}_1 = (k, k + y, k + x_y)^T$, where $k, y \in Z_q$, and

$$\mathbf{c}_3 = (k, k + y, e_2)^T, \quad \mathbf{c}_4 = (k, b_2, k + x_y)^T, \quad \mathbf{c}_5 = (a_2, k + y, k + x_y)^T.$$

It is easy to see that $a_2 \neq k$. Since $\mathcal{C}_D$ has minimum distance 2, we have $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathcal{C}_S$. Then there exist $1 \leq i_1, i_2, i_3 \leq w$ such that

$$\mathbf{c}_3 = (k, k + s_{i_1}, k + t_{i_1})^T, \quad \mathbf{c}_4 = (k, k + s_{i_2}, k + t_{i_2})^T, \quad \mathbf{c}_5 = (a_2, a_2 + s_{i_3}, a_2 + t_{i_3})^T.$$

Since $\mathcal{C}_S$ has minimum distance 2 and $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathcal{C}_S$, we have

$$\begin{cases} s_{i_1} \neq s_{i_2}, \\ t_{i_1} \neq t_{i_2}, \\ k + t_{i_1} \neq a_2 + t_{i_3} \text{ (note that } k + s_{i_1} = k + y = a_2 + s_{i_3}), \\ k + s_{i_2} \neq a_2 + s_{i_3} \text{ (note that } k + t_{i_2} = k + x_y = a_2 + t_{i_3}). \end{cases}$$

Obviously, $i_1 \neq i_2$. We can also derive $i_1 \neq i_3$, otherwise, if $i_1 = i_3$, then $k = a_2$, a contradiction. Similarly, $i_2 \neq i_3$. So i_1, i_2 and i_3 are all distinct, and we have

$$\begin{cases} k + y = k + s_{i_1}, \\ e_2 = k + t_{i_1}, \\ b_2 = k + s_{i_2}, \\ k + x_y = k + t_{i_2}, \\ k + y = a_2 + s_{i_3}, \\ k + x_y = a_2 + t_{i_3}, \end{cases} \Rightarrow \begin{cases} y = s_{i_1}, \\ x_y = t_{i_2}, \\ x_y - y = t_{i_3} - s_{i_3}, \\ a_2 = k + x_y - t_{i_3}, \\ b_2 = k + s_{i_2}, \\ e_2 = k + t_{i_1}. \end{cases}$$

Then $\mathbf{c}_2 = (a_2, b_2, e_2)^T = (k + x_y - t_{i_3}, k + s_{i_2}, k + t_{i_1})^T$.

(1.1) If $\mathbf{c}_2 \in \mathcal{C}_D$, then there exists $z \in Z_q$ such that $\mathbf{c}_2 = (k + x_y - t_{i_3}, k + x_y - t_{i_3} + z, k + x_y - t_{i_3} + x_z)^T$. So we have

$$\begin{cases} k + s_{i_2} = k + x_y - t_{i_3} + z, \\ k + t_{i_1} = k + x_y - t_{i_3} + x_z, \end{cases} \Rightarrow \begin{cases} z = s_{i_2} + t_{i_3} - x_y, \\ x_z = t_{i_1} + t_{i_3} - x_y, \end{cases}$$

a contradiction to condition (I). So this case is impossible.

(1.2) If $\mathbf{c}_2 \in \mathcal{C}_S$, then there exists $1 \leq i_4 \leq w$ such that $\mathbf{c}_2 = (k + x_y - t_{i_3}, k + x_y - t_{i_3} + s_{i_4}, k + x_y - t_{i_3} + t_{i_4})^T$. So we have

$$\begin{cases} k + s_{i_2} = k + x_y - t_{i_3} + s_{i_4}, \\ k + t_{i_1} = k + x_y - t_{i_3} + t_{i_4}, \end{cases} \Rightarrow \begin{cases} s_{i_4} = s_{i_2} + t_{i_3} - x_y, \\ t_{i_4} = t_{i_1} + t_{i_3} - x_y, \end{cases}$$

a contradiction to condition (I). So this case is impossible.

(2) If $\mathbf{c}_1 \in \mathcal{C}_S$, then $\mathbf{c}_1 = (k, k + s_i, k + t_i)^T$, where $1 \leq i \leq w$, and

$$\mathbf{c}_3 = (k, k + s_i, e_2)^T, \quad \mathbf{c}_4 = (k, b_2, k + t_i)^T, \quad \mathbf{c}_5 = (a_2, k + s_i, k + t_i)^T.$$

It is easy to see that $a_2 \neq k$. Since $\mathcal{C}_S$ has minimum distance 2, we have $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathcal{C}_D$. Then there exist $y_1, y_2, y_3 \in Z_q$ such that

$$\mathbf{c}_3 = (k, k + y_1, k + x_{y_1})^T, \quad \mathbf{c}_4 = (k, k + y_2, k + x_{y_2})^T, \quad \mathbf{c}_5 = (a_2, a_2 + y_3, a_2 + x_{y_3})^T.$$

Since $\mathcal{C}_D$ has minimum distance 2 and $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathcal{C}_D$, we have

$$\begin{cases} y_1 \neq y_2, \\ x_{y_1} \neq x_{y_2}, \\ k + x_{y_1} \neq a_2 + x_{y_3} \text{ (note that } k + y_1 = k + s_i = a_2 + y_3), \\ k + y_2 \neq a_2 + y_3 \text{ (note that } k + x_{y_2} = k + t_i = a_2 + x_{y_3}). \end{cases}$$

If $y_1 = y_3$, then $k = a_2$, a contradiction. So, $y_1 \neq y_3$. Similarly, $y_2 \neq y_3$. So y_1, y_2 and y_3 are all distinct, and we have

$$\begin{cases} k + s_i = k + y_1, \\ e_2 = k + x_{y_1}, \\ b_2 = k + y_2, \\ k + t_i = k + x_{y_2}, \\ k + s_i = a_2 + y_3, \\ k + t_i = a_2 + x_{y_3}, \end{cases} \Rightarrow \begin{cases} s_i = y_1, \\ t_i = x_{y_2}, \\ t_i - s_i = x_{y_3} - y_3, \\ a_2 = k + t_i - x_{y_3}, \\ b_2 = k + y_2, \\ e_2 = k + x_{y_1}. \end{cases}$$

Then $\mathbf{c}_2 = (a_2, b_2, e_2)^T = (k + t_i - x_{y_3}, k + y_2, k + x_{y_1})^T$.

(2.1) If $\mathbf{c}_2 \in \mathcal{C}_D$, then there exists $y_4 \in Z_q$, such that $\mathbf{c}_2 = (k + t_i - x_{y_3}, k + t_i - x_{y_3} + y_4, k + t_i - x_{y_3} + x_{y_4})^T$. So we can have

$$\begin{cases} k + y_2 = k + t_i - x_{y_3} + y_4, \\ k + x_{y_1} = k + t_i - x_{y_3} + x_{y_4}, \end{cases} \Rightarrow \begin{cases} y_4 = y_2 + x_{y_3} - t_i, \\ x_{y_4} = x_{y_1} + x_{y_3} - t_i, \end{cases}$$

a contradiction to condition (II). So this case is impossible.

(2.2) If $\mathbf{c}_2 \in \mathcal{C}_S$, then there exists $1 \leq j \leq w$, such that $\mathbf{c}_2 = (k + t_i - x_{y_3}, k + t_i - x_{y_3} + s_j, k + t_i - x_{y_3} + t_j)^T$. So we can have

$$\begin{cases} k + y_2 = k + t_i - x_{y_3} + s_j, \\ k + x_{y_1} = k + t_i - x_{y_3} + t_j, \end{cases} \Rightarrow \begin{cases} s_j = y_2 + x_{y_3} - t_i, \\ t_j = x_{y_1} + x_{y_3} - t_i, \end{cases}$$

a contradiction to condition (II). So this case is impossible.

Therefore, $\mathcal{C}$ is a 2-SMIPPC$(3, q(q + w), q)$. □

5.3.2 The case $q \equiv 1, 5 \pmod 6$

We now consider the case $q \equiv 1, 5 \pmod 6$. To simplify our discussion, let $x_i = 2i$, $0 \leq i \leq q - 1$, $s_{j_1} \neq s_{j_2}$, $1 \leq j_1 \neq j_2 \leq w$, $t_j = 3s_j$, $1 \leq j \leq w$, in D in the form (5.1) and S in the form (5.2), respectively. Then we have two new matrices:

$$D_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & q-1 \\ 0 & 2 & \cdots & 2(q-1) \end{pmatrix}, \tag{5.4}$$

$$S_1 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ s_1 & s_2 & \cdots & s_w \\ 3s_1 & 3s_2 & \cdots & 3s_w \end{pmatrix}. \tag{5.5}$$

Let

$$\mathcal{C}_{D_1} = \{\mathbf{c} + g \mid \mathbf{c} \in D_1, g \in Z_q\}, \mathcal{C}_{S_1} = \{\mathbf{c} + g \mid \mathbf{c} \in S_1, g \in Z_q\}, \mathcal{C}_1 = \mathcal{C}_{D_1} \bigcup \mathcal{C}_{S_1}. \tag{5.6}$$

It is easy to check that D_1 is a $(q, 3, 1)$-CDM. Let $A_1 = \{s_1, s_2, \ldots, s_w\}$, $A_2 = \{2b \mid b \in A_1\}$, and $A_3 = \{-3b \mid b \in A_1\}$. Then for any $(a', b', e')^T \in \mathcal{C}_{S_1}$, we can have $b' - a' \in A_1$, $e' - b' \in A_2$, and $a' - e' \in A_3$.

Theorem 5.3.8 *Suppose $q \equiv 1, 5 \pmod 6$. Then $\mathcal{C}_1$ in the form (5.6) is a $\overline{2}$-SC$(3, q(q + w), q)$ on Z_q provided that the following hold:*
(I) *$s_i \neq 0$ for any positive integer $1 \leq i \leq w$.*
(II) *$s_i + s_j \neq 0$ always holds for any positive integers $1 \leq i < j \leq w$.*

Proof: We apply Theorem 5.3.6. It is not difficult to check that $|\{s_1, s_2, \ldots, s_w\}| = |\{3s_1, 3s_2, \ldots, 3s_w\}| = |\{2s_1, 2s_2, \ldots, 2s_w\}| = w$ from the fact $q \equiv 1, 5 \pmod 6$ and $s_{j_1} \neq s_{j_2}$, $1 \leq j_1 \neq j_2 \leq w$. For any two columns $(0, s_i, 3s_i)^T$ and $(0, s_j, 3s_j)^T$ in S_1, $1 \leq i \neq j \leq w$, suppose $(0, y, 2y)^T$, $(0, z, 2z)^T$, $(0, y_i, 2y_i)^T$, $(0, y_j, 2y_j)^T$, $(0, z_i, 2z_i)^T$, $(0, z_j, 2z_j)^T \in D_1$, where $y, z, y_i, y_j, z_i, z_j \in Z_q$, such that

$$\begin{cases} 2s_i = y, \\ 2s_j = z, \\ 3s_i = 2y_i, \\ 3s_j = 2y_j, \\ s_i = z_i, \\ s_j = z_j. \end{cases}$$

Then

$$\begin{aligned}
&3s_i - 2y = 3s_i - 4s_i = -s_i \neq 0, \\
&3s_j - 2z = 3s_j - 4s_j = -s_j \neq 0, \\
&(3s_i - 2y) \pm (3s_j - 2z) = -(s_i \pm s_j) \neq 0, \\
&s_i - y_i = s_i - \tfrac{3}{2}s_i = -\tfrac{1}{2}s_i \neq 0, \\
&s_j - y_j = s_j - \tfrac{3}{2}s_j = -\tfrac{1}{2}s_j \neq 0, \\
&(s_i - y_i) \pm (s_j - y_j) = -\tfrac{1}{2}(s_i \pm s_j) \neq 0, \\
&3s_i - 2z_i = 3s_i - 2s_i = s_i \neq 0, \\
&3s_j - 2z_j = 3s_j - 2s_j = s_j \neq 0, \\
&(3s_i - 2z_i) \pm (3s_j - 2z_j) = s_i \pm s_j \neq 0.
\end{aligned}$$

Then the conclusion comes from Theorem 5.3.6. □

Theorem 5.3.9 *Suppose that $q \equiv 1, 5 \pmod 6$. Then $\mathcal{C}_1$ in the form (5.6) is a 2-SMIPPC$(3, q(q + w), q)$ on Z_q provided that the following hold:*
(I) $s_i \neq 0$ for any positive integer $1 \leq i \leq w$.
(II) $s_i + s_j \neq 0$ always holds for any positive integers $1 \leq i < j \leq w$.
(III) There does not exist an element $b \in Z_q$ such that $b, \frac{2b}{3}, \frac{b}{2} \in A_1 = \{s_1, s_2, \ldots, s_w\}$ and $13b = 0$.

Proof: According to Theorem 5.3.8, we know that $\mathcal{C}_1$ is a $\overline{2}$-SC. Assume that $\mathcal{C}$ is not a 2-SMIPPC, then one of conditions (I) and (II) of Theorem 5.3.7 does not hold.

(1) Assume that condition (I) of Theorem 5.3.7 does not hold. Then there exist distinct $1 \leq i_1, i_2, i_3 \leq w$ and $y \in Z_q$ such that

$$\begin{cases} y = s_{i_1}, \\ 2y = 3s_{i_2}, \\ y = 2s_{i_3}, \\ (s_{i_2} + 3s_{i_3} - 2y, 3s_{i_1} + 3s_{i_3} - 2y) \in E, \end{cases} \Rightarrow \begin{cases} y = s_{i_1}, \\ \frac{2}{3}y = s_{i_2}, \\ \frac{1}{2}y = s_{i_3}, \\ (\frac{1}{6}y, \frac{5}{2}y) \in E, \end{cases}$$

where $E = \{(y', 2y') \mid y' \in Z_q\} \bigcup \{(s', 3s') \mid s' \in A_1\}$. This means that $y, \frac{2y}{3}, \frac{y}{2} \in A_1$, and $(\frac{1}{6}y, \frac{5}{2}y) \in E$.

(1.1) If $(\frac{1}{6}y, \frac{5}{2}y) \in \{(y', 2y') \mid y' \in Z_q\}$, then $\frac{2}{6}y = \frac{5}{2}y$, which implies $13y = 0$, a contradiction to condition (III).

(1.2) If $(\frac{1}{6}y, \frac{5}{2}y) \in \{(s', 3s') \mid s' \in A_1\}$, then $\frac{3}{6}y = \frac{5}{2}y$, which implies $y = 0$, a contradiction to $0 \notin A_1$.

(2) Assume that condition (II) of Theorem 5.3.7 does not hold. Then there exist distinct $y_1, y_2, y_3 \in Z_q$ and $1 \le i \le w$ such that

$$\begin{cases} s_i = y_1, \\ 3s_i = 2y_2, \\ 2s_i = y_3, \\ (y_2 + 2y_3 - 3s_i, 2y_1 + 2y_3 - 3s_i) \in E, \end{cases} \Rightarrow \begin{cases} y_1 = s_i, \\ \frac{2}{3}y_2 = s_i, \\ \frac{1}{2}y_3 = s_i, \\ (\frac{5}{2}s_i, 3s_i) \in E. \end{cases}$$

(2.1) If $(\frac{5}{2}s_i, 3s_i) \in \{(y', 2y') \mid y' \in Z_q\}$, then $5s_i = 3s_i$, which implies $s_i = 0$, a contradiction to condition (I).

(2.2) If $(\frac{5}{2}s_i, 3s_i) \in \{(s', 3s') \mid s' \in A_1\}$, then $\frac{15}{2}s_i = 3s_i$, which implies $s_i = 0$, a contradiction to condition (I).

The above (1) and (2) show that conditions (I) and (II) of Theorem 5.3.7 always hold, which implies that $\mathcal{C}_1$ is a 2-SMIPPC from Theorem 5.3.7. □

We will use Theorem 5.3.9 to construct optimal 2-SMIPPC$(3, M, q)$s for $q \equiv 1, 5 \pmod 6$.

Lemma 5.3.10 *If $q \equiv 1, 5 \pmod 6$ and $q \not\equiv 0 \pmod{13}$, then there exists a 2-SMIPPC$(3, q^2 + \frac{q(q-1)}{2}, q)$.*

Proof: Let $\mathcal{C}_1$ be in the form (5.6) and $A_1 = \{1, 2, \ldots, \frac{q-1}{2}\}$. The conclusion comes from Theorem 5.3.9. □

Lemma 5.3.11 *If $q \equiv 13, 65 \pmod{78}$, then there exists a 2-SMIPPC$(3, q^2 + \frac{q(q-1)}{2}, q)$.*

Proof: Let $q = 13r$. Suppose that $\mathcal{C}_1$ is in the form (5.6) and $A_1 = \{1, \ldots, 4r - 1, 4r + 1, \ldots, \frac{q-1}{2}, 9r\}$. We want to show that conditions (I), (II), (III) in Theorem 5.3.9 are satisfied. Obviously, conditions (I) and (II) hold. Assume that there exists an element $b \in Z_q$ such that $b, \frac{2b}{3}, \frac{b}{2} \in A_1$ and $13b = 0$. Then b should be a multiple of r and thus we have $b \in \{r, 2r, 3r, 5r, 6r, 9r\}$. Then

b	r	$2r$	$3r$	$5r$	$6r$	$9r$
$\frac{2b}{3}$	$5r$	$10r$	$2r$	$12r$	$4r$	$6r$
$\frac{b}{2}$	$7r$	r	$8r$	$9r$	$3r$	$11r$

Table 5.1

From Table 5.1, we know that for any $b \in \{r, 2r, 3r, 5r, 6r, 9r\}$, one of the elements $\frac{2b}{3}$ and $\frac{b}{2}$ is not contained in A_1, a contradiction to $b, \frac{2b}{3}, \frac{b}{2} \in A_1$. Hence, condition (III) is satisfied.

The conclusion then comes from Theorem 5.3.9. □

Combining Theorem 5.3.3, Lemmas 5.3.10 and 5.3.11, we have

Theorem 5.3.12 *There exists an optimal* 2*-SMIPPC*$(3, q^2 + \frac{q(q-1)}{2}, q)$ *for any* $q \equiv 1, 5 \pmod 6$.

5.3.3 The case $q \equiv 0, 2 \pmod 6$

Next, we deal with the case $q \equiv 0, 2 \pmod 6$. Let $s = q - 1$, then $s \equiv 1, 5 \pmod 6$.

In order to describe our constructions, we introduce a new element $\infty \notin Z_s$, and for any $a \in Z_s$, we define

$$a + \infty = \infty + a = a \cdot \infty = \infty \cdot a = \infty.$$

We now define a code

$$\mathcal{C}_2' = \mathcal{C}_2 \bigcup \mathcal{C}_{T_2} \bigcup \{(\infty, \infty, \infty)^T\} \tag{5.7}$$

on $Q = Z_s \bigcup \{\infty\}$, where $s_1, s_2, \ldots, s_w, m \in Z_s$,

$$D_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & s-1 \\ 0 & 2 & \cdots & 2(s-1) \end{pmatrix}, \qquad S_2 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ s_1 & s_2 & \cdots & s_w \\ 3s_1 & 3s_2 & \cdots & 3s_w \end{pmatrix},$$

$$T_2 = \begin{pmatrix} \infty & m & 0 \\ 0 & \infty & m \\ m & 0 & \infty \end{pmatrix},$$

$\mathcal{C}_{D_2} = \{\mathbf{c} + g \mid \mathbf{c} \in D_2, g \in Z_s\}$, $\mathcal{C}_{S_2} = \{\mathbf{c} + g \mid \mathbf{c} \in S_2, g \in Z_s\}$, $\mathcal{C}_{T_2} = \{\mathbf{c} + g \mid \mathbf{c} \in T_2, g \in Z_s\}$, and $\mathcal{C}_2 = \mathcal{C}_{D_2} \bigcup \mathcal{C}_{S_2}$.

Theorem 5.3.13 $\mathcal{C}_2'$ *in the form* (5.7) *is a* $\overline{2}$*-SC*$(3, s(s+w+3)+1, q)$ *provided that the following hold:*
(I) $s_i \neq 0$ *for any positive integer* $1 \leq i \leq w$.
(II) $s_i + s_j \neq 0$ *always holds for any positive integers* $1 \leq i < j \leq w$.
(III) $m \notin \bigcup_{i=1}^{3} A_i$.

Proof: According to Theorem 5.3.8, we know that $\mathcal{C}_2 = \mathcal{C}_{D_2} \bigcup \mathcal{C}_{S_2}$ is a $\overline{2}$-SC$(3, s(s+w), s)$ defined on Z_s. Hence, in $\mathcal{C}_2$, $|\mathcal{A}_{g_1}^j \bigcap \mathcal{A}_{g_2}^j| \leq 1$ holds for any positive integer

$1 \leq j \leq 3$ and any distinct $g_1, g_2 \in Z_s$ from Lemma 3.3.4. Now we define

$$\mathcal{B}_g^j = \begin{cases} \mathcal{A}_g^j \bigcup \{(\infty, g-m)^T, (g+m, \infty)^T\}, & \text{if } g \in Z_s,\ j = 1,3, \\ \mathcal{A}_g^j \bigcup \{(\infty, g+m)^T, (g-m, \infty)^T\}, & \text{if } g \in Z_s,\ j = 2, \\ \{(i, i+m)^T \mid i \in Z_s\} \bigcup \{(\infty, \infty)^T\}, & \text{if } g = \infty,\ j = 1,3, \\ \{(i+m, i)^T \mid i \in Z_s\} \bigcup \{(\infty, \infty)^T\}, & \text{if } g = \infty,\ j = 2. \end{cases}$$

According to Lemma 3.3.4, in order to prove that $\mathcal{C}_2'$ is a $\overline{2}$-SC, it suffices to show that $|\mathcal{B}_{g_1}^j \bigcap \mathcal{B}_{g_2}^j| \leq 1$ holds for any positive integer $1 \leq j \leq 3$, and any distinct $g_1, g_2 \in Z_s \bigcup \{\infty\}$.

Since for any distinct $g_1, g_2 \in Z_s$, $\{(\infty, g_1 - m)^T, (g_1 + m, \infty)^T\} \bigcap \{(\infty, g_2 - m)^T, (g_2 + m, \infty)^T\} = \emptyset$, and $\{(\infty, g_1 + m)^T, (g_1 - m, \infty)^T\} \bigcap \{(\infty, g_2 + m)^T, (g_2 - m, \infty)^T\} = \emptyset$, we have $\mathcal{B}_{g_1}^j \bigcap \mathcal{B}_{g_2}^j = \mathcal{A}_{g_1}^j \bigcap \mathcal{A}_{g_2}^j$ for any integer $1 \leq j \leq 3$, which implies $|\mathcal{B}_{g_1}^j \bigcap \mathcal{B}_{g_2}^j| \leq 1$.

Next, since $m \notin \bigcup_{i=1}^3 A_i$, we know that for any $g \in Z_s$,

$$\begin{aligned} \mathcal{B}_g^1 \bigcap \mathcal{B}_\infty^1 &= \{(g+m, g+2m)^T\}, \\ \mathcal{B}_g^2 \bigcap \mathcal{B}_\infty^2 &= \{(g+\tfrac{m}{2}, g-\tfrac{m}{2})^T\}, \\ \mathcal{B}_g^3 \bigcap \mathcal{B}_\infty^3 &= \{(g-2m, g-m)^T\}. \end{aligned}$$

Then $|\mathcal{B}_g^j \bigcap \mathcal{B}_\infty^j| = 1$ holds for any integer $1 \leq j \leq 3$.

This completes the proof. □

Theorem 5.3.14 *$\mathcal{C}_2'$ in the form (5.7) is a 2-SMIPPC$(3, s(s+w+3)+1, q)$ provided that the following hold:*
(I) *$s_i \neq 0$ for any positive integer $1 \leq i \leq w$.*
(II) *$s_i + s_j \neq 0$ always holds for any positive integers $1 \leq i < j \leq w$.*
(III) *There does not exist an element $b \in Z_s$ such that $b, \frac{2b}{3}, \frac{b}{2} \in A_1$ and $13b = 0$.*
(IV) *$m \notin \bigcup_{i=1}^3 A_i$, $-\frac{m}{2} \notin A_2$, $-2m \notin A_3$, $m \neq 0$.*

Proof: It is clear that $\mathcal{C}_2'$ is a $\overline{2}$-SC from Theorem 5.3.13. Assume that $\mathcal{C}_2'$ is not a 2-SMIPPC. According to Theorem 5.3.4, there exists $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}_2'$, where $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$, such that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}_2'$ is of the following type:

$$\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}_2' = \begin{array}{c} \begin{array}{ccccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 \end{array} \\ \left(\begin{array}{cc|ccc} a_1 & a_2 & a_1 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 & b_1 \\ e_1 & e_2 & e_2 & e_1 & e_1 \end{array} \right) \end{array}.$$

For convenience, suppose that $\mathbf{c}_3 = (a_1, b_1, e_2)^T$, $\mathbf{c}_4 = (a_1, b_2, e_1)^T$, $\mathbf{c}_5 = (a_2, b_1, e_1)^T$.

(1) If $\mathbf{c}_1 \in \mathcal{C}_{D_2}$, then $\mathbf{c}_1 = (k, k+b, k+2b)^T$, where $k, b \in Z_s$.

(1.1) If $b \notin \{m, -\frac{m}{2}\}$, then $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathcal{C}_2 = \mathcal{C}_{D_2} \bigcup \mathcal{C}_{S_2}$, and also $\mathbf{c}_2 \in \mathcal{C}_2$. According to the proofs of Theorems 5.3.7 and 5.3.9, this case is impossible.

(1.2) If $b = m$, then $\mathbf{c}_4 = (k, b_2, k + 2m)^T$. Since $s \equiv 1, 5 \pmod 6$ and $m \neq 0$, we have $-2m \neq m$, which implies $\mathbf{c}_4 \notin \mathcal{C}_{T_2}$. Since $-2m \notin A_3$, we can derive that $\mathbf{c}_4 \notin \mathcal{C}_{S_2}$. Hence $\mathbf{c}_4 \in \mathcal{C}_{D_2}$, which, together with the fact that $\mathcal{C}_{D_2}$ has minimum distance 2, implies $\mathbf{c}_4 = \mathbf{c}_1$, a contradiction. So this case is impossible.

(1.3) If $b = -\frac{m}{2}$, then $\mathbf{c}_5 = (a_2, k - \frac{m}{2}, k - m)^T$. Since $s \equiv 1, 5 \pmod 6$ and $m \neq 0$, we have $-\frac{m}{2} \neq m$, which implies $\mathbf{c}_5 \notin \mathcal{C}_{T_2}$. Since $-\frac{m}{2} \notin A_2$, we can derive that $\mathbf{c}_5 \notin \mathcal{C}_{S_2}$. Hence $\mathbf{c}_5 \in \mathcal{C}_{D_2}$, which implies $\mathbf{c}_5 = \mathbf{c}_1$, a contradiction. So this case is impossible.

(2) If $\mathbf{c}_1 \in \mathcal{C}_{S_2}$, then $\mathbf{c}_1 = (k, k + b, k + 3b)^T$, where $k \in Z_s, b \in A_1 \subseteq Z_s$. Since $m \notin \bigcup_{i=1}^{3} A_i$, we know that $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \notin \mathcal{C}_{T_2}$, which implies $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathcal{C}_2 = \mathcal{C}_{D_2} \bigcup \mathcal{C}_{S_2}$, and also $\mathbf{c}_2 \in \mathcal{C}_2$. According to the proofs of Theorems 5.3.7 and 5.3.9, this case is impossible.

(3) If $\mathbf{c}_1 \in \mathcal{C}_{T_2}$, without loss of generality, we may assume that $\mathbf{c}_1 = (\infty, b, b + m)^T$. Then $\mathbf{c}_3 = \mathbf{c}_1$, a contradiction. So this case is impossible.

(4) If $\mathbf{c}_1 = (\infty, \infty, \infty)^T$, then $\mathbf{c}_3 = \mathbf{c}_1$, a contradiction. So this case is impossible.

According to (1)-(4), we know that $\mathcal{C}_2'$ is a 2-SMIPPC$(3, s(s + w + 3) + 1, q)$. □

Lemma 5.3.15 *If $q \equiv 0 \pmod 6 \geq 12$ and $q \not\equiv 1 \pmod{13}$, then there exists a 2-SMIPPC$(3, q^2 + \frac{q(q-1)}{2}, q)$.*

Proof: Let $\mathcal{C}_2'$ be in the form (5.7), $A_1 = \{1, 2, \ldots, \frac{s-1}{2}\}$, and $m = -2$. Obviously, conditions (I) and (II) of Theorem 5.3.14 are satisfied. Since $q \not\equiv 1 \pmod{13}$, $s = q - 1 \not\equiv 0 \pmod{13}$. Then, except the element $0 \in Z_s$, there is no element $b \in Z_s$, such that $13b = 0$, but $0 \notin A_1$. This implies that condition (III) of Theorem 5.3.14 is satisfied. Now consider condition (IV) of Theorem 5.3.14. Remember that $A_2 = \{2b \mid b \in A_1\}$, $A_3 = \{-3b \mid b \in A_1\}$.

(1) Obviously, $m \neq 0$, and $-\frac{m}{2} = 1 \notin A_2$.

(2) $-2m = 4 \notin A_3$. Assume not. Then there exists $b \in A_1$, such that $4 = -3b$. Then $b = -\frac{4}{3}$. Since $s = q - 1 \equiv 5 \pmod 6$, we write $s = 6h + 5$ for some integer $h \geq 1$. Then $b = 4h + 2$ and $A_1 = \{1, 2, \ldots, 3h + 2\}$, which implies $b \notin A_1$, a contradiction.

(3) Obviously, $m = -2 \notin A_1 \bigcup A_2$. It suffices to show that $m = -2 \notin A_3$. Assume not. Then there exists $b \in A_1$, such that $-2 = -3b$. Then $b = \frac{2}{3} = 4h + 4$, which implies $b \notin A_1$, a contradiction.

The conclusion then comes from Theorem 5.3.14. □

Lemma 5.3.16 *If $q \equiv 66 \pmod{78}$, then there exists a 2-SMIPPC$(3, q^2 + \frac{q(q-1)}{2}, q)$.*

Proof: Let $s = q - 1 = 13r$, $\mathcal{C}_2'$ be in the form (5.7), $A_1 = \{1, \ldots, 4r - 1, 4r + 1, \ldots, \frac{s-1}{2}, 9r\}$, and $m = -2$. Obviously, conditions (I) and (II) of Theorem 5.3.14

are satisfied. Since $q \equiv 66 \pmod{78}$, $s = q-1 \equiv 65 \pmod{78}$, then we can know condition (III) of Theorem 5.3.14 is satisfied from the proof of Lemma 5.3.11. Now consider condition (IV) of Theorem 5.3.14. Remember that $A_2 = \{2b \mid b \in A_1\}$, $A_3 = \{-3b \mid b \in A_1\}$.

(1) Obviously, $m \neq 0$, and $-\frac{m}{2} = 1 \notin A_2$.

(2) $-2m = 4 \notin A_3$. Assume not. Then there exists $b \in A_1$, such that $4 = -3b$. Write $s = 78h+65$. Then $r = 6h+5$ and $b = -\frac{4}{3} = 52h+42$. Since $\frac{s-1}{2} = 39h+32$, it should hold that $b = 9r$, that is, $2h+3 = 0$, which is impossible.

(3) Since $s \geq 65$, we have $r \geq 5$. Then $s-2 = 13r-2 > 9r$, which implies $m = -2 \notin A_1$. Also, $s-2 = 13r-2 \neq 5r$, which implies $m = -2 \notin A_2$. It suffices to show that $m = -2 \notin A_3$. Assume not. Then there exists $b \in A_1$, such that $-2 = -3b$. Then $b = \frac{2}{3} = 52h+44$. Since $\frac{s-1}{2} = 39h+32$, it should hold that $b = 9r$, that is, $2h+1 = 0$, which is impossible.

The conclusion then comes from Theorem 5.3.14. □

Lemma 5.3.17 *If $q \equiv 2 \pmod 6 \geq 44$ and $q \not\equiv 1 \pmod{13}$, then there exists a 2-SMIPPC$(3, q^2 + \frac{q(q-1)}{2}, q)$.*

Proof: Let $\mathcal{C}_2'$ be in the form (5.7), $A_1 = \{1, 2, \ldots, \frac{s-1}{2}\}$, and $m = -10$. Obviously, conditions (I) and (II) of Theorem 5.3.14 are satisfied. Since $q \not\equiv 1 \pmod{13}$, $s = q-1 \not\equiv 0 \pmod{13}$. Then, except the element $0 \in Z_s$, there is no element $b \in Z_s$, such that $13b = 0$, but $0 \notin A_1$. This implies that condition (III) of Theorem 5.3.14 is satisfied. Now consider condition (IV) of Theorem 5.3.14. Remember that $A_2 = \{2b \mid b \in A_1\}$, $A_3 = \{-3b \mid b \in A_1\}$.

(1) Obviously, $m \neq 0$, and $-\frac{m}{2} = 5 \notin A_2$.

(2) $-2m = 20 \notin A_3$. Assume not. Then there exists $b \in A_1$, such that $20 = -3b$. Then $b = -\frac{20}{3}$. Write $s = 6h+1$ for some integer $h \geq 7$. Then $b = 4h-6$ and $A_1 = \{1, 2, \ldots, 3h\}$, which implies $b \notin A_1$, a contradiction.

(3) Since $s \geq 43$, we have $s - 10 = 6h - 9$, and $\frac{s-1}{2} = 3h$, which implies $m = -10 \notin A_1$. It is also clear that $m = -10 \notin A_2$. We show that $m = -10 \notin A_3$. Assume not. Then there exists $b \in A_1$, such that $-10 = -3b$. Then $b = \frac{10}{3} = 4h+4$, which implies $b \notin A_1$, a contradiction.

So, the conclusion comes from Theorem 5.3.14. □

Lemma 5.3.18 *If $q \equiv 14 \pmod{78} \geq 92$, then there exists a 2-SMIPPC$(3, q^2 + \frac{q(q-1)}{2}, q)$.*

Proof: Let $s = q-1 = 13r$, $\mathcal{C}_2'$ be in the form (5.7), $A_1 = \{1, \ldots, 4r-1, 4r+1, \ldots, \frac{s-1}{2}, 9r\}$, and $m = -10$. Obviously, conditions (I) and (II) of Theorem 5.3.14 are satisfied. Since $q \equiv 14 \pmod{78}$, $s = q-1 \equiv 13 \pmod{78}$, then we can know that condition (III) of Theorem 5.3.14 is satisfied from the proof of Lemma 5.3.11. Now we consider condition (IV) of Theorem 5.3.14.

(1) Obviously, $m \neq 0$, and $-\frac{m}{2} = 5 \notin A_2$.

(2) $-2m = 20 \notin A_3$. Assume not. Then there exists $b \in A_1$, such that $20 = -3b$. Write $s = 78h + 13$. Then $r = 6h + 1$, and $b = -\frac{20}{3} = 52h + 2$. Since $\frac{s-1}{2} = 39h + 6$, it should hold that $b = 9r$, that is, $2h + 7 = 0$, which is impossible.

(3) Since $s \geq 91$, we can have $r \geq 7$. Then $s - 10 = 13r - 10 > 9r$, which implies $m = -10 \notin A_1$.

$m = -10 \notin A_2$. Assume not. Then there exists $b \in A_1$, such that $-10 = 2b$, which implies $b = -5 = s - 5$. Since $s \geq 91$, we have $s - 5 > \frac{s-1}{2}$, which implies $b = 9r$, that is, $-10 = 2 \cdot 9r = 18r = 5r$. Hence $r = -2 = s - 2 \equiv 5 \pmod 6$, a contradiction.

It suffices to show that $m = -10 \notin A_3$. Assume not. Then there exists $b \in A_1$, such that $-10 = -3b$. Then $b = \frac{10}{3} = 52h + 12$. Since $\frac{s-1}{2} = 39h + 6$, it should hold that $b = 9r$, then $-10 = -3 \cdot 9r = -r$, $r \equiv 10 \pmod s \equiv 10 \pmod{13r}$, and $r = 10 \not\equiv 1 \pmod 6$, a contradiction.

So the conclusion comes from Theorem 5.3.14. □

Lemma 5.3.19 *There exists a 2-SMIPPC*$(3, q^2 + \frac{q(q-1)}{2}, q)$ *for any* $q \in \{20, 26, 32, 38\}$.

Proof: Let
$A^{(20)} = \{1, 2, 3, 4, 5, 7, 8, 10, 13\}$, $m^{(20)} = 9$,
$A^{(26)} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13\}$, $m^{(26)} = 24$,
$A^{(32)} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 17\}$, $m^{(32)} = 21$,
$A^{(38)} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 19\}$, $m^{(38)} = 27$.

For any $q \in \{20, 26, 32, 38\}$, let $s = q - 1$, $\mathcal{C}^{(q)}$ be in the form (5.7), $A_1 = A^{(q)}$, and $m = m^{(q)}$. Then the conclusion comes from Theorem 5.3.14. □

The following result comes from Lemmas 5.3.15-5.3.19 and Theorem 5.3.3.

Theorem 5.3.20 *Suppose that* $q \equiv 0, 2 \pmod 6$*, and* $q \notin \{2, 6, 8, 14\}$*, then there exists an optimal* 2-*SMIPPC*$(3, q^2 + \frac{q(q-1)}{2}, q)$.

For each $q \in \{6, 8\}$, we want to find the set A_1 and the element m satisfying the conditions (I)-(IV) of Theorem 5.3.14. Unfortunately, we fail to do this. However, we can construct a 2-SMIPPC$(3, q^2 + \frac{q(q-1)}{2}, q)$ for each $q \in \{6, 8\}$ by making a detailed analysis of the proof of Theorem 5.3.14.

Lemma 5.3.21 *There exists a 2-SMIPPC*$(3, 51, 6)$.

Proof: Let $s = 5$, $\mathcal{C}_2^{'}$ be in the form (5.7), $A_1 = \{1, 2\}$, and $m = 3$. Then $A_2 = A_3 = \{2, 4\}$. It is not difficult to check that $m \neq 0$, $-\frac{m}{2} = 1 \notin A_2$, $m \notin \bigcup_{i=1}^{3} A_i$, and conditions (I), (II), (III) of Theorem 5.3.14 are satisfied. According to the proof of Theorem 5.3.14, it suffices to prove the following assertion:

There does not exist $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(k, k+3, k+1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}_2^{'}$, where $k \in Z_5$, $a_2, b_2, e_2 \in Z_5 \bigcup \{\infty\}$, $a_2 \neq k$, $b_2 \neq k+3$, and $e_2 \neq k+1$, such that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}_2^{'}$ is of the following type:

$$\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}_2^{'} = \begin{array}{c} \\ \\ \end{array}\left(\begin{array}{cc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 \\ k & a_2 & k & k & a_2 \\ k+3 & b_2 & k+3 & b_2 & k+3 \\ k+1 & e_2 & e_2 & k+1 & k+1 \end{array}\right),$$

where $\mathbf{c}_3 = (k, k+3, e_2)^T$, $\mathbf{c}_4 = (k, b_2, k+1)^T$, $\mathbf{c}_5 = (a_2, k+3, k+1)^T$.

Assume not. Obviously, $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \notin \mathcal{C}_{D_2}$, because of the fact that $\mathcal{C}_{D_2}$ has minimum distance 2 and $\mathbf{c}_1 \in \mathcal{C}_{D_2}$. It is not difficult to see that $\mathbf{c}_3, \mathbf{c}_5 \notin \mathcal{C}_{S_2}$ since $3 \notin A_1 \bigcup A_2$, which implies $\mathbf{c}_3, \mathbf{c}_5 \in \mathcal{C}_{T_2}$. Hence $\mathbf{c}_3 = (k, k+3, \infty)^T$, $\mathbf{c}_5 = (\infty, k+3, k+1)^T$, and $\mathbf{c}_2 = (\infty, \infty, \infty)^T$, which implies $\mathbf{c}_4 = (k, \infty, k+1)^T$. Clearly, since $m = 3 \neq -1$, we know that $\mathbf{c}_4 = (k, \infty, k+1)^T \notin \mathcal{C}_2^{'}$, a contradiction.

So, $\mathcal{C}_2^{'}$ is a 2-SMIPPC$(3, 51, 6)$. □

Lemma 5.3.22 *There exists a 2-SMIPPC*$(3, 92, 8)$.

Proof: Let $s = 7$, $\mathcal{C}_2^{'}$ be in the form (5.7), $A_1 = \{1, 2, 4\}$, and $m = 3$. Then $A_2 = A_3 = \{1, 2, 4\}$. It is not difficult to check that $m \neq 0$, $m \notin \bigcup_{i=1}^{3} A_i$ and conditions (I), (II), (III) of Theorem 5.3.14 are satisfied. According to the proof of Theorem 5.3.14, it suffices to prove the following assertion:

There does not exist $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(k, k+b, k+2b)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}_2^{'}$, where $k \in Z_7$, $b \in \{2, 3\}$, $a_2, b_2, e_2 \in Z_7 \bigcup \{\infty\}$, $a_2 \neq k$, $b_2 \neq k+b$, and $e_2 \neq k+2b$, such that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}_2^{'}$ is of the following type:

$$\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}_2^{'} = \left(\begin{array}{cc|ccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 \\ k & a_2 & k & k & a_2 \\ k+b & b_2 & k+b & b_2 & k+b \\ k+2b & e_2 & e_2 & k+2b & k+2b \end{array}\right),$$

where $\mathbf{c}_3 = (k, k+b, e_2)^T$, $\mathbf{c}_4 = (k, b_2, k+2b)^T$, $\mathbf{c}_5 = (a_2, k+b, k+2b)^T$.

Assume not. Since $\mathcal{C}_{D_2}$ has minimum distance 2 and $\mathbf{c}_1 \in \mathcal{C}_{D_2}$, we know that $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \notin \mathcal{C}_{D_2}$.

(1) The case $b = 2$. We can directly check that $\mathbf{c}_3, \mathbf{c}_5 \notin \mathcal{C}_{T_2}$ and $\mathbf{c}_4 \notin \mathcal{C}_{S_2}$, which implies $\mathbf{c}_3, \mathbf{c}_5 \in \mathcal{C}_{S_2}$ and $\mathbf{c}_4 \in \mathcal{C}_{T_2}$. Hence $\mathbf{c}_3 = (k, k+2, k+6)^T$, $\mathbf{c}_5 = (k+1, k+2, k+4)^T$ and $\mathbf{c}_4 = (k, \infty, k+4)^T$, which implies $\mathbf{c}_2 = (k+1, \infty, k+6)^T$. Obviously, since $m = 3 \neq -5$, we know that $\mathbf{c}_2 = (k+1, \infty, k+6)^T \notin \mathcal{C}_2^{'}$, a contradiction.

(2) The case $b = 3$. It is not difficult to see that $\mathbf{c}_3, \mathbf{c}_5 \notin \mathcal{C}_{S_2}$, which implies $\mathbf{c}_3, \mathbf{c}_5 \in \mathcal{C}_{T_2}$. Hence $\mathbf{c}_3 = (k, k+3, \infty)^T$, $\mathbf{c}_5 = (\infty, k+3, k+6)^T$, and $\mathbf{c}_2 =$

$(\infty,\infty,\infty)^T$, which implies $\mathbf{c}_4 = (k,\infty,k+6)^T$. Obviously, since $m = 3 \neq 1$, we know that $\mathbf{c}_4 = (k,\infty,k+6)^T \notin \mathcal{C}_2^{'}$, a contradiction.

So, $\mathcal{C}_2^{'}$ is a 2-SMIPPC$(3, 92, 8)$. □

Lemma 5.3.23 *There exists a 2-SMIPPC*$(3, 287, 14)$.

Proof: We construct a (3, 287, 14) code $\mathcal{C}_3^{'}$ on $Z_{13}\bigcup\{\infty\}$ as follows. Let

$$D_3 = \begin{pmatrix} 0 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 12 \\ 0 & 2 & \cdots & 2\times 12 \end{pmatrix}, \quad S_3 = \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 2 & 3 & 5 & 6 & 9 \\ 3 & 6 & 9 & 2 & 5 & 1 \end{pmatrix},$$

$$T_3 = \begin{pmatrix} \infty & 6 & 0 \\ 0 & \infty & 4 \\ 7 & 0 & \infty \end{pmatrix},$$

$\mathcal{C}_{D_3} = \{\mathbf{c}+g \mid \mathbf{c} \in D_3, g \in Z_{13}\}$, $\mathcal{C}_{S_3} = \{\mathbf{c}+g \mid \mathbf{c} \in S_3, g \in Z_{13}\}$, $\mathcal{C}_{T_3} = \{\mathbf{c}+g \mid \mathbf{c} \in T_3, g \in Z_{13}\}$, $\mathcal{C}_3 = \mathcal{C}_{D_3}\bigcup\mathcal{C}_{S_3}$, $\mathcal{C}_3^{'} = \mathcal{C}_3\bigcup\mathcal{C}_{T_3}\bigcup\{(\infty,\infty,\infty)^T\}$. Let $A_1 = \{1,2,3,5,6,9\}$, $A_2 = \{2b \mid b \in A_1\}$, and $A_3 = \{-3b \mid b \in A_1\}$.

According to the proof of Lemma 5.3.11, we know that $\mathcal{C}_3$ is a 2-SMIPPC defined on Z_{13}. We first prove that $\mathcal{C}_3^{'}$ is a $\overline{2}$-SC defined on $Z_{13}\bigcup\{\infty\}$.

According to Theorem 5.3.8, we know that $\mathcal{C}_3 = \mathcal{C}_{D_3}\bigcup\mathcal{C}_{S_3}$ is a $\overline{2}$-SC$(3, 247, 13)$ defined on Z_{13}. Hence, $|\mathcal{A}_{g_1}^j\bigcap\mathcal{A}_{g_2}^j| \leq 1$ holds for any positive integers $1 \leq j \leq 3$ and any distinct $g_1, g_2 \in Z_{13}$ from Lemma 3.3.4. Now we define

$$\mathcal{B}_g^j = \begin{cases} \mathcal{A}_g^j\bigcup\{(\infty,g-6)^T,(g+4,\infty)^T\}, & if \ \ g \in Z_{13},\ j=1, \\ \mathcal{A}_g^j\bigcup\{(\infty,g+7)^T,(g-4,\infty)^T\}, & if \ \ g \in Z_{13},\ j=2, \\ \mathcal{A}_g^j\bigcup\{(\infty,g-7)^T,(g+6,\infty)^T\}, & if \ \ g \in Z_{13},\ j=3, \\ \{(i,i+7)^T \mid i \in Z_{13}\}\bigcup\{(\infty,\infty)^T\}, & if \ \ g=\infty,\ j=1, \\ \{(i+6,i)^T \mid i \in Z_{13}\}\bigcup\{(\infty,\infty)^T\}, & if \ \ g=\infty,\ j=2, \\ \{(i,i+4)^T \mid i \in Z_{13}\}\bigcup\{(\infty,\infty)^T\}, & if \ \ g=\infty,\ j=3. \end{cases}$$

According to Lemma 3.3.4, in order to prove that $\mathcal{C}_3^{'}$ is a $\overline{2}$-SC, it suffices to show that $|\mathcal{B}_{g_1}^j\bigcap\mathcal{B}_{g_2}^j| \leq 1$ holds for any positive integer $1 \leq j \leq 3$, and any distinct $g_1, g_2 \in Z_{13}\bigcup\{\infty\}$.

For any distinct $g_1, g_2 \in Z_{13}$, we have

$$\begin{aligned} &\{(\infty,g_1-6)^T,(g_1+4,\infty)^T\}\bigcap\{(\infty,g_2-6)^T,(g_2+4,\infty)^T\} = \emptyset, \\ &\{(\infty,g_1+7)^T,(g_1-4,\infty)^T\}\bigcap\{(\infty,g_2+7)^T,(g_2-4,\infty)^T\} = \emptyset, \\ &\{(\infty,g_1-7)^T,(g_1+6,\infty)^T\}\bigcap\{(\infty,g_2-7)^T,(g_2+6,\infty)^T\} = \emptyset. \end{aligned}$$

Then $\mathcal{B}_{g_1}^j\bigcap\mathcal{B}_{g_2}^j = \mathcal{A}_{g_1}^j\bigcap\mathcal{A}_{g_2}^j$ for any integer $1 \leq j \leq 3$, which implies $|\mathcal{B}_{g_1}^j\bigcap\mathcal{B}_{g_2}^j| \leq 1$. For any $g \in Z_{13}$, we can also have

$$\begin{aligned}\mathcal{B}_g^1 \bigcap \mathcal{B}_\infty^1 &= \{(g+7, g+1)^T\},\\ \mathcal{B}_g^2 \bigcap \mathcal{B}_\infty^2 &= \{(g+3, g-3)^T\},\\ \mathcal{B}_g^3 \bigcap \mathcal{B}_\infty^3 &= \{(g-8, g-4)^T\}.\end{aligned}$$

Then $|\mathcal{B}_g^j \bigcap \mathcal{B}_\infty^j| = 1$ for any integer $1 \le j \le 3$. This implies $\mathcal{C}_3'$ is a $\overline{2}$-SC.

Now assume that $\mathcal{C}_3'$ is not a 2-SMIPPC. According to Theorem 5.3.4, there exists $\mathcal{C}_0 = \{\mathbf{c}_1, \mathbf{c}_2\} = \{(a_1, b_1, e_1)^T, (a_2, b_2, e_2)^T\} \subseteq \mathcal{C}_3'$, where $a_1 \neq a_2$, $b_1 \neq b_2$, and $e_1 \neq e_2$, such that $\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}_3'$ is of the following type:

$$\mathsf{desc}(\mathcal{C}_0) \bigcap \mathcal{C}_3' = \begin{array}{c} \begin{array}{ccccc} \mathbf{c}_1 & \mathbf{c}_2 & \mathbf{c}_3 & \mathbf{c}_4 & \mathbf{c}_5 \end{array} \\ \left(\begin{array}{cc|ccc} a_1 & a_2 & a_1 & a_1 & a_2 \\ b_1 & b_2 & b_1 & b_2 & b_1 \\ e_1 & e_2 & e_2 & e_1 & e_1 \end{array}\right) \end{array},$$

where $\mathbf{c}_3 = (a_1, b_1, e_2)^T$, $\mathbf{c}_4 = (a_1, b_2, e_1)^T$, $\mathbf{c}_5 = (a_2, b_1, e_1)^T$.

(1) If $\mathbf{c}_1 \in \mathcal{C}_{D_3}$, then $\mathbf{c}_1 = (k, k+b, k+2b)^T$, where $k, b \in Z_{13}$. Since $\mathcal{C}_{D_3}$ has minimum distance 2, we have $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \notin \mathcal{C}_{D_3}$.

(1.1) If $b \notin \{4, 7, 10\}$, then $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathcal{C}_3$, and also $\mathbf{c}_2 \in \mathcal{C}_3$, which contradict to the fact that $\mathcal{C}_3$ is a 2-SMIPPC. So this case is impossible.

(1.2) If $b = 4$, noting that $-2b = 5 \notin A_3 \bigcup \{6\}$, we have $\mathbf{c}_4 \notin \mathcal{C}_{S_3} \bigcup \mathcal{C}_{T_3}$, which implies $\mathbf{c}_4 \notin \mathcal{C}_3'$, a contradiction. So this case is impossible.

(1.3) If $b = 7$ or 10, noting that $b \notin A_1 \bigcup \{4\}$, we have $\mathbf{c}_3 \notin \mathcal{C}_{S_3} \bigcup \mathcal{C}_{T_3}$, which implies $\mathbf{c}_3 \notin \mathcal{C}_3'$, a contradiction. So this case is impossible.

(2) If $\mathbf{c}_1 \in \mathcal{C}_{S_3}$, then $\mathbf{c}_1 = (k, k+b, k+3b)^T$, where $k \in Z_{13}, b \in \{1, 2, 3, 5, 6, 9\}$. We can check that $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \notin \mathcal{C}_{T_3}$, which implies $\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5 \in \mathcal{C}_3$ and also $\mathbf{c}_2 \in \mathcal{C}_3$. This is a contradiction to the fact that $\mathcal{C}_3$ is a 2-SMIPPC. So this case is impossible.

(3) $\mathbf{c}_1 \in \mathcal{C}_{T_3}$. If $\mathbf{c}_1 = (\infty, k, k+7)^T$ (or $\mathbf{c}_1 = (k, \infty, k-6)^T$), $k \in Z_{13}$, then $\mathbf{c}_3 = \mathbf{c}_1$, a contradiction. Similarly, if $\mathbf{c}_1 = (k, k+4, \infty)^T$, $k \in Z_{13}$, then $\mathbf{c}_4 = \mathbf{c}_1$, a contradiction. So this case is impossible.

(4) If $\mathbf{c}_1 = (\infty, \infty, \infty)^T$, then $\mathbf{c}_3 = \mathbf{c}_1$, a contradiction. So this case is impossible.

According to (1)-(4), we know that $\mathbf{c}_1 \notin \mathcal{C}_3'$, a contradiction.

So, $\mathcal{C}_3'$ is a 2-SMIPPC$(3, 287, 14)$. □

Finally, we can also construct an optimal binary 2-SMIPPC of length 3.

Lemma 5.3.24 *There exists an optimal* 2-*SMIPPC*$(3, 4, 2)$.

Proof: The following code $\mathcal{C}$ is a 2-SMIPPC$(3, 4, 2)$ from Example 5.1.2.

$$\mathcal{C} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

In order to show that the code $\mathcal{C}$ above is optimal, we only need to prove that there is no 2-SMIPPC$(3, M, 2)$ for $M \ge 5$. Assume not. Suppose $\mathcal{C}'$ is a

2-SMIPPC$(3, M, 2)$ with $M \geq 5$. Noting that $q = 2$, we know that $M \leq 8$. Choose arbitrary 5 codewords $\mathbf{c}_i = (a_i, b_i, e_i) \in \mathcal{C}'$, $1 \leq i \leq 5$. Then there must be two codewords $\mathbf{c}_i$ and $\mathbf{c}_j$, $1 \leq i \neq j \leq 5$, such that $d(\mathbf{c}_i, \mathbf{c}_j) = 3$. We may assume that $d(\mathbf{c}_1, \mathbf{c}_2) = 3$, $a_1 = 0$ and $a_2 = 1$. Hence $\text{desc}(\{\mathbf{c}_1, \mathbf{c}_2\}) = \{0,1\} \times \{0,1\} \times \{0,1\}$.

Now, we are going to show that $\text{desc}(\{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5\}) = \{0,1\} \times \{0,1\} \times \{0,1\}$. If $a_3 = a_4 = a_5 = 0$, then $\{\mathbf{c}_1, \mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5\} = \{(0,0,0)^T, (0,0,1)^T, (0,1,0)^T, (0,1,1)^T\}$. Hence $\text{desc}(\{(0,0,0)^T, (0,1,1)^T\}) = \text{desc}(\{(0,0,1)^T, (0,1,0)^T\})$, while $\{(0,0,0)^T, (0,1,1)^T\} \bigcap \{(0,0,1)^T, (0,1,0)^T\} = \emptyset$, a contradiction to the definition of a 2-SMIPPC. So, it is impossible that $a_3 = a_4 = a_5 = 0$. Similarly, it is impossible that $a_3 = a_4 = a_5 = 1$. This means that $\{a_3, a_4, a_5\} = \{0, 1\}$. Similarly, we can prove that $\{b_3, b_4, b_5\} = \{0, 1\}$ and $\{e_3, e_4, e_5\} = \{0, 1\}$. So, $\text{desc}(\{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5\}) = \{0,1\} \times \{0,1\} \times \{0,1\}$, which implies $\text{desc}(\{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5\}) = \text{desc}(\{\mathbf{c}_1, \mathbf{c}_2\})$, while $\{\mathbf{c}_3, \mathbf{c}_4, \mathbf{c}_5\} \bigcap \{\mathbf{c}_1, \mathbf{c}_2\} = \emptyset$, a contradiction to the definition of a 2-SMIPPC.

So, there does not exist a 2-SMIPPC$(3, M, 2)$ with $M \geq 5$. □

According to Theorems 5.3.3 and 5.3.20, and Lemmas 5.3.21-5.3.24, we can derive the following result.

Theorem 5.3.25 *There exists an optimal q-ary 2-SMIPPC of length 3 for any positive integer $q \equiv 0, 2 \pmod 6$.*

We would like to make some remarks here. Although the values of parameter n of the codes in this thesis are small, these codes are of practical use because of the concatenation constructions. For example, in the famous Baboon picture, $n = 19497$. We constructed a 2-SMIPPC$(3, q^2 + \frac{q(q-1)}{2}, q)$ for any positive integer $q \equiv 0, 1, 2, 5 \pmod 6$ and $q \neq 2$ in Section 5.3. Then, by using the concatenation construction (Lemma 5.1.7), we can derive a 2-SMIPPC$(19497, 63352252, 2)$ from a 2-SMIPPC$(3, 63352252, 6499)$. Now, the codewords of the 2-SMIPPC$(19497, 63352252, 2)$ can be embedded into the Baboon picture, and, in this case, we can identify at least one colluder when the number of colluders in the averaging attack is at most 2.

Chapter 6

Conclusions and Open Problems

We now give a brief summary of new results obtained in this thesis, and some interesting open problems.

6.1 Conclusions

In this thesis, we introduced three new types of anti-collusion codes to construct fingerprints resistant to the averaging collusion attack on multimedia contents. We also designed the colluder tracing algorithms for these codes. Moreover, we paid much attention to the constructions of four types of anti-collusion codes including separable codes and our new codes. We briefly list the main results of these codes in this thesis as follows.

Traceability of different types of codes

	Catch Colluders	Complexity
$\bar{t}$-SC$(n, M, 2)$	all	$O(nM^t)$
$\bar{t}$-SSC$(n, M, 2)$	all	$O(nM)$
t-MIPPC$(n, M, 2)$	at least one	$O(nM^t)$
t-SMIPPC$(n, M, 2)$	at least one	$O(nM)$

Relationships among different types of codes and hash families

Relationships among different types of codes and hash families were summarized by Stinson et al. [46], and was extended by Cheng and Miao [17]. Now it can be extended again to include the newly introduced SSCs, MIPPCs and SMIPPCs. The relationships among FPCs, SCs, SSCs, MIPPCs and SMIPPCs come from Lemmas 3.2.1, 3.2.7, 4.1.3, 5.1.3 and 5.1.5. Here we omit the definitions of different types of codes and hash families. The interested reader is referred to [17], [46] for more details.

$$\begin{tikzcd}
 & (n,M,q) \text{ code with } d_{\min} > n(1-1/t^2) \arrow[d, Rightarrow] & \\
 & (t,1-1/t)\text{-CFC}(n,M,q) \arrow[d, Rightarrow] & \\
 & t\text{-TAC}(n,M,q) \arrow[d, Rightarrow] & \\
\text{PHF}(n;M,q,\lfloor\frac{(t+2)^2}{4}\rfloor) \arrow[r, Rightarrow] & t\text{-IPPC}(n,M,q) \arrow[d, Rightarrow] \arrow[r, Rightarrow] & \text{PHF}(n;M,q,t+1) \arrow[dd, Rightarrow] \\
\text{SHF}(n;M,q,\{t,t\}) \arrow[r, Leftrightarrow] & t\text{-SFPC}(n,M,q) \arrow[d, Rightarrow] & \\
t\text{-CFF}(nq,M) & t\text{-FPC}(n,M,q) \arrow[d, Rightarrow] \arrow[l, Rightarrow] \arrow[r, Leftrightarrow] & \text{SHF}(n;M,q,\{t,1\}) \\
t\text{-SMIPPC}(n,M,q) \arrow[d, Rightarrow] & \bar{t}\text{-SSC}(n,M,q) \arrow[d, Rightarrow] \arrow[l, Rightarrow] & \\
t\text{-MIPPC}(n,M,q) & \bar{t}\text{-SC}(n,M,q) \arrow[l, Rightarrow] \arrow[r, Leftrightarrow, "q=2"] \arrow[d, Rightarrow, "q=2"] & t\text{-LACC}(n,M,2) \\
 & t\text{-AND-ACC}(2n,M,2) \arrow[d, Rightarrow] & \\
 & t\text{-LACC}(2n,M,2) &
\end{tikzcd}$$

Key

$d_{\min}$	minimum distance of the code
CFC	cover-free code
TAC	traceability code
IPPC	identifiable parent property code
SFPC	secure frameproof code
FPC	frameproof code
SSC	strong separable code
SMIPPC	strong multimedia identifiable parent property code
SC	separable code
MIPPC	multimedia identifiable parent property code
AND-ACC	AND anti-collusion code
LACC	logical anti-collusion code
PHF	perfect hash family
SHF	separating hash family
CFF	cover-free family

Figure 6.1: Relationships among different types of codes and hash families

Separable codes

- We gave an upper bound for $\overline{2}$-SC$(2, M, q)$s by a graph theoretical approach, and constructed such codes from projective planes, some of which are in fact optimal.

- We derived asymptotically optimal $\overline{2}$-SC$(4, M, q)$s for any prime power $q > 2$.

Strong separable codes

- We derived optimal $\overline{2}$-SSC$(2, M, q)$s for any $q \in \{k^2 - 1, k^2 + k - 2, k^2 + k - 1, k^2 + k, k^2 + k + 1\}$, where $k \geq 2$ is a prime power.

- We presented a construction of $\overline{2}$-SSC$(3, M, q)$s.

Multimedia identifiable parent property codes

- We gave an upper bound for t-MIPPC(n, M, q)s.

- We derived a tight upper bound for 3-MIPPC$(2, M, q)$s by using bipartite graphs.

- We constructed optimal 3-MIPPC$(2, (k^2 + 1)(k + 1)^2, (k^2 + 1)(k + 1))$s for any prime power k, and several infinite series of asymptotically optimal 3-MIPPC$(2, M, q)$s by using generalized quadrangles.

Strong multimedia identifiable parent property codes

- We derived optimal 2-SMIPPC$(2, M, q)$s for any $q \in \{k^2 - 1, k^2 + k - 2, k^2 + k - 1, k^2 + k, k^2 + k + 1\}$, where $k \geq 2$ is a prime power.

- We derived optimal 3-SMIPPC$(2, (k^2 + 1)(k + 1)^2, (k^2 + 1)(k + 1))$s for any prime power k.

- We constructed optimal 2-SMIPPC$(3, M, q)$s for each $q \equiv 0, 1, 2, 5 \pmod 6$ by using cyclic difference matrices.

6.2 Open problems

Now, we gather some open problems arising from this thesis.

1. As we mentioned, in order to reduce the computational complexity of the tracing algorithm based on a $\overline{t}$-SC (or a t-MIPPC, respectively), we introduced the notion of a $\overline{t}$-SSC (or a t-SMIPPC, respectively). Can we find some other kinds of codes with more efficient tracing algorithm, for example, with computational complexity $O(tn \log M)$?

2. We only derived asymptotically optimal $\overline{2}$-SC$(4, M, q)$s for any prime power $q > 2$ in Section 2.3. Can we give a tight bound on such codes? Furthermore, how to construct optimal $\overline{2}$-SC$(4, M, q)$s for each positive integer q?

3. In Section 3.3, we gave a construction for $\overline{2}$-SSC$(3, M, q)$s. We do not know whether these $\overline{2}$-SSC$(3, M, q)$s are optimal, even asymptotically optimal. So, it is desired to derive an upper bound for $\overline{2}$-SSC$(3, M, q)$s.

4. We derived a tight upper bound for 3-MIPPC$(2, M, q)$s by considering bipartite graphs with girth at least 8. However, we only constructed an infinite series of optimal 3-MIPPC$(2, M, q)$s. Is it possible to consider such codes in a way similar to the way used in Section 2.2?

5. How can one construct optimal 2-SMIPPC$(3, M, q)$s for $q \equiv 3, 4 \pmod 6$.

6. It would be of interest to characterize and construct these four types of codes with large parameters, that is,

   (1) $\overline{t}$-SC(n, M, q)s

   (i) $t = 2, n \geq 5$.

   (ii) $t \geq 3, n \geq t$.

   (2) $\overline{t}$-SSC(n, M, q)s

   (i) $t = 2, n \geq 4$.

   (ii) $t \geq 3, n \geq t$.

   (3) t-MIPPC(n, M, q)s

   (i) $t = 3, n \geq 3$.

   (ii) $t \geq 4, n \geq 2$.

   (4) t-SMIPPC(n, M, q)s

   (i) $t = 2, n \geq 3$.

   (ii) $t = 3, n \geq 3$.

   (iii) $t \geq 4, n \geq 2$.

Bibliography

[1] N. Alon, G. Cohen, M. Krivelevich and S. Litsyn, Generalized hashing and parent-identifying codes, *Journal of Combinatorial Theory, Series A*, vol. 104, no. 1, pp. 207-215, 2003.

[2] N. Alon and U. Stav, New bounds on parent-identifying codes: The case of multiple parents, *Combinatorics, Probability and Computing*, vol. 13, no. 6, pp. 795-807, 2004.

[3] A. Barg, G. R. Blakley and G. A. Kabatiansky, Digital fingerprinting codes: problem statements, constructions, identification of traitors, *IEEE Transactions on Information Theory*, vol. 49, no. 4, pp. 852-865, 2003.

[4] A. Barg, G. Cohen, S. Encheva, G. Kabatiansky and G. Zémor, A hypergraph approach to the identifying parent property: The case of multiple parents, *SIAM Journal on Discrete Mathematics*, vol. 14, no. 3, pp. 423-431, 2001.

[5] A. Barg and G. Kabatiansky, A class of I.P.P. codes with efficient identification, *Journal of Complexity*, vol. 20, no. 2-3, pp. 137-147, 2004.

[6] M. Bazrafshan and T. V. Trung, On optimal bounds for separating hash families, *Germany-Africa Workshop on Information and Communication Technology*, Essen, Germany, 2008.

[7] C. T. Benson, Minimal regular graphs of girths eight and twelve, *Canadian Journal of Mathematics*, vol. 18, pp. 1091-1094, 1966.

[8] S. R. Blackburn, An upper bound on the size of a code with the k-identifiable parent property, *Journal of Combinatorial Theory, Series A*, vol. 102, no. 1, pp. 179-185, 2003.

[9] S. R. Blackburn, Combinatorial schemes for protecting digital content, *Surveys in Combinatorics*, 2003 (Bangor), London Mathematical Society Lecture Note Series, vol. 307, pp. 43-78, Cambridge University Press, Cambridge, 2003.

[10] S. R. Blackburn, Frameproof codes, *SIAM Journal on Discrete Mathematics*, vol. 16, no. 3, pp. 499-510, 2003.

[11] B. Bollobás, Extremal Graph Theory, Academic Press, New York, 1978.

[12] D. Boneh and J. Shaw, Collusion-secure fingerprinting for digital data, *IEEE Transactions on Information Theory*, vol. 44, no. 5, pp. 1897-1905, 1998.

[13] D. E. Bryant and H. L. Fu, C_4-saturated bipartite graphs, *Discrete Mathematics*, vol. 259, pp. 263-268, 2002.

[14] D. de Caen and L. A. Székely, On dense bipartite graphs of girth eight and upper bounds for certain configurations in planar point-line systems, *Journal of Combinatorial Theory, Series A*, vol. 77, no. 2, pp. 268-278, 1997.

[15] B. Chen and G. W. Wornell, Quantization index modulation: a class of provably good methods for digital watermarking and information embedding, *IEEE Transactions on Information Theory*, vol. 47, no. 4, pp. 1423-1443, 2001.

[16] M. Cheng, L. Ji and Y. Miao, Separable codes, *IEEE Transactions on Information Theory*, vol. 58, no. 3, pp. 1791-1803, 2012.

[17] M. Cheng and Y. Miao, On anti-collusion codes and detection algorithms for multimedia fingerprinting, *IEEE Transactions on Information Theory*, vol. 57, no. 7, pp. 4843-4851, 2011.

[18] B. Chor, A. Fiat, M. Naor and B. Pinkas, Tracing traitors, *IEEE Transactions on Information Theory*, vol. 46, no. 3, pp. 893-910, 2000.

[19] C. J. Colbourn and J. H. Dinitz (eds.), The CRC Handbook of Combinatorial Designs, Second Edition, Chapman & Hall/CRC, Boca Raton, Florida, 2007.

[20] C. J. Colbourn, D. Horsley and V. R. Syrotiuk, Frameproof codes and compressive sensing, *Forty-Eighth Annual Allerton Conference*, pp. 985-990, Illinois, USA, 2010.

[21] I. J. Cox, J. Kilian, F. T. Leighton and T. G. Shamoon, Secure spread spectrum watermarking for multimedia, *IEEE Transactions on Image Processing*, vol. 6, no. 12, pp. 1673-1687, 1997.

[22] G. Damásdi, H. Héger and T. Szőnyi, The Zarankiewicz problem, cages, and geometries, *Annales Universitatis Scientiarum Budapestinensis de Rolando Eőtvős Nominatae. Sectio Mathematica*, vol. 56, pp. 3-37, 2013.

[23] J. Dittmann, P. Schmitt, E. Saar, J. Schwenk and J. Ueberberg, Combining digital watermarks and collusion secure fingerprints for digital images, *Journal of Electronic Imaging*, vol. 9, no. 4, pp. 456-467, 2000.

[24] S. Engle, Fingerprinting and the marking assumption, *Ecs*228 *Cryptography for E-commerce*, 2005.

[25] P. Erdős, A. Sárkőzy and V. T. Sós, On product representations of powers, I, *European Journal of Combinatorics*, vol. 16, no. 6, pp. 567-588, 1995.

[26] F. Ergun, J. Kilian and R. Kumar, A note on the limits of collusion-resistant watermarks, *Cryptology* (*Eurocrypt' 99*), vol. 1592 of Lecture Notes in Computer Science, pp. 140-149, 1999.

[27] F. Gao and G. Ge, New bounds on separable codes for multimedia fingerprinting, *IEEE Transactions on Information Theory*, vol. 60, no. 9, pp. 5257-5262, 2014.

[28] P. García-Vázquez, C. Balbuena, X. Marcote and J. C. Valenzuela, On extremal bipartite graphs with high girth, *Electronic Notes in Discrete Mathematics*, vol. 26, pp. 67-73, 2006.

[29] W. Goddard, M. A. Henning and O. R. Oellermann, Bipartite Ramsey numbers and Zarankiewicz numbers, *Discrete Mathematics*, vol. 219, pp. 85-95, 2000.

[30] E. Györi, C_6-free bipartite graphs and product representations of squares, *Discrete Mathematics*, vol. 165/166, pp. 371-375, 1997.

[31] J. W. P. Hirschfeld, Projective Geometries over Finite Fields, Second Edition, Oxford Science, Oxford, 1998.

[32] H. D. L. Hollmann, J. H. van Lint, J.-P. Linnartz and L. M. G. M. Tolhuizen, On codes with the identifiable parent property, *Journal of Combinatorial Theory, Series A*, vol. 82, no. 1, pp. 121-133, 1998.

[33] S. Hoory, The size of bipartite graphs with a given girth, *Journal of Combinatorial Theory, Series B*, vol. 86, no. 2, pp. 215-220, 2002.

[34] R. S. Irving, Integers, Polynomials, and Rings: A Course in Algebera, Springer-Verlag, New York, 2004.

[35] J. Kilian, F. T. Leighton, L. R. Matheson, T. G. Shamoon, R. E. Tarjan and F. Zane, Resistance of digital watermarks to collusive attacks, *Technical Report TR-585-98*, Computer Science Department, Princeton University, 1998.

[36] T. Lam, A result on $2k$-cycle-free bipartite graphs, *Australasian Journal of Combinatorics*, vol. 32, pp. 163-170, 2005.

[37] T. Lam, Graphs without cycles of even length, *Bulletin of the Australian Mathematical Society*, vol. 63, no. 3, pp. 435-440, 2001.

[38] Q. Li, X. Wang, Y. Li, Y. Pan and P. Fan, Construction of anti-collusion codes based on cover-free families, *6th International Conference on Information Technology: New Generations*, pp. 362-365, Las Vegas, USA, 2009.

[39] Z. Li and W. Trappe, Collusion-resistant fingerprints from WBE sequence sets, *IEEE International Conference on Communications* (*ICC'* 05), Seoul, Korea, 2005.

[40] K. J. R. Liu, W. Trappe, Z. J. Wang, M. Wu and H. Zhao, Multimedia Fingerprinting Forensics for Traitor Tracing, Hindawi Publishing Corporation, New York, 2005.

[41] A. Naor and J. Verstraëthe, A note on bipartite graphs without $2k$-cycles, *Combinatorics, Probability and Computing*, vol. 14, no. 5-6, pp. 845-849, 2005.

[42] S. Neuwirth, The size of bipartite graphs with girth eight, arXiv:math/0102210, 2001.

[43] C. I. Podilchuk and W. Zeng, Image-adaptive watermarking using visual models, *IEEE Journal on Selected Areas in Communications*, vol. 16, no. 4, pp. 525-539, 1998.

[44] H. V. Poor, An Introduction to Signal Detection and Estimation, Second edition, Springer, New York, 1999.

[45] J. Singer, A theorem in finite projective geometry and some applications to number theory, *Transactions of the American Mathematical Society*, vol. 43, no. 3, pp. 377-385, 1938.

[46] J. N. Staddon, D. R. Stinson and R. Wei, Combinatorial properties of frameproof and traceability codes, *IEEE Transactions on Information Theory*, vol. 47, no. 3, pp. 1042-1049, 2001.

[47] D. R. Stinson, Combinatorial Designs: Constructions and Analysis, Springer, New York, 2004.

[48] D. R. Stinson, T. V. Trung and R. Wei, Secure frameproof codes, key distribution patterns, group testing algorithms and related structures, *Journal of Statistical Planning and Inference*, vol. 86, no. 2, pp. 595-617, 2000.

[49] H. S. Stone, Analysis of attacks on image watermarks with randomized coefficients, *NEC Research Institute, Technical Report*, Princeton, 1996.

[50] J. K. Su, J. J. Eggers and B. Girod, Capacity of digital watermarks subjected to an optimal collusion attack, *European Signal Processing Conference*, Tampere, Finland, 2000.

[51] W. Trappe, M. Wu and K. J. R. Liu, Anti-collusion codes: multi-user and multimedia perspectives, *Proceedings of IEEE International Conference on Image Processing*, vol. 2, pp. 981-984, Rochester, USA, 2002.

[52] W. Trappe, M. Wu, Z. J. Wang and K. J. R. Liu, Anti-collusion fingerprinting for multimedia, *IEEE Transactions on Signal Processing*, vol. 51, no. 4, pp. 1069-1087, 2003.

[53] Tran van Trung and S. Martirosyan, New constructions for IPP codes, *Designs, Codes and Cryptography*, vol. 35, no. 2, pp. 227-239, 2005.

[54] Z. J. Wang, M. Wu, H. Zhao, W. Trappe and K. J. R. Liu, Resistance of orthogonal gaussian fingerprints to collusion attacks, *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing* (*ICASSP'* 03), vol. 1, pp. 724-727, 2003.

[55] R. Wenger, Extremal graphs with no C^4's, C^6's, or C^{10}'s, *Journal of Combinatorial Theory, Series B*, vol. 52, no. 1, pp. 113-116, 1991.

[56] K. Zarankiewicz, Problem of P101, *Colloquium Mathematicum*, vol. 2, pp. 301, 1951.

[57] H. Zhao, M. Wu, Z. J. Wang and K. J. R. Liu, Nonlinear collusion attacks on independent fingerprints for multimedia, *Proceedings of IEEE International Conference on Acoustics, Speech and Signal Processing* (*ICASSP'* 03), vol. 5, pp. 664-667, Hong Kong, 2003.

List of Publications

Papers related to this thesis

1. M. Cheng, H. L. Fu, J. Jiang, Y. H. Lo and Y. Miao, New bounds on $\overline{2}$-separable codes of length 2, *Designs, Codes and Cryptography*, DOI: 10.1007/s10623-013-9849-9. (Section 2.2)

2. M. Cheng, J. Jiang and Y. Miao, $\overline{2}$-Separable codes of length 4, in preparation. (Section 2.3)

3. J. Jiang, M. Cheng and Y. Miao, Strong separable codes, submitted. (Chapter 3)

4. M. Cheng, H. L. Fu, J. Jiang, Y. H. Lo and Y. Miao, Codes with the identifiable parent property for multimedia fingerprinting, submitted. (Chapter 4)

5. J. Jiang, M. Cheng, Y. Miao and D. Wu, Multimedia IPP codes with efficient tracing, submitted. (Chapter 5)

Papers not related to this thesis

1. J. Jiang, D. Wu and P. Fan, General constructions of optimal variable-weight optical orthogonal codes, *IEEE Transactions on Information Theory*, 57(7), pp. 4488-4496, 2011.

2. J. Jiang, D. Wu and P. Fan, More results on optimal optical orthogonal codes with weight four, *Proceedings of The Fifth International Workshop on Signal Design and Its Applications in Communications*, pp. 122-125, Guilin, China, 2011.

3. J. Jiang, D. Wu and P. Fan, General constructions for $(v, 4, 1)$ optical orthogonal codes via perfect difference families, *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences* E95-A(11): 1921-1925, 2012.

4. J. Jiang, D. Wu and M. H. Lee, Some infinite classes of optimal $(v, \{3, 4\}, 1, Q)$-OOCs with $Q = \{(1/3, 2/3), (2/3, 1/3)\}$, *Graphs and Combinatorics*, 29(6), pp. 1795-1811, 2013.

5. M. Cheng, J. Jiang and D. Wu, Bounds and constructions for two-dimensional variable-weight optical orthogonal codes, *Journal of Combinatorial Designs*, 22(9), pp. 391-408, 2014.

6. M. Cheng, J. Jiang, Y. Miao and H. Li, Bounds and constructions for $\overline{3}$-separable codes of length 3, in preparation.