Combinatorial designs and codes related to information-communication

Yiling Lin

Acknowledgments

When I came to Japan, I never dared to imagine that I would pursue a PhD at Nagoya University. Without my supervisor, I might not have completed the long journey of my PhD studies. So, first and foremost, I would like to thank my supervisor, Professor Masakazu Jimbo, Nagoya University, for his kind supervision and encouragement, not only in my studies but also in my private life. He has provided an environment full of possibilities and encouraged me to seek the opportunities. I am most grateful to him for bringing me to the world of combinatorial mathematics and letting me have a chance to solve so many problems. I was able to complete this thesis because of his patience, excellent guidance and advice. I am also very grateful to Professor Miwako Mishima of Gifu University. She is really kind and caring. She always patiently helped me with the insufficient part of my papers. I thank her for teaching me how to write a fluent and professional paper. I would like to thank both of them for encouraging me to and supporting me in, not only attending meetings and conferences, but also taking part in the preparatory group for international conferences. These were all very good opportunities for me to practice presentation skills and to develop communication and coordination.

I would like to thank Professor Junya Satoh, who is a member of my thesis committee. He taught me a lot about number theory. He also helped to review my papers and offered valuable comments. Without him, my research could not be so complete and productive. I express my warm thanks to Professor Hung-Lin Fu, National Chiao Tung University (Taiwan), and Professor Chin-Mei Kau, Tamkang University (Taiwan). It was really an important experience for me to meet and get to know researchers from my own country. I thank them for giving me valuable advice and encouragement during my student life in Japan.

I would like to thank Professor Yo Matsubara and Dr. Janet Nora Henderson for dedicating their time to read and check the English grammar of my

writing. I also express my sincere gratitude to Professor Tomio Hirata and Professor Mutsunori Yagiura, who are also members of my thesis committee, for carefully reading and commenting on my thesis.

I want to say thanks to Professor Masanori Sawa and Dr. Koji Momihara, who are excellent researchers in combinatorial mathematics. Their passion for research influenced me to try to get the PhD degree. I thank them for sharing their knowledge and thoughts on my research topic. Special thanks go to Professor Ryoh Fuji-Hara, University of Tsukuba, and Professor Tomoko Adachi, Toho University, for taking care of me during my first conference in the USA. Many thanks to Professor Ying Miao, University of Tsukuba, Professor Keisuke Shiromoto, Kumamoto University, Professor Nobuko Miyamoto, Tokyo University of Science, Professor Akihiro Munemasa, Tohoku University, and Mariko Hagita, Ochanomizu University, whom I met at conferences. My communication skills and thinking skills were improved because of your unselfish teaching. Also, I would like to thank all our laboratory members. The time we studied in the laboratory will be an unforgettable memory in my life.

Finally, I wish to express my gratitude to my family and my friends for their support, especially my husband, Lipu, who spent many sleepless nights with me and was always my best listener. It would have been impossible to complete my doctoral studies without their hearty encouragement.

Yiling Lin
Nagoya University

Contents

Chapter 1

Introduction

Combinatorics cuts across vast areas of mathematics. Since it has many applications, including computer science, genetics, experimental design, scheduling and so on, it has become one of the fastest-growing branches of mathematics today. Design theory, coding theory, cryptology, combinatorial algorithms, graph theory, enumeration, combinatorial set theory, and combinatorial representation theory are all included in combinatorics.

There are many problems in combinatorics, such as, selection problems, binomial coefficients, enumeration problems, combinatorial identities and inequalities. Combinatorial design theory, which contains block designs, difference sets, Latin squares, orthogonal arrays, Hadamard matrices, and finite geometries, is an important research areas in combinatorics. The subject of combinatorial designs is studied from several viewpoints: optimal structure, existence, constructions, counting of nonisomorphic structures, relations to other fields of mathematics, etc. In this thesis, we look at combinatorial designs and combinatorial codes from the viewpoint of existence and constructions of optimal combinatorial configurations.

The origin of combinatorial designs can be traced back to 1782, when L. P. Euler introduced the famous "36 officers problem" and began the search for mutually orthogonal Latin squares. In the mid-19th century, T. P. Kirkman, J. Steiner and A. Cayley explored such topics as triple systems and Room squares. It is often said that the modern history of combinatorial design (since the 20th century) originated in the statistical design of experiments established by R. A. Fisher and F. Yates in the 1920s. Their investigations revealed a connection between "combinatorial design" and "statistical design of experiments" [26, 27, 88]. Such demands from practical applications con-

tributed a lot to the growth of combinatorial design theory. For example, the two combinatorial designs "balanced incomplete block designs" and "orthogonal arrays," which arose from the design of experiments, were introduced by Yates [88] and Rao [65] respectively. These two combinatorial designs are still of interest to modern researchers.

Combinatorial designs have had a connection with the field of statistics from the earliest stage of research. In 1948, C. E. Shannon [70] published the paper *"A mathematical theory of communication,"* which formed the foundation of information theory. He also worked on essential mathematical research in many areas related to information processing and communication. Shannon proved the existence of codes attaining the channel capacity with error probability tending to zero by using probabilistic methods, but he did not give any concrete constructions of a series of such good codes. In 1950, Hamming [33] gave methods to achieve good communication based on linear codes, which are now known as Hamming codes. His approach provided a combinatorial viewpoint to coding theory. Actually, the properties and structures of combinatorial designs, such as t-designs and balanced incomplete block designs, can be found in some "good" codes. Due to this relation, combinatorial designs and coding theory have mutually contributed to each other's development.

Codes are used not only as a tool for detecting and correcting errors caused by noise in transmission networks and storage devices, but also as protocols for data transmission over multiple-access channels. Regardless of whether a single user or multiple users exist in a channel, the problem of synchronization may occur during transmission. The theory of "difference families" from combinatorial designs plays an important role in solving such problems. A combinatorial design called a "difference system of sets (DSS)" was introduced by Levenshtein [45] for constructing codes that synchronize data frames in transmission. For successful transmission in multiple-access communication, combinatorial codes such as "optical orthogonal codes" and "conflict-avoiding codes" are typical examples of applications of difference families.

With the popularization of the Internet, security of information during transmission has become very important. Security requirements for Internet communication triggered the development of modern cryptography. The idea of "public key cryptography," which is one of the main research directions of modern cryptography, was proposed in the 1970s. After that, one of the most famous public key cryptosystems, "RSA," which is based on the complexity of factoring large integers, was introduced by R. Rivest, A. Shamir

and L. Adleman in 1977. Such public key cryptosystems are utilized by both sender and receiver to exchange encrypted messages in an insecure network without communicating the secret key in advance through a secure channel. As attacks on communication become more severe and more sophisticated, the necessity of protecting the "key" is more critical than ever. Secret sharing schemes, which provide ways of secure key management, is a prominent subject in modern cryptography. In particular, combinatorial designs give important tools for the study of secret sharing.

In the late 20th century, a new field, "quantum information science," which is based on quantum physics and information science, was founded. Recall that the RSA cryptosystem is based on the complexity of the problem of factoring large integers in current computer system. In 1994, P. W. Shor gave a quantum algorithm for integer factorization on a quantum computer which could break RSA fast. Due to Shor's pioneering work, the field of quantum information science has begun to attract many researchers. Error correction in quantum systems is studied because of its importance in the theory of quantum computation and quantum communications. Quantum error correcting codes are used to protect quantum information from errors due to decoherence and other quantum noise. Shor [71] and Steane [75] introduced the first constructions of quantum error correcting codes. Since then, quantum error correcting codes have been studied by many researchers (see, for example, [9, 10, 20, 75, 76]). Techniques from combinatorial designs are useful in constructing families of quantum error correcting codes (see, for example, [18, 30, 84]). Among such quantum error correcting codes, there is a special code called a quantum jump code, which is designed to correct quantum decay and jump errors in the memory of quantum computers [1]. To realize a quantum jump code, a family of combinatorial designs called a "t-spontaneous emission error design (t-SEED)" is used. Finding applications of combinatorial designs to quantum systems is also an interesting problem.

As discussed above, there are a variety of applications of combinatorial designs. In this thesis, we focus on two topics in combinatorial designs and codes related to information-communication: "t-spontaneous emission error designs" and "conflict-avoiding codes." We first study their optimalities from the viewpoint of applications and investigate the existence and constructions of such optimal combinatorial structures.

1.1 t-designs and large sets

Here, we introduce the notion of a t-design, which is closely related to a t-SEED.

Let V be a set with v *points* and $\mathcal{B}$ be a family of k-subsets, called *blocks*, of V. A t-(v,k,λ) design is a pair $(V,\mathcal{B})$ such that every t-tuple of V is contained in exactly λ blocks. That is, a pair $(V,\mathcal{B})$ is a t-(v,k,λ) design if $|\{B \in \mathcal{B} : T \subset B\}| = \lambda$ holds for any $T \in \binom{V}{t}$.

Note that, in general, there is no requirement that all the blocks in a design be different. If two blocks have the same set of points, then we say there is a repeated block. A t-design is said to be *simple* if it contains no repeated blocks. A t-design with $\lambda = 1$ is called a *Steiner t-design*. It is obvious that a Steiner t-design is simple.

Generally, the terms "subset" and "tuple" are used interchangeably. In this thesis, when we need to choose any t points from a point set, we use the term "t-tuple," whereas the term "k-subset" is utilized for a block.

Example 1.1.1. Let $V = \{0, 1, \cdots, 6\}$ and

$$\mathcal{B} = \{013, 124, 235, 346, 450, 561, 602\},$$

where 013 stands for $\{0, 1, 3\}$ and so on. Then $(V,\mathcal{B})$ is a 2-$(7, 3, 1)$ design.

Example 1.1.2. Let $V = \{0, 1, \cdots, 7\}$ and

$$\begin{aligned}\mathcal{B} =\{&0124, 0235, 0346, 0457, 0561, 0672, 0713,\\ &3567, 4671, 5712, 6123, 7234, 1345, 2456\}.\end{aligned}$$

Then $(V,\mathcal{B})$ is a 3-$(8, 4, 1)$ design.

The following elementary lemmas on t-designs are well-known. For the reader's convenience, proofs of the lemmas are given.

Lemma 1.1.3. *The number of blocks in a t-(v,k,λ) design is*

$$|\mathcal{B}| = \lambda \binom{v}{t} \Big/ \binom{k}{t}.$$

Proof. For a t-(v,k,λ) design, counting the number of pairs $(T, B) \in \binom{V}{t} \times \mathcal{B}$ in two ways, we get $\lambda\binom{v}{t} = |\mathcal{B}|\binom{k}{t}$. □

Lemma 1.1.4. *A t-(v,k,λ) design is also an s-(v,k,λ_s) design for $0 \le s \le t$, where*

$$\lambda_s = \lambda \binom{v-s}{t-s} \Big/ \binom{k-s}{t-s}. \tag{1.1.1}$$

Proof. For any given s-subset I, let $V' = V \setminus I$ and $\mathcal{B}' = \{B \setminus I : I \subset B \in \mathcal{B}\}$. Then it is easy to show that $(V', \mathcal{B}')$ is a $(t-s)$-$(v-t, t-s, \lambda_s)$ design. By Lemma 1.1.3, we have

$$\lambda \binom{v-s}{t-s} = |\mathcal{B}'| \binom{k-s}{t-s}.$$

Note that λ_s is the number of blocks containing a given s-subset I. Then $|\mathcal{B}'| = \lambda_s$, which completes the proof. □

A t-design is often specified by its incidence matrix.

Let $(V, \mathcal{B})$ be a t-design. Denote the v points in V as $p_1, p_2, \cdots, p_v$ and b blocks in $\mathcal{B}$ as $B_1, B_2, \cdots, B_b$. A $v \times b$ matrix $N = (a_{ij})$ with

$$a_{ij} = \begin{cases} 1 & \text{if } p_i \in B_j, \\ 0 & \text{otherwise} \end{cases}$$

is called the *incidence matrix* of a design $(V, \mathcal{B})$. That is, each point corresponds to a row of N, and each block corresponds to a column of N.

Example 1.1.5. An incidence matrix N of a 2-$(7,3,1)$ design is

$$N = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}.$$

There are $b = \lambda \binom{v}{t} \Big/ \binom{k}{t}$ blocks in a t-(v,k,λ) design, but the number of all k-subsets of V is $\binom{v}{k}$, which is larger than b for $k > t$. This means that we have a chance to find some other t-(v,k,λ) designs which are mutually disjoint.

A *large set* of t-designs, denoted by $LS_\lambda(t,k,v)$, is a partition of the complete design (that is, the set of all k-subsets of V) into N disjoint t-(v,k,λ) designs, where $N = \binom{v-t}{k-t}/\lambda$. Large sets are also denoted by $LS[N](t,k,v)$.

We give an example of a large set. Throughout this thesis, we identify the residue ring class $[i]$ in $\mathbb{Z}_v = \mathbb{Z}/v\mathbb{Z}$ with $i \in \mathbb{Z}$.

Example 1.1.6. The following $(V; \mathcal{B}^{(0)}, \mathcal{B}^{(2)}, \ldots, \mathcal{B}^{(6)})$ is an $LS_1(2,3,9)$ containing 7 disjoint 2-$(9,3,1)$ designs, where $V = \{\infty, \infty'\} \cup \mathbb{Z}_7$. Let

$$\begin{aligned}\mathcal{B}^{(i)} = \big\{&\{\infty, \infty', i\}, \{i, 1+i, 6+i\}, \{i, 2+i, 5+i\},\\ &\{i, 3+i, 4+i\}, \{1+i, 2+i, 4+i\}, \{3+i, 5+i, 6+i\},\\ &\{\infty, 1+i, 5+i\}, \{\infty, 2+i, 3+i\}, \{\infty, 4+i, 6+i\},\\ &\{\infty', 1+i, 3+i\}, \{\infty', 2+i, 6+i\}, \{\infty', 4+i, 5+i\}\big\}.\end{aligned}$$

That is, $\{\mathcal{B}^{(0)}, \mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(6)}\}$ is a partition of $\binom{V}{3}$, and each $(V, \mathcal{B}^{(i)})$ is a 2-$(9,3,1)$ design.

Given parameters t, v and k, there is a smallest positive integer $\lambda_{\min}$, denoted also by $\lambda_{\min}(t,k,v)$, such that the right hand side of (1.1.1) in Lemma 1.1.4 is an integer for each s. If a t-(v,k,λ) design exists, it is easy to verify that $\lambda_{\min}$ divides λ. If a t-(v,k,λ) design exists, then λ must be a multiple of $\lambda_{\min}(t,k,v)$. The large sets that are known to exist are listed below:

- An $LS_{\lambda_{\min}}(1,k,v)$ exists. [4, 34]
- An $LS_1(2,3,v)$ exists for $v \equiv 1,3 \pmod 6$ except for $v = 7$. [50, 51, 67, 68, 81, 79]
- An $LS_1(2,4,13)$ exists. [15]
- An $LS_6(2,4,14)$ exists. [43]
- An $LS_1(2,4,16)$ exists. [55]
- An $LS_{39}(2,4,29)$ exists. [21]
- An $LS_{\lambda_{\min}}(2,5,v)$ exists for $v = 13, 14, 15$. [12]
- An $LS_{\lambda_{\min}}(2,6,13)$ exists. [12]
- An $LS_2(3,4,13)$ exists. [43]
- An $LS_{\lambda_{\min}}(3,4,v)$ exists for $v \equiv 0 \pmod 3$. [82]

- An $LS_3(3,4,v)$ exists for $v \equiv 0$ or $6 \pmod{12}$. [82]
- An $LS_6(3,4,v)$ exists for $v \equiv 9 \pmod{12}$. [82]
- An $LS_{12}(3,4,v)$ exists for $v \equiv 3 \pmod{12}$. [82]
- An $LS_{\lambda_{\min}}(3,4,14v+3)$ exists for $v \geq 1$. [12]
- An $LS_{\lambda_{\min}}(3,6,13)$ exists. [12]
- An $LS_3(4,5,13)$ exists. [43]
- An $LS_{\lambda_{\min}}(4,5,20v+4)$ exists for $\gcd(v,30)=1$. [83]
- An $LS_{60}(4,5,60v+4)$ exists for $\gcd(v,60)=1,2$. [83]

Etzion and Hartman [22] constructed $(v-5)$ disjoint 3-$(v,4,1)$ designs for $v = 5{\cdot}2^n$. If an $LS_1(3,4,v)$ exists, then there are $(v-3)$ disjoint 3-$(v,4,1)$ designs. So, the existence of only two more is required to show an $LS_1(3,4,v)$ exists. Chee and Magliveras [12] showed the following result:

Lemma 1.1.7 ([12]). *If an $LS[N_1](t,k,v)$ and an $LS[N_2](t,k+1,v)$ exist, then an $LS[\gcd(N_1,N_2)](t,k+1,v+1)$ exists.*

For a t-(v,k,λ) design, if we select all blocks containing a fixed point x and delete x from each block, then we get a $(t-1)$-$(v-1,k-1,\lambda)$ design, called a *derived design*. Moreover, we get that the existence of an $LS[N](t,k,v)$ implies the existence of an $LS[N](t-1,k-1,v-1)$, by deleting a point x.

t-designs have applications in cryptography. Stinson and Vanstone [77] proposed a combinatorial characterization of a perfect threshold scheme, named "m mutually $(t+1)$-compatible k-uniform hypergraphs," which is also a family of designs. As a special example, it was shown that a perfect threshold scheme with the maximum key space can be constructed by a t-$(v,k,1)$ design which can be partitioned into $(t-1)$-$(v,k,1)$ designs (see [66, 77]). As this representative example shows, mutually disjoint designs play a significant role in the application process.

1.2 t-spontaneous emission error designs

As stated in Section 1.1, a large set $LS[N](t,k,v)$ contains N disjoint t-designs, and each t-design satisfies a "balancedness" property such that the parameter λ depends on the number t. In this section, we consider a t-spontaneous emission error design whose structure is different but similar to a large set of t-designs in some sense. In a t-spontaneous emission error

design, the balancedness property is configured such that the parameter λ depends on the chosen t-subset of V.

The origin of t-spontaneous emission error designs, or t-SEEDs for short, arises from t-error correcting quantum jump codes. A quantum jump code is a kind of quantum error correcting code. Quantum error correcting codes have been studied by many authors [9, 10, 20, 75, 76], motivated by the pioneering work of Shor [71]. Among them, Alber et al. [1] introduced a quantum jump code to correct errors caused by quantum jumps. Beth et al. [6] proposed a special type of combinatorial design to construct a quantum jump code, which they named a t-SEED. A t-SEED has a close connection to a large set of t-designs. The definition of a t-SEED is given as follows:

For positive integers $v > k \geq t > 0$ and m,et V be a set with v points and $\mathcal{B}^{(i)}$ be a family of k-subsets of V for $1 \leq i \leq m$.

A system $(V; \mathcal{B}^{(1)}, \mathcal{B}^{(2)}, \ldots, \mathcal{B}^{(m)})$ is called a t-$(v, k; m)$ SEED if the following conditions are satisfied:

(i) Any two families $\mathcal{B}^{(i)}$ and $\mathcal{B}^{(j)}$ are disjoint. This means that there are no common blocks in $\mathcal{B}^{(i)}$ and $\mathcal{B}^{(j)}$ for any $i \neq j$.

(ii) For any u-tuple T of V $(u \leq t)$, the parameter $\mu_T = \lambda_T^{(i)}/|\mathcal{B}^{(i)}|$ is a constant not depending on i.

Throughout this article, we often call $(V, \mathcal{B}^{(i)})$ or simply $\mathcal{B}^{(i)}$ a *design* of a t-SEED. For a t-SEED, let $\mathcal{T} = \{T \in \binom{V}{t} : \mu_T > 0\}$, where $\binom{V}{t}$ denotes the set of all t-tuples of V. That is, $\mathcal{T}$ is the family of t-tuples contained in some blocks of $\mathcal{B}^{(i)}$ for any i. In order to avoid the trivial case, we assume that $m > 1$ and $\mathcal{T} \neq \emptyset$.

Example 1.2.1. Let $V = \{0, 1, \ldots, 5\}$ be a set of 6 points and let $k = 3$. An example of a 2-$(6, 3; 2)$ SEED $(V; \mathcal{B}^{(1)}, \mathcal{B}^{(2)})$ is shown as follows:

$$\mathcal{B}^{(1)} = \{012, 023, 034, 045, 015, 135, 124, 235, 134, 245\},$$
$$\mathcal{B}^{(2)} = \{013, 024, 035, 014, 025, 123, 234, 345, 145, 125\},$$

where 012 stands for $\{0, 1, 2\}$. In this case, $\mu_T = \frac{1}{5}$ and $\lambda_T^{(i)} = 2$ for any pair $T \in \binom{V}{2}$ and $i = 1, 2$. Another example of a 2-$(6, 3; 2)$ SEED is shown as follows:

$$\mathcal{B}^{(1)} = \{024, 134, 125, 035\},$$
$$\mathcal{B}^{(2)} = \{124, 034, 025, 135\}.$$

In this example, $\mathcal{T} = \binom{V}{2} \setminus \{01, 23, 45\}$ and $\lambda_T^{(i)} = 1$ (hence, $\mu_T = \frac{1}{4}$) if $T \in \mathcal{T}$, otherwise $\lambda_T^{(i)} = 0$.

Beth et al. [6] showed the following in terms of quantum jump codes:

Lemma 1.2.2 ([6]). *If* $(V; \mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m)})$ *is a* t-$(v, k; m)$ *SEED, then* $(V; \bar{\mathcal{B}}^{(1)}, \ldots, \bar{\mathcal{B}}^{(m)})$ *is a* t-$(v, v-k; m)$ *SEED, where* $\bar{\mathcal{B}}^{(i)} = \{B^c : B \in \mathcal{B}^{(i)}\}$.

Lemma 1.2.3 ([6]). *If* $(V; \mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m)})$ *is a* t-$(v, k; m)$ *SEED, then for any* $p \in V$, $(V \setminus \{p\}; \mathcal{B}^{(1)'}, \ldots, \mathcal{B}^{(m)'})$ *is a* $(t-1)$-$(v-1, k-1; m)$ *SEED, where* $\mathcal{B}^{(i)'} = \{B \setminus \{p\} : p \in B \in \mathcal{B}^{(i)}\}$.

Example 1.2.4. Any t-(v, k, λ) design $(V, \mathcal{B})$ is a t-$(v, k; 1)$ SEED, where μ_T is a constant depending only on the size $|T| = u$.

Example 1.2.5. A large set $LS_\lambda(t, k, v)$ is a t-$(v, k; \binom{v-t}{k-t}/\lambda)$ SEED.

The parameter μ_T (≤ 1) can be seen as the ratio of occurrence of a specific subset T in every design $\mathcal{B}^{(i)}$. It is clear that the conditions of a t-SEED are less restrictive than that of a large set of t-designs, since the parameter μ_T can differ depending on the choice of T, whereas in the case of a large set $\lambda_T^{(i)}$ is a constant depending only on the size of T. Hence if $\lambda_T^{(i)}$ is a constant for all $T \in \binom{V}{t}$, and does not depend on T, then the t-SEED is a collection of t-designs.

So far, only a few constructions of t-SEEDs are known. Recently, Fang and Chang [23, 24] gave constructions of 3-$(v, k; m)$ SEEDs for $(v, k, m) \in \{(32, 8, 5), (56, 12, 9), (56, 16, 9), (56, 24, 9), (80, 16, 52)\}$ and some scattered 5-SEEDs. Moreover, the nonexistence of some t-SEEDs can be found in [25].

1.3 Conflict-avoiding codes

Conflict-avoiding codes have been studied as protocol sequences for a multiple-access channel (collision channel) without feedback [32, 46, 47, 56, 63, 86]. For the technical description of such a multiple-access channel model, see [5, 54]. In such channels, the time axis is partitioned into time units, called slots, in each of which a single packet can be transmitted. All users have slot synchronization but no other synchronization is assumed. The channel is assumed to be a collision channel without feedback. In a particular slot, if none of the users is sending a packet, then the channel output in that slot is the silence symbol. If exactly one user is sending a packet, then the packet

has successful transmission and the channel output in that slot is the sent packet. If two or more users are sending packets, then there is a conflict and the channel output in that slot is the collision symbol (see Figure 1.3.1). In order for each user to send packets successfully in a collision channel without feedback, he/she makes copies of each packet and sends them in a frame consisting of the prescribed number of consecutive slots.

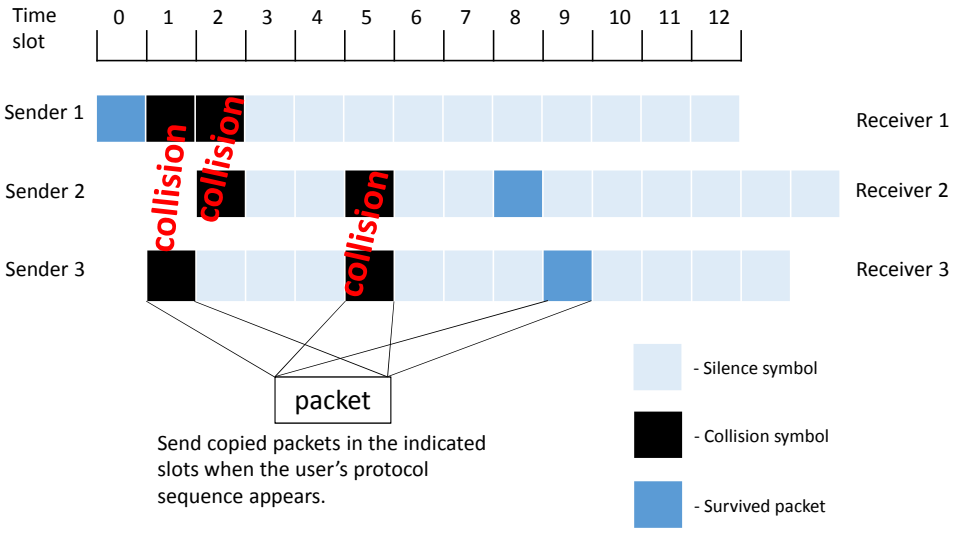

Figure 1.3.1: Schematic view of a multiple-access channel

As a transmission protocol, a binary sequence $C = (x_0, x_1, \ldots, x_{n-1})$, called a "codeword", is uniquely assigned to each user, where x_i corresponds to the ith slot in a frame. Each user in a channel can start his/her transmission at any slot, that is, the frame synchronization is not assumed, and he/she sends copies of a packet or stays silent at the ith slot in a frame depending on $x_i = 1$ or 0. Note that each user uses his/her protocol sequence periodically until he/she has no more packets to send. A *conflict-avoiding code* is a code which guarantees that each of the active users sends at least one packet successfully even if collisions occur in the channel.

A conflict-avoiding code (CAC) of length n and weight w is defined as a set $\mathcal{C} \subseteq \{0,1\}^n$ of binary vectors, called *codewords*, of Hamming weight w such that arbitrary cyclic shifts x', y' of distinct codewords $x, y \in \mathcal{C}$ intersect at most at one coordinate, that is, $\mathrm{dist}(x', y') \geq 2w - 2$ holds, where $\mathrm{dist}(x', y')$ is the Hamming distance between x' and y'. We denote the class of all the CACs of length n and weight w by $\mathrm{CAC}(n, w)$.

The *support* of a codeword $x = (x_0, x_1, \ldots, x_{n-1})$ is the set of indices of its nonzero coordinates. In this article, a codeword is expressed by its support, not as a binary vector. Then any code $\mathcal{C} \in \mathrm{CAC}(n, w)$ can be regarded as a collection of w-subsets of $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$, the ring of residues modulo n, such that

$$\Delta(x) \cap \Delta(y) = \emptyset \quad \text{for any } x, y \in \mathcal{C},$$

where $\Delta(x) = \{j - i \pmod n : i, j \in x, i \neq j\}$ is the set of differences arising from x. Since for any codeword x in a code $\mathcal{C} \in \mathrm{CAC}(n, w)$, the elements of $\Delta(x)$ are symmetric with respect to $n/2$, we henceforth consider the halved difference set

$$\Delta_2(x) = \left\{ i \in \Delta(x) : i \leq \left\lfloor \frac{n}{2} \right\rfloor \right\}$$

instead of $\Delta(x)$. We also use the notation $\Delta_2(\mathcal{C})$ to denote $\cup_{x \in \mathcal{C}} \Delta_2(x)$.

If x is of form $\{0, i, \ldots, (w-1)i\}$, then it is said to be *equi-difference* (or *centered* when $w = 3$), and, if every codeword in a code $\mathcal{C} \in \mathrm{CAC}(n, w)$ is equi-difference, then $\mathcal{C}$ is called an *equi-difference* code (or *centered* code when $w = 3$). The class of all the equi-difference CACs of length n and weight w is denoted by $\mathrm{CAC}^e(n, w)$. Obviously $\mathrm{CAC}^e(n, w) \subseteq \mathrm{CAC}(n, w)$.

Let $M(n, w)$ be the maximum size of a code in $\mathrm{CAC}(n, w)$, that is,

$$M(n, w) = \max\{|\mathcal{C}| : \mathcal{C} \in \mathrm{CAC}(n, w)\}.$$

A code $\mathcal{C} \in \mathrm{CAC}(n, w)$ is said to be *optimal* if $|\mathcal{C}| = M(n, w)$. Furthermore, an optimal code $\mathcal{C} \in \mathrm{CAC}(n, w)$ is said to be *tight* if $\Delta_2(\mathcal{C}) = \{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor\}$. The maximum size of a code in $\mathrm{CAC}^e(n, w)$ is defined as

$$M^e(n, w) = \max\{|\mathcal{C}| : \mathcal{C} \in \mathrm{CAC}^e(n, w)\}$$

similarly to $M(n, w)$. It is known that a tight equi-difference CAC of weight w is equivalent to a perfect $(w-1)$-shift code [48] and a necessary and sufficient condition for the existence of a perfect $(w-1)$-shift code in a finite abelian group is known for $w = 2, 3$ due to Levenshtein and Vinck [48], and for $w = 4, 5$ due to Munemasa [61].

For $w = 3$, the functions $M(n, 3)$ and $M^e(n, 3)$ were studied in [36, 46, 47, 59]. Levenshtein and Tonchev [47] proved that

$$M(n, 3) = M^e(n, 3) = \frac{n-2}{4} \quad \text{if } n \equiv 2 \pmod 4 \tag{1.3.1}$$

and

$$M(n, 3) \simeq M^e(n, 3) \simeq \frac{m}{4} \quad \text{for odd prime } n. \tag{1.3.2}$$

Levenshtein [46] extended the asymptotic result (1.3.2) to all sufficiently large odd n.

For even n, the spectrum of $M(n,3)$ was settled by Jimbo et al. [36], Mishima et al. [58] and Fu et al. [28] together with (1.3.1) due to Levenshtein and Tonchev [47].

On the other hand, for odd n, the known results on $M(n,3)$ are far from complete (see [74]). Indeed, we can find in Momihara [59] a necessary and sufficient condition for the existence of a tight code in $\mathrm{CAC}^e(n,3)$ for odd n and an algorithm for finding admissible n. In Fu et al. [29], the condition is restated in terms of the multiplicative suborder of 2 modulo p for all prime factors p of n. But the conditions in both [29] and [59] are fairly complex and must be examined for each prime factor of n. For this reason, only a few explicit series of odd n are known. These are $n = 2^{2k}+1$ and $2^{2^k}-1$ due to Wu and Fu [87]. Ma et al. [52] presented constructions of an optimal equi-difference CAC and an optimal tight CAC of odd prime length p and weight 3, and formulated $M(p,3)$ and $M^e(p,3)$. However, for their formulae to have practical meaning, the number of cosets of $-(2)_p \cup (2)_p$ still needs to be determined, where $(2)_p$ is the multiplicative subgroup of $\mathbb{Z}_p^*$ with generator 2. Moreover, their construction of an optimal tight CAC imposes a certain precondition. This implies that, even restricting ourselves to odd prime length, providing a series of odd n for which $M(n,3)$ and $M^e(n,3)$ can be determined is a demanding problem.

As for $w \geq 4$, several constructions of optimal equi-difference CACs for weight $w = 4, 5$ are given in [60], and an upper bound of $M(n,w)$ for general weights w can be found in [72]. Lo et al. [49] proposed a graphical representation of an equi-difference CAC, and then determined $M^e(2^a 3^b, 4)$ for $a, b \geq 0$ by finding a "maximum weighted matching" in a weighted directed graph. However, their graphical representation tends to be rather complex to deal with for a general length n. Hence, we also focus on the weight four case and investigate sizes and constructions of optimal codes in equi-difference CACs of weight four by using properly defined directed graphs.

We show our results about equi-difference conflict-avoiding codes of weight three and four in Chapter 3.

1.4 Thesis summary

We discuss some properties and constructions of optimal t-SEEDs and optimal conflict-avoiding codes, in the next two chapters.

In Chapter 2, we study the extremal properties of a t-$(v, k; m)$ SEED, since, in the application to quantum jump codes, the number of designs m corresponds to the dimension of the jump code and it is required to be as large as possible. By utilizing some fundamental combinatorial configurations, several recursive constructions are presented. Moreover, a new application of t-SEEDs to secret sharing schemes is given.

In Chapter 3, we discuss optimal equi-difference CACs of weights three and four. Firstly, we give some explicit series of optimal equi-difference CACs of odd length n and weight three by applying properties of the multiplicative order of the unit 2 in $\mathbb{Z}_n$ and cyclotomic polynomials. Moreover, we investigate sizes and constructions of optimal equi-difference CACs of weight four by using properties of the multiplicative orders of $2, 3$ and properly defined directed graphs. As a consequence, several series of optimal equi-difference CACs of weights three and four are provided.

In Chapter 4, we provide concluding remarks and open problems.

Chapter 2

Extremal properties of t-SEEDs and recursive constructions

In this chapter, we show the relation between a t-SEED and a large set of t-designs. In particular, in Section 2.1, we prove that an optimal t-SEED is a large set of t-designs. The extremal properties of a t-SEED imply the nonexistence of some t-SEEDs.

In Section 2.2, we introduce fundamental combinatorial designs: group divisible designs, transversal designs, orthogonal arrays, and a large set of orthogonal arrays. By utilizing these combinatorial designs, some recursive constructions of t-SEEDs are given.

A t-SEED originates from a quantum jump code. It is known that the properties of disjoint t-designs can be applied to secret sharing schemes due to Stinson and Vanstone [77]. In a similar manner, in Section 2.3, we propose a new application to secret sharing schemes by utilizing the properties of a t-SEED. A performance comparison between our result and that of [77] is also discussed.

2.1 Optimal t-SEEDs and large sets

In order to find a t-SEED having m as large as possible for given t, k and v, we need to know the bound of designs m. Indeed, an upper bound for the dimension of a quantum jump code can be regarded as an upper bound for a t-SEED since t-SEEDs are a special class of quantum jump codes [6].

Theorem 2.1.1 ([6]). *The number m of the $\mathcal{B}^{(i)}$s of a t-$(v,k;m)$ SEED is bounded by*

$$m \le \min\left\{ \binom{v-t}{k-t}, \binom{v-t}{k} \right\}. \tag{2.1.1}$$

For families $\mathcal{A}$ and $\mathcal{B}$ of subsets of V, let $\mathcal{A}+\mathcal{B} = \{A \cup B : A \in \mathcal{A}, B \in \mathcal{B}\}$. In particular, if $\mathcal{B} = \{B\}$, then we write $\mathcal{A}+B$ instead of $\mathcal{A}+\{B\}$. Note that $\mathcal{B}+\emptyset = \mathcal{B}$ for the empty set $\emptyset$.

A t-$(v,k;m)$ SEED $(V;\mathcal{B}^{(1)},\mathcal{B}^{(2)},\ldots,\mathcal{B}^{(m)})$ is said to be *optimal* if the number m of designs attains the upper bound of Theorem 2.1.1. For an optimal t-$(v,k;m)$ SEED, the number m is $\binom{v-t}{k-t}$ or $\binom{v-t}{k}$, depending on the values of t, k and v. We can get the same result by considering the complement. For convenience, we only discuss an optimal t-$(v,k;m)$ SEED with $1 \le t < k \le v/2$ in this thesis, and hence $m = \binom{v-t}{k-t}$.

Lemma 2.1.2. *For any optimal t-$(v,k;m)$ SEED, $\lambda_T^{(i)} \le 1$ holds, where $T \in \binom{V}{t}$ and $\lambda_T^{(i)} = |\{B \in \mathcal{B}^{(i)} : B \supset T\}|$.*

Proof: For a t-tuple $T \in \mathcal{T}$, there are $\binom{v-t}{k-t}$ k-subsets containing T. Since $m = \binom{v-k}{k-t}$, $\lambda_T^{(i)} = 1$ must hold. Hence, we have $\lambda_T^{(i)} \le 1$ for any $T \in \binom{V}{t}$. □

It is obvious that a large set of t-designs with $\lambda = 1$ is an optimal t-SEED. Conversely, we can show the following:

Theorem 2.1.3. *If an optimal t-$(v,k;m)$ SEED exists, then it is an $LS_1(t,k,v)$.*

Proof: Take a nontrivial t-$(v,k;m)$ SEED $(V;\mathcal{B}^{(1)},\ldots,\mathcal{B}^{(m)})$. Assume that every design contains a t-tuple T, that is, $T \in \mathcal{T}$. Let $Y = V \setminus T$ and $\mathcal{B}^{(i)}(S) = \{B \in \mathcal{B}^{(i)} : B \cap T = S\}$ for any $S \subseteq T$.

We prove by induction that

$$\binom{T}{t-j} + \binom{Y}{j} \subset \mathcal{T} \tag{2.1.2}$$

and

$$|\mathcal{B}^{(i)}(S)| = \frac{\binom{v-k}{j}}{\binom{k-t+j}{j}} \tag{2.1.3}$$

hold for any $S \in \binom{T}{t-j}$ and $j = 0,1,\ldots,t$.

It is obvious that (2.1.2) holds for $j = 0$ since

$$\binom{T}{t} + \binom{Y}{0} = \{T\} \subset \mathcal{T}.$$

Since there are $m = \binom{v-t}{k-t}$ designs, every $(k-t)$-tuple of Y together with T must form a block of each design, which implies that $|\mathcal{B}^{(i)}(T)| = 1$ for any i. Hence the assertion is proved for $j = 0$.

Now, we assume that the assertion holds for any $j \leq \ell$. Then, by (2.1.3),

$$\sum_{i=1}^{m} |\mathcal{B}^{(i)}(S)| = \binom{v-t}{k-t} \frac{\binom{v-k}{\ell}}{\binom{k-t+\ell}{\ell}} = \binom{v-t}{k-t+\ell} = \left| \binom{Y}{k-t+\ell} \right|$$

holds for $S \in \binom{T}{t-\ell}$. By the fact that $\mathcal{B}^{(i)}(S)$'s are disjoint for any distinct i, it follows that

$$\bigcup_{i=1}^{m} \mathcal{B}^{(i)}(S) = S + \binom{Y}{k-t+\ell}$$

holds. Moreover, since $S \in \binom{T}{t-\ell}$ is chosen arbitrarily,

$$\bigcup_{S \in \binom{T}{t-\ell}} \bigcup_{i=1}^{m} \mathcal{B}^{(i)}(S) = \binom{T}{t-\ell} + \binom{Y}{k-t+\ell} \tag{2.1.4}$$

holds. Then, by (2.1.4), every t-tuple T' of V such that $|T' \cap Y| = \ell + 1$ must be in $\mathcal{T}$, that is,

$$\binom{T}{t-(\ell+1)} + \binom{Y}{\ell+1} \subset \mathcal{T}, \tag{2.1.5}$$

hence (2.1.2) holds for $j = \ell + 1$.

Now, we prove (2.1.3) for $j = \ell + 1$. Let

$$\chi_B(C) = \begin{cases} 1 & \text{if } C \subset B, \\ 0 & \text{otherwise,} \end{cases}$$

for $C \subset Y$ and $B \in \mathcal{B}^{(i)}$. For a fixed $(t-(\ell+1))$-subset $S \in \binom{T}{t-(\ell+1)}$, we count $\sum_{S \subset B \in \mathcal{B}^{(i)}} \sum_{C \in \binom{Y}{\ell+1}} \chi_B(C)$ in two ways. Firstly,

$$\sum_{C \in \binom{Y}{\ell+1}} \sum_{S \subset B \in \mathcal{B}^{(i)}} \chi_B(C) = \binom{v-t}{\ell+1} \tag{2.1.6}$$

holds since $C \cup S$ is in $\mathcal{T}$ for any $C \in \binom{Y}{\ell+1}$. Secondly, by noting that

$$\{B \in \mathcal{B}^{(i)} : B \supset S\} = \bigcup_{j=0}^{\ell+1} \bigcup_{S \subset S_j \in \binom{T}{t-j}} \mathcal{B}^{(i)}(S_j)$$

is a disjoint union, we obtain

$$\sum_{S \subset B \in \mathcal{B}^{(i)}} \sum_{C \in \binom{Y}{\ell+1}} \chi_B(C) = \sum_{j=0}^{\ell+1} \sum_{S \subset S_j \in \binom{T}{t-j}} \sum_{B \in \mathcal{B}^{(i)}(S_j)} \sum_{C \in \binom{Y}{\ell+1}} \chi_B(C). \tag{2.1.7}$$

Since there are $\binom{k-t+j}{\ell+1}$ $(\ell+1)$-subsets $C \subset Y \cap B$ for any $B \in \mathcal{B}^{(i)}(S_j)$, the right hand side of (2.1.7) can be computed as follows by the induction hypothesis (2.1.3) for $j \leq \ell$:

$$\begin{aligned}
\sum_{S \subset B \in \mathcal{B}^{(i)}} \sum_{C \in \binom{Y}{\ell+1}} \chi_B(C) &= \sum_{j=0}^{\ell+1} \sum_{S \subset S_j \in \binom{T}{j}} |\mathcal{B}^{(i)}(S_j)| \binom{k-t+j}{\ell+1} \\
&= |\mathcal{B}^{(i)}(S)| \binom{k-t+(\ell+1)}{\ell+1} + \sum_{j=0}^{\ell} \sum_{S \subset S_j \in \binom{T}{j}} \frac{\binom{v-k}{j}}{\binom{k-t+j}{j}} \binom{k-t+j}{\ell+1} \\
&= |\mathcal{B}^{(i)}(S)| \binom{k-t+(\ell+1)}{\ell+1} + \sum_{j=0}^{\ell} \binom{\ell+1}{j} \frac{\binom{v-k}{j}}{\binom{k-t+j}{j}} \binom{k-t+j}{\ell+1} \\
&= |\mathcal{B}^{(i)}(S)| \binom{k-t+(\ell+1)}{\ell+1} + \sum_{j=0}^{\ell} \binom{v-k}{j} \binom{k-t}{(\ell+1)-j} \\
&= |\mathcal{B}^{(i)}(S)| \binom{k-t+(\ell+1)}{\ell+1} + \binom{v-t}{\ell+1} - \binom{v-k}{\ell+1}.
\end{aligned}$$

From equation (2.1.6), we obtain

$$|\mathcal{B}^{(i)}(S)| = \frac{\binom{v-k}{\ell+1}}{\binom{k-t+(\ell+1)}{\ell+1}}.$$

Hence (2.1.2) and (2.1.3) hold for any $j = 0, 1, \ldots, t$.

Thus, by (2.1.2), every t-tuple of V is included exactly once in a block of each design. This means that an optimal t-$(v, k; m)$ SEED must be an $LS_1(t, k, v)$. □

Remark: Note that the right hand side of (2.1.3) must be an integer for any $\ell = 0, 1, \ldots, t$. Hence,

$$(v-k)_j \equiv 0 \pmod{(k-t+j)_j} \tag{2.1.8}$$

holds for $j = 1, \ldots, t$, where $(x)_n = x(x-1)\cdots(x-n+1)$ is a falling factorial. We can show that this is equivalent to the assertion that

$$(v-t+j)_j \equiv 0 \pmod{(k-t+j)_j} \tag{2.1.9}$$

holds for $j = 1, \ldots, t$, which is a well-known necessary condition for the existence of t-designs. In fact, it is true for $j = 1$. Assume that the assertion is true for $j < \ell$. Then, by letting $x = v-k$, $y = k-t+\ell$, and $n = \ell$ in the binomial identity $(x+y)_n = \sum_{i=0}^{n} \binom{n}{i}(x)_i(y)_{n-i}$, we obtain

$$(v-t+\ell)_\ell - (v-k)_\ell = \sum_{j=0}^{\ell-1} \binom{\ell}{j} (v-k)_j (k-t+\ell)_{\ell-j}. \tag{2.1.10}$$

By noting $(k-t+\ell)_\ell = (k-t+\ell)_{\ell-j}(k-t+j)_j$ and (2.1.8), we have

$$(v-k)_j(k-t+\ell)_{\ell-j} \equiv 0 \pmod{(k-t+\ell)_\ell}$$

for $j \leq \ell-1$ by the induction hypothesis. According to (2.1.10), $(v-t+\ell)_\ell - (v-k)_\ell \equiv 0 \pmod{(k-t+\ell)_\ell}$ holds. Hence $(v-t+\ell)_\ell \equiv 0 \pmod{(k-t+\ell)_\ell}$ holds if and only if $(v-k)_\ell \equiv 0 \pmod{(k-t+\ell)_\ell}$, that is, (2.1.8) and (2.1.9) are equivalent.

Corollary 2.1.4. *An optimal t-$(v, k; m)$ SEED exists if and only if an $LS_1(t, k, v)$ exists.*

It is remarkable that in the extremal case attaining the upper bound (2.1.1), a t-SEED must be a large set of t-designs with $\lambda = 1$. The existence of large sets with $\lambda = 1$ has not been shown except for infinite series of Steiner triple systems and some sporadic examples, as was stated in Section 1.1.

Lemma 2.1.5. *For a t-$(v, k; m)$ SEED with $\emptyset \neq \mathcal{T} \subsetneq \binom{V}{t}$, there exist t-tuples $T_1 \in \mathcal{T}$ and $T_2 \notin \mathcal{T}$ such that $|T_1 \cap T_2| = t-1$.*

Proof: It is obvious that there are t-subsets $T \in \mathcal{T}$ and $T' \in \mathcal{T}$. Consider a sequence of t-subsets $T_0 = T, T_1, \ldots, T_n = T'$ such that $|T_i \cap T_{i+1}| = t-1$. Let i be the smallest integer such that $T_i \notin \mathcal{T}$. Then T_{i-1} and T_i are the desired t-tuples. □

Theorem 2.1.6. *For a t-$(v,k;m)$ SEED with $\emptyset \neq \mathcal{T} \subsetneq \binom{V}{t}$,*

$$m \leq \binom{v-t-1}{k-t}$$

holds. Moreover, if $v-k-1$ is not divisible by $k-t+1$, then we have

$$m < \binom{v-t-1}{k-t}.$$

Proof: By Lemma 2.1.5, there are t-tuples $T_1 \in \mathcal{T}$ and $T_2 \notin \mathcal{T}$ such that $|T_1 \cap T_2| = t-1$. Let

$$\mathcal{B}_{T_1}^{T_2} = \left\{ B \in \binom{V}{k} : B \supset T_1, B \not\supset T_2 \right\}.$$

Then, $|\mathcal{B}_{T_1}^{T_2}| = \binom{v-t-1}{k-t}$ holds, which implies $m \leq \binom{v-t-1}{k-t}$.

Now, assume that $m = \binom{v-t-1}{k-t}$. Then, each k-subset in $\mathcal{B}_{T_1}^{T_2}$ must be contained in a design of the t-SEED as a block. Hence $\mathcal{T}$ includes the t-tuples in $\mathcal{T}_{T_1}^{T_2} = \{T \in \binom{V}{t} : T \subset B \in \mathcal{B}_{T_1}^{T_2}\}$. We look at t-tuples containing $T_1 \cap T_2$. There are $v-t-1$ such t-tuples in $\mathcal{T}_{T_1}^{T_2}$, apart from T_1. These t-tuples must be included in blocks of every design. In a design $\mathcal{B}^{(i)}$, there is a single block B_0 containing T_1. B_0 contains $k-t$ t-tuples containing $T_1 \cap T_2$, apart from T_1. Hence the remaining $v-k-1$ t-tuples must be included in blocks in $\mathcal{B}^{(i)}$. Since a block $B(\neq B_0)$ containing $T_1 \cap T_2$ contains $k-t+1$ such t-tuples, we need $\lceil \frac{v-k-1}{k-t+1} \rceil$ such blocks in a design, where $\lceil x \rceil$ is the minimum integer not smaller than x. Since there are $\binom{v-t-1}{k-t+1}$ k-subsets including $T_1 \cap T_2$, apart from T_1 and T_2, hence the mean value of the number of such blocks in a design is

$$\frac{\binom{v-t-1}{k-t+1}}{m} = \frac{v-k-1}{k-t+1}.$$

Hence, unless

$$\left\lceil \frac{v-k-1}{k-t+1} \right\rceil = \frac{v-k-1}{k-t+1}$$

holds, the number of designs must be less than $m = \binom{v-t-1}{k-t}$, which proves the theorem. □

Corollary 2.1.7. *A 2-$(7,3;m)$ SEED does not exist for $m \geq 4$.*

Proof: By the upper bound (2.1.1), we have $m \leq 5$. In the case when $\mu_T > 0$ for any pair (2-subset) T, if $m \geq 4$, there are two possibilities for the value of $\lambda_T^{(i)}$: (i) $\lambda_T^{(i)} = 1$ for any T and i; in this case $m = 5$, (ii) $\lambda_T^{(i)} = 2$ for some i and $\lambda_T^{(j)} = 1$ for j other than i; in this case $m = 4$. In both cases, each design must be a 2-design with $\lambda = 1$, or 2. However, it is known that there does not exist an $LS_1(2, 3, 7)$ and the maximum number of disjoint 2-designs is three, which are two 2-$(7, 3, 1)$ designs and a 2-$(7, 3, 3)$ design ([11]). Hence, in the case when $\mu_T > 0$ for any T, we have $m \leq 3$.

If there is some T such that $\mu_T = 0$, then $\lambda_T^{(i)} = 0$ for any i. In this case, by Theorem 2.1.6, $m \leq 3$. Thus the corollary is proved. □

Example 2.1.8. A 2-$(7, 3; 3)$ SEED exists. We give an example of a 2-$(7, 3; 3)$ SEED as follows:

$$\begin{aligned}
\mathcal{B}^{(1)} =& \{013, 124, 235, 346, 045, 156, 026\},\\
\mathcal{B}^{(2)} =& \{023, 134, 245, 356, 046, 015, 126\},\\
\mathcal{B}^{(3)} =& \{024, 135, 246, 035, 146, 025, 136, 012, 123, 234,\\
& 345, 456, 056, 016, 014, 125, 236, 034, 145, 256, 036\}.
\end{aligned}$$

Note that $\mathcal{B}^{(1)}$ and $\mathcal{B}^{(2)}$ are 2-$(7, 3, 1)$ designs, and $\mathcal{B}^{(3)}$ is a 2-$(7, 3, 3)$ design.

2.2 Recursive constructions

In this section, we give some recursive constructions. To describe the constructions, we need the following combinatorial designs.

A *group divisible design* (or t-GDD) of order v, block size k, denoted by t-$GDD(k, v)$, is a triple $(V, \mathcal{G}, \mathcal{B})$, where (i) V is a set of v points; (ii) $\mathcal{G} = \{G_1, G_2, \ldots\}$ is a partition of V into subsets called *groups*; (iii) $\mathcal{B}$ is a collection of k-subsets (blocks) of V such that each block and each group contain at most one common point; (iv) every t-set of points from t distinct groups is contained in exactly one block. A 2-GDD is simply written as a GDD. The *type* of the groups of a t-GDD is defined as a multi-set $\{|G_i| : G_i \in \mathcal{G}\}$. For example, if $|G_i| = n$ for any i and $v = gn$, the type is represented by n^g.

Let $v = kn$. A *transversal design* is a t-$GDD(k, v)$ of type n^k, denoted by $TD(t, k, n)$. Note that in a $TD(t, k, n)$, the size of each group is the same,

any group and any block contain exactly one common point, and every t-set of points from distinct groups is contained in exactly one block. There are n^t blocks in a $TD(t, k, n)$.

It is well-known that a transversal design is equivalent to an *orthogonal array* with $\lambda = 1$. A $k \times \lambda q^t$ array consisting of q symbols is called an orthogonal array $OA_\lambda(t, k, q)$ if every one of the possible q^t ordered t-tuples of symbols occurs in exactly λ columns in any t rows of the array. Note that an orthogonal array is usually defined as a $\lambda q^t \times k$ array. Here we use the transposed representation. It is easier to treat columns of an OA as groups of a GDD when we construct a t-SEED by an OA. When $\lambda = 1$, we write an $OA_1(t, k, q)$ as an $OA(t, k, q)$. A *large set* of orthogonal arrays $LOA_\lambda(t, k, q)$ is a collection $\{A^{(r)}\}_{r\in R}$ of $OA_\lambda(t, k, q)$s such that each possible k-tuple of symbols occurs in exactly one of the OAs in the collection. When $\lambda = 1$, we write an $LOA_1(t, k, q)$ as an $LOA(t, k, q)$. Note that $|R| = q^{k-t}$. It is well-known (see, for example, Raghavarao [64]) that for any prime power q, there exists an $LOA(t, k, q)$ for $k \leq q + 1$.

Moreover, let $[q] = \{0, 1, 2, \ldots, q-1\}$ and $[q]^k$ be the direct product of $[q]$. In this thesis, an orthogonal array $A = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{\lambda q^t})$ is often identified with the set of column vectors $\mathcal{A} = \{\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{\lambda q^t}\}$. An $LOA(t, k, q)$ contains all ordered k-tuples of a q-set $[q]$ and partitions these k-tuples into q^{k-t} OAs, and any t-tuple of $[q]$ occurs exactly once in any t rows of each OA. That is, for $u \leq t$, any u-tuple of $[q]$ occurs exactly q^{t-u} times in each OA.

2.2.1 Recursive constructions by direct product and LOAs

The first construction is based on a direct product of two t-SEEDs.

Theorem 2.2.1. *(Direct product construction) If there exist a t-$(v, k; m)$ SEED and a t-$(v', k'; m')$ SEED, then there exists a t-$(vv', kk'; mm')$ SEED.*

Proof: Let $(V_1; \mathcal{A}^{(1)}, \ldots, \mathcal{A}^{(m)})$ and $(V_2; \mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m')})$ be a t-$(v, k; m)$ SEED and a t-$(v', k'; m')$ SEED, respectively. We define $V = V_1 \times V_2 = \{(a, b) : a \in V_1, b \in V_2\}$ and $\mathcal{A}^{(i)} \times \mathcal{B}^{(j)} = \{A \times B : A \in \mathcal{A}^{(i)}, B \in \mathcal{B}^{(j)}\}$ where $A \times B = \{(a, b) : a \in A, b \in B\}$ for any $A \in \mathcal{A}^{(i)}$ and $B \in \mathcal{B}^{(j)}$. Thus, for every block $A \times B \in \mathcal{A}^{(i)} \times \mathcal{B}^{(j)}$, the new block size $|A \times B|$ is kk'.

For two blocks $A\times B$ and $A'\times B'$ in $\mathcal{A}^{(i)}\times\mathcal{B}^{(j)}$, $A\times B = A'\times B'$ implies $A = A'$ and $B = B'$. Thus all blocks in $\mathcal{A}^{(i)} \times \mathcal{B}^{(j)}$ are distinct. Since $\mathcal{A}^{(i)} \cap \mathcal{A}^{(i')} = \emptyset$

for any $i \neq i'$ and $\mathcal{B}^{(j)} \cap \mathcal{B}^{(j')} = \emptyset$ for any $j \neq j'$, $\mathcal{A}^{(i)} \times \mathcal{B}^{(j)}$ and $\mathcal{A}^{(i')} \times \mathcal{B}^{(j')}$ are disjoint. That is, for any $(i,j) \neq (i',j')$, $(\mathcal{A}^{(i)} \times \mathcal{B}^{(j)}) \cap (\mathcal{A}^{(i')} \times \mathcal{B}^{(j')}) = \emptyset$ holds.

For any $u \leq t$, choose a u-tuple $T = \{(a_1, b_1), (a_2, b_2), \ldots, (a_u, b_u)\} \in V$. Let $T_1 = \{a_1, \ldots, a_u\}$ and $T_2 = \{b_1, \ldots, b_u\}$. Then there are $\mu_{T_1}|\mathcal{A}^{(i)}|$ block A's in $\mathcal{A}^{(i)}$ containing T_1. Similarly, there are $\mu_{T_2}|\mathcal{B}^{(j)}|$ block B's in $\mathcal{B}^{(j)}$ containing T_2. That is, T occurs $\mu_{T_1}\mu_{T_2}|\mathcal{A}^{(i)}||\mathcal{B}^{(j)}|$ times for any i and j. Hence $(V; \mathcal{A}^{(i)} \times \mathcal{B}^{(j)})$ for $i = 1, \ldots, m; j = 1, \ldots, m'$ is a t-$(vv', kk'; mm')$ SEED. □

In Section 2.1, we mentioned that a large set of t-designs can be viewed as a t-SEED. There are several results about the existence of large sets of t-designs. Applying Theorem 2.2.1 to these large sets, we obtain many series of t-SEEDs.

Corollary 2.2.2. *If there exist an $LS_{\lambda_1}(t,k,v)$ and an $LS_{\lambda_2}(t,k',v')$, then there exists a t-$(vv', kk'; m)$ SEED, where $m = \frac{\binom{v-t}{k-t}\binom{v'-t}{k'-t}}{\lambda_1\lambda_2}$.*

Proof: Since a large set $LS_\lambda(t,k,v)$ is a t-$\left(v, k; \binom{v-t}{k-t}/\lambda\right)$ SEED, we have a t-$\left(v, k; \binom{v-t}{k-t}/\lambda_1\right)$ SEED and a t-$\left(v', k'; \binom{v'-t}{k'-t}/\lambda_2\right)$ SEED. Thus, by Theorem 2.2.1, a t-$(vv', kk'; mm')$ SEED is obtained. □

An $LS_1(t,k,v)$ attains the upper bound of Theorem 2.1.1. Unfortunately, the upper bound of Theorem 2.1.1 is not attained by applying the recursive construction method to large sets of t-designs. For example, constructing $LS_1(t,k,v)$ and $LS_1(t,k',v')$ by Corollary 2.2.2, we have a t-$\left(vv', kk'; \binom{v-t}{k-t}\binom{v'-t}{k'-t}\right)$ SEED. If an $LS_1(t, kk', vv')$ exists then a t-$\left(vv', kk'; \binom{vv'-t}{kk'-t}\right)$ SEED exists. The number $\binom{vv'-t}{kk'-t}$ is always larger than $\binom{v-t}{k-t}\binom{v'-t}{k'-t}$.

Example 2.2.3. It is known that an $LS_1(2,3,v)$ exists for $v \equiv 1$ or $3 \pmod 6$ except for $v = 7$. Also, an $LS_1(2,4,13)$ exists. These large sets correspond to a 2-$(v, 3; v-2)$ SEED and a 2-$(13, 4; 55)$ SEED, respectively. Hence, by Theorem 2.2.1, we get a 2-$(13v, 12; 55v-110)$ SEED for $v \equiv 1$ or $3 \pmod 6$ and $v \neq 7$.

An $LOA(t,k,q)$ also can be used to construct a t-SEED. Jimbo and Shiromoto [38] gave constructions of t-SEEDs by utilizing LOAs in the following lemma and theorem, without giving proofs. For the reader's convenience, we provide the proofs here.

Lemma 2.2.4 ([38]). *If there exists an $LOA(t,k,q)$, then there exists a t-$(kq,k;q^{k-t})$ SEED. In particular, if q is a prime power, then a t-$(q(q+1),q+1;q^{k-t})$ SEED exists.*

Proof: Let $\{A^{(r)}=(a_{ij}^{(r)}) : 1 \le r \le q^{k-t}\}$ be an $LOA(t,k,q)$ with elements in $[q]$. Now let $V=[q]\times[k]$. Each orthogonal array $A^{(r)}$ is a $TD(t,k,q)$ $(V,\mathcal{G},\mathcal{B}^{(r)})$, where

$$\mathcal{G}=\big\{[q]\times\{0\},[q]\times\{1\},\ldots,[q]\times\{k-1\}\big\},$$

and

$$\mathcal{B}^{(r)}=\big\{\{(a_{1j}^{(r)},0),(a_{2j}^{(r)},1),\ldots,(a_{kj}^{(r)},k-1)\} : j=1,2,\ldots,q^t\big\}.$$

Since there are no two columns which are identical in any $A^{(r)}$ and $A^{(r')}$, $\mathcal{B}^{(r)}$ and $\mathcal{B}^{(r')}$ are disjoint for any $r\neq r'$. By the properties of transversal designs, any t-tuple from t distinct groups is contained in exactly one block. Hence, in any design $\mathcal{B}^{(r)}$, any u-tuple T of V $(u\le t)$ is contained in exactly q^{t-u} blocks. Thus $(V;\mathcal{B}^{(1)},\ldots,\mathcal{B}^{(q^{k-t})})$ forms a t-$(kq,k;q^{k-t})$ SEED. □

Remark: Beth et al. [6] proved the existence of a t-$(q^2,q;q^{q-t})$ SEED for any prime power q, which is a special case of Lemma 2.2.4, shown by letting $k=q$.

Theorem 2.2.5 ([38]). *(LOA construction) If there exist an $LOA(t,k,q)$ and a t-$(v,k;m)$ SEED, then there exists a t-$(qv,k;mq^{k-t})$ SEED.*

Proof: Let $\{A^{(r)}=(a_{ij}^{(r)}) : 1\le r\le q^{k-t}\}$ be an $LOA(t,k,q)$ with elements in $[q]$ and $\mathcal{A}^{(r)}$ be the set of column vectors in an OA $A^{(r)}$. Let $(V_1;\mathcal{B}^{(1)},\ldots,\mathcal{B}^{(m)})$ be a t-$(v,k;m)$ SEED. For a block $B=\{b_1,\ b_2,\ \ldots,\ b_k\}$ $\in\mathcal{B}^{(i)}$, we identify B with an ordered k-tuple $(b_1,\ldots,b_k)$. Define $V=V_1\times[q]$ and $B_{\mathbf{a}}=\{(b_1,a_1),(b_2,a_2),\ldots,(b_k,a_k)\}$ for a block $B\in\mathcal{B}^{(i)}$ and a column $\mathbf{a}\in\mathcal{A}^{(r)}$. Let

$$\mathcal{B}^{(i)}_{\mathcal{A}^{(r)}}=\{B_{\mathbf{a}} : B\in\mathcal{B}^{(i)},\mathbf{a}\in\mathcal{A}^{(r)}\}$$

be a design on V.

There are no common blocks in $\mathcal{B}^{(i)}$ and $\mathcal{B}^{(i')}$ for $i\neq i'$, and no identical columns in $\mathcal{A}^{(r)}$ and $\mathcal{A}^{(r')}$ for $r\neq r'$, so $\mathcal{B}^{(i)}_{\mathcal{A}^{(r)}}$ and $\mathcal{B}^{(i')}_{\mathcal{A}^{(r')}}$ are disjoint for $(i,r)\neq(i',r')$.

For any $u\le t$, choose a u-tuple $T=\{(d_1,c_1),(d_2,c_2),\ldots,(d_u,c_u)\}\subset V$. Let $T_D=\{d_1,d_2,\ldots,d_u\}$. Then there are $\mu_{T_D}|\mathcal{B}^{(i)}|$ blocks in $\mathcal{B}^{(i)}$ satisfying

$b_{i_1} = d_1$, $b_{i_2} = d_2$, ..., $b_{i_u} = d_u$, and there exist q^{t-u} $\mathbf{a}$'s in $\mathcal{A}^{(r)}$ such that $a_{i1} = c_1$, $a_{i2} = c_2$, ..., $a_{iu} = c_u$. Hence, for any $1 \le i \le m$ and $1 \le r \le q^{k-t}$, we get

$$\begin{aligned}
&\frac{|\{B_{\mathbf{a}} \in \mathcal{B}^{(i)}_{\mathcal{A}^{(r)}} : T \subset B_{\mathbf{a}}\}|}{|\mathcal{B}^{(i)}_{\mathcal{A}^{(r)}}|} \\
&= \frac{|\{B \in \mathcal{B}^{(i)} : T_D \subset B\}|}{|\mathcal{B}^{(i)}|} \frac{|\{\mathbf{a} \in \mathcal{A}^{(r)} : a_{i1} = c_1, \ldots, a_{iu} = c_u\}|}{|\mathcal{A}^{(r)}|} \\
&= \mu_{T_D} \frac{q^{t-u}}{q^t} = \mu_{T_D} q^{-u},
\end{aligned}$$

which does not depend on i and r. Thus $(V; \mathcal{B}^{(1)}_{\mathcal{A}^{(1)}}, \ldots, \mathcal{B}^{(m)}_{\mathcal{A}^{(q^{k-t})}})$ forms a t-$(qv, k; mq^{k-t})$ SEED. □

Corollary 2.2.6 ([38]). *For any prime power q, there exists a t-$(q^n(q+1), q+1; q^{n(q+1-t)})$ SEED.*

Proof: When q is a prime power, an $LOA(t, q+1, q)$ exists. By Lemma 2.2.4, we obtain a t-$(q^n(q+1), q+1; q^{n(q+1-t)})$ SEED. □

Example 2.2.7. A 2-$(6, 3; 2)$ SEED $(V; \mathcal{B}^{(1)}, \mathcal{B}^{(2)})$ is presented in Example 1.2.1. We give an example of $LOA(2, 3, 2)$ as follows: Then we can construct

$$\left(\begin{array}{cccc|cccc}
0 & 1 & 1 & 0 & 1 & 0 & 0 & 1 \\
0 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 1 & 0 & 1 & 1 & 0 & 1 & 0
\end{array}\right)$$

a 2-$(12, 3; 4)$ SEED for $qv = 2{\cdot}6 = 12$, $k = 3$ and $mq^{k-t} = 2{\cdot}2^{3-2} = 4$, by Theorem 2.2.5.

Let $V = \mathbb{Z}_6 \times \mathbb{Z}_2 = \{(0,0), (1,0), (2,0), (3,0), (4,0), (5,0), (0,1), (1,1), (2,1), (3,1), (4,1), (5,1)\}$. Define a new block $B_{\mathbf{a}} = \{(b_1, a_1), (b_2, a_2), \ldots, (b_k, a_k)\}$ for a block $B = \{b_1, b_2, \ldots, b_k\}$ in $\mathcal{B}^{(i)}$ and a column $\mathbf{a} = (a_1, a_2, \ldots, a_k)$ of $A^{(r)}$. For example, take $B = \{0, 1, 2\}$ and $\mathbf{a} = (0, 0, 0)$, then the new block is $B_{\mathbf{a}} = \{(0,0), (1,0), (2,0)\}$. Let the expression $\{00, 10, 20\}$ stand for $\{(0,0), (1,0), (2,0)\}$. Combining $\mathcal{B}^{(1)}$ and $A^{(1)}$, the new design $\mathcal{B}^{(1)}_{\mathcal{A}^{(1)}}$ contains the following blocks:

$$\{00,10,20\},\{01,10,21\},\{01,11,20\},\{00,11,21\},$$
$$\{00,20,30\},\{01,20,31\},\{01,21,30\},\{00,21,31\},$$
$$\{00,30,40\},\{01,30,41\},\{01,31,40\},\{00,31,41\},$$
$$\{00,40,50\},\{01,40,51\},\{01,41,50\},\{00,41,51\},$$
$$\{00,10,50\},\{01,10,51\},\{01,11,50\},\{00,11,51\},$$
$$\{10,30,50\},\{11,30,51\},\{11,31,50\},\{10,31,51\},$$
$$\{10,20,40\},\{11,20,41\},\{11,21,40\},\{10,21,41\},$$
$$\{20,30,50\},\{21,30,51\},\{21,31,50\},\{20,31,51\},$$
$$\{10,30,40\},\{11,30,41\},\{11,31,40\},\{10,31,41\},$$
$$\{20,40,50\},\{21,40,51\},\{21,41,50\},\{20,41,51\}.$$

The other blocks are obtained similarly.

2.2.2 Recursive constructions based on s-resolvability

A t-$(v,k;m)$ SEED $(V;\mathcal{B}^{(1)},\ldots,\mathcal{B}^{(m)})$ is said to be *s-resolvable* if each design $\mathcal{B}^{(i)}$ is partitioned into h sub-designs $\mathcal{B}^{(i,1)},\mathcal{B}^{(i,2)}$, …, $\mathcal{B}^{(i,h)}$ and a $(V;\mathcal{B}^{(1,1)}$, $\mathcal{B}^{(1,2)}$, …, $\mathcal{B}^{(m,h)})$ forms an s-$(v,k;mh)$ SEED. A t-SEED $(V;\mathcal{B}^{(1)},\ldots,\mathcal{B}^{(m)})$ is said to be *equi-partitioned* if $|\mathcal{B}^{(1)}|=|\mathcal{B}^{(2)}|=\cdots=|\mathcal{B}^{(m)}|$ holds. An equi-partitioned t-SEED is denoted by a t^*-SEED. Moreover, an s-resolvable t^*-SEED $(V;\mathcal{B}^{(1,1)}$, $\mathcal{B}^{(1,2)}$, …, $\mathcal{B}^{(m,h)})$ is called s^*-resolvable if every family $\mathcal{B}^{(i)}$ is partitioned into the same number $(=h)$ of $\mathcal{B}^{(i,j)}$'s with $|\mathcal{B}^{(i,1)}|=\cdots=|\mathcal{B}^{(i,h)}|$.

Jimbo and Shiromoto [38] gave a specific construction with $k'=2$ as a corollary of Theorem 2.2.8. We generalize the construction for any k'.

Theorem 2.2.8. *If there exist a $\lfloor\frac{t}{2}\rfloor$*-resolvable t*-$(v,k;m)$ SEED and a t*-$(n,k';m')$ SEED, then there exists a $\lfloor\frac{t}{2}\rfloor$*-resolvable t*-$(nv,kk';h^{k'-1}m^{k'}m')$ SEED for any n, $k'\geq 2$, where h is the number of subfamilies $\mathcal{B}^{(i,j)}$ in $\mathcal{B}^{(i)}$.*

Proof: Let $(V_1;\mathcal{B}^{(1)},\ldots,\mathcal{B}^{(m)})$ be a $\lfloor\frac{t}{2}\rfloor$*-resolvable t^*-$(v,k;m)$ SEED with parameter $\{\bar{\mu}_T:|T|\leq t\}$, and $(V_1;\mathcal{B}^{(1,1)},\mathcal{B}^{(1,2)},\ldots,\mathcal{B}^{(m,h)})$ be a $\lfloor\frac{t}{2}\rfloor^*$-$(v,k;mh)$ SEED with parameter $\{\mu_T:|T|\leq\lfloor\frac{t}{2}\rfloor\}$, such that $\mathcal{B}^{(i)}=\bigcup_{j=1}^{h}\mathcal{B}^{(i,j)}$. Let $(V';\mathcal{X}^{(1)},\ldots,\mathcal{X}^{(m')})$ be a t^*-$(n,k';m')$ SEED with parameter $\{\mu'_Y:|Y|\leq t\}$. Now let $V=V_1\times V'$ be a point set. For any $B_i=\{b_{i1},\ldots,b_{ik}\}\in\binom{V_1}{k}$ $(i=1,\ldots,k')$ and $X=\{x_1,x_2,\ldots,x_{k'}\}\in\binom{V'}{k'}$, we define the set addition $\oplus$ as follows:

$$\oplus\big(B_1,\ldots,B_{k'};X\big)=\big\{(b_{ij},x_i):i=1,\ldots,k';j=1,\ldots,k\big\}.$$

Using this notation, we define

$$\begin{aligned}&\oplus\left(\mathcal{B}^{(p_1,l_1)},\mathcal{B}^{(p_2,l_2)},\ldots,\mathcal{B}^{(p_{k'},l_{k'})};X\right)\\=&\bigcup_{i=1}^{k'}\bigcup_{B^{(p_i,l_i)}\in\mathcal{B}^{(p_i,l_i)}}\oplus\left(B^{(p_1,l_1)},B^{(p_2,l_2)},\ldots,B^{(p_{k'},l_{k'})};X\right)\end{aligned}\tag{2.2.1}$$

for $X\in\mathcal{X}^{(s)}$. Let

$$\begin{aligned}\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s)}=&\bigcup_{l=1}^{h}\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s,l)}\\=&\bigcup_{l=1}^{h}\bigcup_{X\in\mathcal{X}^{(s)}}\oplus\left(\mathcal{B}^{(p_1,l)},\mathcal{B}^{(p_2,l+\Delta_2)},\ldots,\mathcal{B}^{(p_{k'},l+\Delta_{k'})};X\right)\end{aligned}$$

be a design on V, where $\mathbf{p}=(p_1,\ldots,p_{k'})\in[m]^{k'}$, $\mathbf{\Delta}=(\Delta_2,\ldots,\Delta_{k'})\in[h]^{k'-1}$ and $l+\mathbf{\Delta}=(l,l+\Delta_2,\ldots,l+\Delta_{k'})\pmod h$. Then the collection of designs

$$\left\{\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s)}:\mathbf{p}\in[m]^{k'},\mathbf{\Delta}\in[h]^{k'-1},s=1,2,\ldots,m'\right\}$$

forms a t^*-$(nv,kk';h^{k'-1}m^{k'}m')$ SEED.

It is clear that the new designs $\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s)}$ and $\mathcal{C}^{(\mathbf{p}',\mathbf{\Delta}',s')}$ are disjoint since the designs $\mathcal{B}^{(p,l)}$ and $\mathcal{B}^{(p',l')}$ are disjoint for $(p,l)\neq(p',l')$, and $\mathcal{X}^{(s)}$ and $\mathcal{X}^{(s')}$ are also disjoint.

For any $u\le t$, choose a u-tuple $T\subset V$, and let $T_i=T\cap G_i$ for any group $G_i=V_1\times\{i\}$. Assume that there are $u_i=|T_i|=|T\cap G_i|$ points in each group G_i, then $u=u_1+\cdots+u_n$. Let $Y=\{i:T_i\neq\emptyset\}$. We consider the number of occurrences of T in three cases.

Case 1 $|Y|>k'$: Since any block in $\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s)}$ is defined by choosing k points from each of k' groups $G_{x_1},\ldots,G_{x_{k'}}$, where $X=\{x_1,\ldots,x_{k'}\}\in\mathcal{X}^{(s)}$, the u-tuple T does not occur in $\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s)}$. That is, the number of occurrences of T is zero.

Case 2 $|Y|=k'$: By the definition of addition $\oplus$, $\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s,l)}$ is constructed for all possible $X\in\mathcal{X}^{(s)}$. Without loss of generality, we assume $u_1,\ldots,u_{k'}>0$ and $u_{k'+1}=u_{k'+2}=\cdots=u_n=0$. Then $u=u_1+u_2+\cdots+u_{k'}$. If $u_i\le\lfloor\frac{t}{2}\rfloor$, then T_i occurs $\mu_{T_i}\cdot q$ times in each $\mathcal{B}^{(p,l)}$, where $|\mathcal{B}^{(p,l)}|=q$. If $u_i>\lfloor\frac{t}{2}\rfloor$, then T_i occurs $\bar{\mu}_{T_i}\cdot hq$ times in each $\mathcal{B}^{(p)}$. Thus, the number of occurrences of T can be computed as the following two sub-cases.

Case 2.1 $u_i\le\lfloor\frac{t}{2}\rfloor$ for all i : In this case, by noting that Y occurs $\mu'_Y\cdot|\mathcal{X}^{(s)}|=\mu'_Y\cdot q'$ times in each of $\mathcal{X}^{(s)}$, T occurs

$$\tilde{\mu}_T=\mu_{T_1}q\cdot\mu_{T_2}q\cdots\mu_{T_{k'}}q\cdot\mu'_Y\cdot q'$$

times in $\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s,l)}$. Moreover, T occurs

$$\begin{aligned}\tilde{\mu}_T &= \sum_{l=1}^{h} \mu_{T_1} q \cdot \mu_{T_2} q \cdots \mu_{T_{k'}} q \cdot \mu'_Y q' \\ &= \mu_{T_1}\mu_{T_2}\cdots\mu_{T_{k'}} \cdot h \cdot q^{k'} \cdot \mu'_Y q'\end{aligned}$$

times in $\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s)}$.

Case 2.2 One of $u_1, u_2, \ldots, u_{k'}$ is larger than $\lfloor \frac{t}{2} \rfloor$: Without loss of generality, we assume that $u_1 > \lfloor \frac{t}{2} \rfloor$, then T_1 occurs $\bar{\mu}_{T_1} \cdot hq$ times in each $\mathcal{B}^{(p)}$. Hence T occurs

$$\begin{aligned}\tilde{\mu}_T &= \bar{\mu}_{T_1} hq \cdot \mu_{T_2} q \cdots \mu_{T_{k'}} q \cdot \mu'_Y q' \\ &= \bar{\mu}_{T_1}\mu_{T_2}\cdots\mu_{T_{k'}} \cdot h \cdot q^{k'} \cdot \mu'_Y q'\end{aligned}$$

times in $\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s)}$.

Case 3 $|Y| < k'$: The proof is similar to Case 2. The number of occurrences of T is obtained by multiplying $q^{k'-|Y|}$ with each result in Case 2.

Hence, we get a t*-$(nv, kk'; h^{k'-1}m^{k'}m')$ SEED. Moreover, it is shown that the constructed t*-SEED is $\lfloor \frac{t}{2} \rfloor$*-resolvable by a similar argument to Case 2.1. In fact, for any u-tuple $T \subset V$ $(u \leq \lfloor \frac{t}{2} \rfloor)$,

$$u_i = |T_i| = |T \cap G_i| \leq \lfloor \frac{t}{2} \rfloor$$

holds and T_i occurs $\mu_{T_i}|\mathcal{B}^{(p,l)}|$ times in $\mathcal{B}^{(p,l)}$, as stated in Case 2.1. Hence T occurs

$$\mu_{T_1}\mu_{T_2}\cdots\mu_{T_{k'}} q^{k'} \mu'_Y q'$$

times in $\mathcal{C}^{(\mathbf{p},\mathbf{\Delta},s,l)}$. Thus the theorem is proved. □

We will give an example of Theorem 2.2.8. For even v, let K_v be the complete graph of order v. A 1-factorization can be seen as a 1*-resolvable 3*-$(v, 2; 1)$ SEED with $h = v - 1$. Hence we obtain the following corollary by letting $k = k' = 2$.

Corollary 2.2.9. *For any even integer v and any integer $n \geq 2$, there exists a 3*-$(nv, 4; v - 1)$ SEED.*

Example 2.2.10. In Table 2.2.1, a 1-factorization of K_4 is presented. A column of Table 2.2.1 corresponds to an edge. Any two columns partitioned by vertical lines correspond to 1-factors. Utilizing Theorem 2.2.8, we find a 3*-$(8, 4; 3)$ SEED in Table 2.2.2.

In Table 2.2.2, each column corresponds to a block. Let $V = [4] \times [2]$. Then a column ${}^t(a, b \mid c, d)$ implies a block $\{(a, 0), (b, 0), (c, 1), (d, 1)\}$.

Table 2.2.1: A 1-factorization of K_4

0	2	0	1	0	1
1	3	2	3	3	2

Table 2.2.2: A 3*-$(8, 4; 3)$ SEED for $v = 4$, $n = 2$, $m = 1$ and $h = 3$

$\mathcal{B}^{(1)}$

0	0	2	2	0	0	1	1	0	0	1	1
1	1	3	3	2	2	3	3	3	3	2	2
0	2	0	2	0	1	0	1	0	1	0	1
1	3	1	3	2	3	2	3	3	2	3	2

$\mathcal{B}^{(2)}$

0	0	2	2	0	0	1	1	0	0	1	1
1	1	3	3	2	2	3	3	3	3	2	2
0	1	0	1	0	1	0	1	0	2	0	2
2	3	2	3	3	2	3	2	1	3	1	3

$\mathcal{B}^{(3)}$

0	0	2	2	0	0	1	1	0	0	1	1
1	1	3	3	2	2	3	3	3	3	2	2
0	1	0	1	0	2	0	2	0	1	0	1
3	2	3	2	1	3	1	3	2	3	2	3

Next, we consider an improvement of Theorem 2.2.8. Suppose an $LOA(t, k', q)$ containing $q^{k'-t}$ $OA(t, k', q)$s exists. Utilizing the $LOA(t, k', q)$ to partition each design $\mathcal{B}^{(i)}$ in Theorem 2.2.8, a new t-SEED can be obtained.

Theorem 2.2.11. *If there exist an $LOA(t, k', q)$, a t*-$(n, k'; m')$ SEED and a $\lfloor \frac{t}{2} \rfloor$*-resolvable t*-$(v, k; m)$ SEED such that each sub-design $\mathcal{B}^{(i,j)}$ contains q blocks, then there exists a $\lfloor \frac{t}{2} \rfloor$*-resolvable t*-$(nv, kk'; q^{k'-t}h^{k'-1}m^{k'}m')$ SEED, where h is the number of subfamilies $\mathcal{B}^{(i,j)}$ in $\mathcal{B}^{(i)}$.*

Proof: Let $\{A^{(r)} = (a_{ij}^{(r)}) : r = 1, \ldots, q^{k'-t}\}$ be an $LOA(t, k', q)$ with elements in $[q]$ and $\mathcal{A}^{(r)} = (\mathbf{a}_1, \mathbf{a}_2, \ldots, \mathbf{a}_{q^t})$ be the set of column vectors in an OA $A^{(r)}$. A $\lfloor \frac{t}{2} \rfloor$*-resolvable t*-$(v, k; m)$ SEED and a t*-$(n, k'; m')$ SEED are defined similarly to the proof of Theorem 2.2.8.

We consider the blocks in $\mathcal{B}^{(p,l)}$ as an ordered set of blocks. Let $\mathcal{B}^{(p,l)} = (B_1^{(p,l)}, \ldots, B_q^{(p,l)})$. For given sub-designs $\mathcal{B}^{(p_1,l_1)}$, ..., $\mathcal{B}^{(p_{k'},l_{k'})}$, choose a block $B_{\cdot}^{(p_i,l_i)}$ from each $\mathcal{B}^{(p_i,l_i)}$, and then define a new block by

$$\oplus\big(B_{a_{1i}}^{(p_1,l_1)}, B_{a_{2i}}^{(p_2,l_2)}, \ldots, B_{a_{k'i}}^{(p_{k'},l_{k'})}; X\big)$$

for each column vector $\mathbf{a} = {}^t(a_{1i}, \ldots, a_{k'i}) \in \mathcal{A}^{(r)}$ and a block X in a design $\mathcal{X}^{(s)}$ of a t*-$(n, k'; m')$ SEED. Then

$$\mathcal{C}^{(\mathbf{p},\boldsymbol{\Delta},r,s,l)} = \bigcup_{X\in\mathcal{X}^{(s)}} \bigcup_{\mathbf{a}_i\in\mathcal{A}^{(r)}} \oplus\big(B_{a_{1i}}^{(p_1,l)}, B_{a_{2i}}^{(p_2,l+\Delta_2)}, \ldots, B_{a_{k'i}}^{(p_{k'},l+\Delta_{k'})}; X\big)$$

is a sub-design on V, where $\mathbf{p} = (p_1, \ldots, p_{k'}) \in [m]^{k'}$, $\boldsymbol{\Delta} = (\Delta_2, \ldots, \Delta_{k'}) \in [h]^{k'-1}$ and $l + \boldsymbol{\Delta} = (l, l + \Delta_2, \ldots, l + \Delta_{k'}) \pmod h$.

Hence we can partition the family of blocks of (2.2.1) into $q^{k'-t}$ sub-families of blocks by utilizing an $LOA(t, k', q)$, each of which forms a design of the desired t*-SEED. Then a new design

$$\mathcal{C}^{(\mathbf{p},\boldsymbol{\Delta},r,s)} = \bigcup_{l=1}^{h} \mathcal{C}^{(\mathbf{p},\boldsymbol{\Delta},r,s,l)}.$$

is defined. It is shown that a collection of designs

$$\big\{\mathcal{C}^{(\mathbf{p},\boldsymbol{\Delta},r,s)} : \mathbf{p} \in [m]^{k'}, \boldsymbol{\Delta} \in [h]^{k'-1}, r \in \{1, \ldots, q^{k'-t}\}\big\}$$

forms a t*-$(nv, kk'; q^{k'-t}h^{k'-1}m^{k'}m')$ SEED by a similar argument to that of Theorem 2.2.8.

To complete the proof, we have only to note the following: In this construction, we treat a block B_i in $\mathcal{B}$ as a symbol i in OA. Thus we define a w-"block-tuple" as an ordered w blocks. By the definition of orthogonal array $OA(t, k', q)$, every ordered w-tuple of $[q]$ occurs exactly q^{t-w} times in any w rows of each OA. That is, every ordered w-"block-tuple" occurs exactly q^{t-w} times in every sub-design $\mathcal{C}^{(\mathbf{p},\boldsymbol{\Delta},r,s,l)}$.

Hence we obtain a $\lfloor \frac{t}{2} \rfloor$*-resolvable t*-$(nv, kk'; q^{k'-t}h^{k'-1}m^{k'}m')$ SEED. □

Example 2.2.12. An $LOA(2, 3, 2)$ and a 1*-resolvable 2*-(4,2;1) SEED are presented in Example 2.2.7 and Table 2.2.1, respectively. Assume that X is a block chosen from a 2-$(n, 3; m')$ SEED. Utilizing Theorem 2.2.11, we find a 2*-$(4n, 6; 18m')$ SEED in Table 2.2.3.

Let $V = [4] \times [n]$, and fix a block $X = \{0, 1, 2\}$ from a 2*-$(n, 3; m')$ SEED to construct a design $\mathcal{B}$. Then a column ${}^t(a, b \mid c, d \mid e, f)$ implies a block $\{(a, 0), (b, 0), (c, 1), (d, 1), (e, 2), (f, 2)\}$. For convenience, we show only some parts of new designs here. In Table 2.2.3, designs $\mathcal{C}^{(\mathbf{p}_1, \mathbf{\Delta}_1, 1, s)}$ and $\mathcal{C}^{(\mathbf{p}_1, \mathbf{\Delta}_1, 2, s)}$ are presented, where $\mathbf{p}_1 = (1, 1, 1)$, $\mathbf{\Delta}_1 = (0, 0, 0)$.

Table 2.2.3: Designs $\mathcal{C}^{(\mathbf{p}_1, \mathbf{\Delta}_1, 1, s)}$ and $\mathcal{C}^{(\mathbf{p}_1, \mathbf{\Delta}_1, 2, s)}$ of a 2*-$(4n, 6; 18m')$ SEED

$\mathcal{C}^{((1,1,1),(0,0,0),1,s)}$	$\mathcal{C}^{((1,1,1),(0,0,0),2,s)}$
0 2 2 0 0 1 1 0 0 1 1 0	2 0 0 2 1 0 0 1 1 0 0 1
1 3 3 1 2 3 3 2 3 2 2 3	3 1 1 3 3 2 2 3 2 3 3 2
$\bar{0}$ $\bar{0}$ $\bar{2}$ $\bar{2}$ $\bar{0}$ $\bar{0}$ $\bar{1}$ $\bar{1}$ $\bar{0}$ $\bar{0}$ $\bar{1}$ $\bar{1}$	$\bar{2}$ $\bar{2}$ $\bar{0}$ $\bar{0}$ $\bar{1}$ $\bar{1}$ $\bar{0}$ $\bar{0}$ $\bar{1}$ $\bar{1}$ $\bar{0}$ $\bar{0}$
1 1 3 3 2 2 3 3 3 3 2 2	3 3 1 1 3 3 2 2 2 2 3 3
$\bar{0}$ $\bar{2}$ $\bar{0}$ $\bar{2}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$	$\bar{2}$ $\bar{0}$ $\bar{2}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$
1 3 1 3 2 3 2 3 3 2 3 2	3 1 3 1 3 2 3 2 2 3 2 3

In Table 2.2.4, another two designs $\mathcal{C}^{(\mathbf{p}_2, \mathbf{\Delta}_2, 1, s)}$ and $\mathcal{C}^{(\mathbf{p}_2, \mathbf{\Delta}_2, 2, s)}$ are presented, where $\mathbf{p}_2 = (1, 1, 1)$, $\mathbf{\Delta}_2 = (0, 0, 1)$. The other designs are obtained similarly.

Table 2.2.4: Designs $\mathcal{C}^{(\mathbf{p}_2, \mathbf{\Delta}_2, 1, s)}$ and $\mathcal{C}^{(\mathbf{p}_2, \mathbf{\Delta}_2, 2, s)}$ of a 2*-$(4n, 6; 18m')$ SEED

$\mathcal{C}^{((1,1,1),(0,0,1),1,s)}$	$\mathcal{C}^{((1,1,1),(0,0,1),2,s)}$
0 2 2 0 0 1 1 0 0 1 1 0	2 0 0 2 1 0 0 1 1 0 0 1
1 3 3 1 2 3 3 2 3 2 2 3	3 1 1 3 3 2 2 3 2 3 3 2
$\bar{0}$ $\bar{0}$ $\bar{2}$ $\bar{2}$ $\bar{0}$ $\bar{0}$ $\bar{1}$ $\bar{1}$ $\bar{0}$ $\bar{0}$ $\bar{1}$ $\bar{1}$	$\bar{2}$ $\bar{2}$ $\bar{0}$ $\bar{0}$ $\bar{1}$ $\bar{1}$ $\bar{0}$ $\bar{0}$ $\bar{1}$ $\bar{1}$ $\bar{0}$ $\bar{0}$
1 1 3 3 2 2 3 3 3 3 2 2	3 3 1 1 3 3 2 2 2 2 3 3
$\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{2}$ $\bar{0}$ $\bar{2}$	$\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{1}$ $\bar{0}$ $\bar{2}$ $\bar{0}$ $\bar{2}$ $\bar{0}$
2 3 2 3 3 2 3 2 1 3 1 3	3 2 3 2 2 3 2 3 3 1 3 1

2.3 Applications of t-SEEDs

In this section, we will describe two applications of t-SEEDs. Actually a t-SEED was introduced from an application to quantum jump codes by Beth et al. [6]. In Section 2.3.1, we will give a brief description of the relation between a t-SEED and a quantum jump code. In Section 2.3.2, a new application of t-SEEDs to secret sharing schemes in cryptography is derived.

2.3.1 Quantum jump codes and t-SEEDs

Quantum jump codes have a close connection with t-SEEDs. Beth et al. [6] introduced the notion of a t-SEED, which is a special class of quantum jump codes. In 2011, Jimbo and Shiromoto [38] gave a brief survey of quantum jump codes together with some new results.

We give the definition of quantum jump codes as a generalization of t-SEEDs and state a relation to t-SEEDs. For further details on quantum jump codes, we refer the reader to [1, 2, 9, 10, 20, 38, 75, 76].

For a v-set V and a positive integer $k < v$, let

$$\mathcal{B}^{(i)} = \sum_{B \in \binom{V}{k}} \alpha_B^{(i)} B \quad (i = 1, 2, \ldots, m)$$

be a formal sum with coefficients $\alpha_B^{(i)} \in \mathbb{C}$. A family of formal sums $\{\mathcal{B}^{(i)} : i = 1, 2, \ldots, m\}$ is called a *t-error correcting quantum jump code* with length v, weight k and dimension m, denoted by a $(v, m, t)_k$ jump code, if

$$\sum_{T \subset B \in \binom{V}{k}} \overline{\alpha}_B^{(i)} \alpha_B^{(j)} = \delta_{ij} \mu_T \tag{2.3.1}$$

holds for any $T \subset V$ such that $|T| \leq t$, where the summation is taken for all k-subsets B containing T and $\delta_{ij} = 1$, or 0 according as $i = j$, or not. Note that $\overline{\alpha}$ is the complex conjugate of α and μ_T is a constant depending only on T. Without loss of generality, we assume that $\mu_\emptyset = 1$. In a quantum jump code, a larger dimension is better in the sense that the code has a larger code space for given t, k and v.

Though the coefficients of a quantum jump code are taken from $\mathbb{C}$, by restricting $\alpha_B^{(i)} = 0$ or c_i, where c_i is a positive real number, we obtain a t-SEED. Actually, the block size of each B is k. Each $\mathcal{B}^{(i)}$ can be regarded as a family of k-subsets whose coefficients are not zero. By letting $T = \emptyset$ and $i \neq j$, the equation (2.3.1) implies that at least one of $\alpha_B^{(i)}$ or $\alpha_B^{(j)}$ is zero, since $\alpha_B^{(i)} \geq 0$, which means that $\mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m)}$ are disjoint. Whereas, when $T = \emptyset$ and $i = j$, we obtain $c_i^2 = |\mathcal{B}^{(i)}| \mu_\emptyset = |\mathcal{B}^{(i)}|$. Hence, $c_i = \frac{1}{\sqrt{|\mathcal{B}^{(i)}|}}$.

Moreover, in the case of $i = j$, for any $T \subset V$ satisfying $|T| \leq t$, we have

$$\sum_{T \subset B \subset \binom{V}{k}} \overline{\alpha}_B^{(i)} \alpha_B^{(i)} = c_i^2 \cdot \mu_T |\mathcal{B}^{(i)}| = \mu_T,$$

thus the jump code is a t-$(v, k; m)$ SEED.

Hence, a t-$(v, k; m)$ SEED with larger dimension m is desired for given t, k and v. The upper bound for a t-SEED in Theorem 2.1.1 was originally proved for that of a quantum jump code [6].

2.3.2 Secret sharing schemes and t-SEEDs

In this subsection, we describe the notion of a "secret sharing scheme" and show how a secret sharing scheme is constructed by utilizing a t-SEED. In cryptography, "secret sharing" refers to any method for distributing a secret among participants. It is a method of "secure key management." The basic idea is to divide the secret key (*secret*) into pieces and then distribute each piece to each participant. The secret key can only be recovered when certain subsets of the participants get together.

In 1979, Blakley [8] and Shamir [69] proposed two different secret sharing schemes. Blakely's scheme is an approach based on a simple geometric idea. Shamir's scheme is based on Lagrange interpolating polynomials. In 1988, Stinson and Vanstone [77] realized a secret sharing scheme (a *threshold scheme*) based on combinatorial designs. Some results and characterizations of threshold schemes can be found in [14, 16, 57, 66, 77]. Here, we will discuss the relation between a *t-secure* secret sharing scheme and a t-SEED in a similar way to [77].

In a secret sharing scheme, there are a dealer and k participants $P = \{p_1, p_2, \ldots, p_k\}$. The dealer chooses a secret key s from a key space $\Omega = \{1, 2, \ldots, m\}$. A key s is associated to a subfamily $\mathcal{B}^{(s)}$ of $\binom{V}{k}$. Each element in $B \in \mathcal{B}^{(s)}$ is called a *share* of secret. Furthermore, the dealer randomly chooses one k-subset $B = \{b_1, b_2, \ldots, b_k\} \in \mathcal{B}^{(s)}$ and distributes each share b_i to each participant p_i. In order that a secret key can be recovered uniquely, assume that $\mathcal{B}^{(s)}$ and $\mathcal{B}^{(s')}$ are disjoint for any $s \neq s'$.

A subset $Q \subset P$ is called a *qualified subset* if a secret s can be recovered from the set of shares $\{b_i : i \in Q\}$. The family of all qualified subsets is called the *access structure* of the scheme. If the access structure $\mathcal{A}$ corresponding to a secret sharing scheme contains no qualified subsets Q with $|Q| \leq t$, such a scheme is said to be *t-secure*. A secret sharing scheme is said to be *perfect* if no subsets of fewer than t participants can get any partial information regarding the secret.

Here we say that a secret sharing scheme is either *regular* or *non-regular*,

according to whether each $\mathcal{B}^{(i)}$ has the same number of blocks or not.

Though the discussion below is along the line of those in [77], for the reader's convenience, we restate it in our setting.

Let S be a set of shares with $|S| = u(\leq t)$. We identify the set S, an event that a set of shares S occurs. Let K be a random variable defined on the key space Ω. The dealer will choose the secret s with the same probability $P(K = s) = 1/m$. The probability distribution on the set of all possible shares S for a chosen $B \in \mathcal{B}^{(s)}$ is as follows:

$$P(S|B) = P(S|B \cap \{K = s\}) = \frac{\chi(S, B)}{\binom{k}{u}},$$

where $\chi(S, B)$ is 1 or 0 depending on whether $S \subset B$ or not.

A necessary and sufficient condition for a secret sharing scheme to be perfect is that

$$P(K = s|S) = \frac{P(S|K = s)P(K = s)}{P(S)} = P(K = s) = \frac{1}{m}$$

holds, which implies that $P(S|K = s) = P(S)$ for any s. Now, assume that a block $B \in \mathcal{B}^{(s)}$ has been chosen and the shares have been distributed to k participants. Then we have

$$\begin{aligned} P(S|K = s) &= \sum_{B \in \mathcal{B}^{(s)}} P(S, B|K = s) \\ &= \sum_{B \in \mathcal{B}^{(s)}} P(S|B \cap \{K = s\})P(B|K = s) \\ &= \frac{1}{\binom{k}{u}|\mathcal{B}^{(s)}|} \sum_{B \in \mathcal{B}^{(s)}} \chi(S, B) = \frac{\lambda_S^{(s)}}{\binom{k}{u}|\mathcal{B}^{(s)}|}, \end{aligned}$$

where $\lambda_S^{(s)}$ is the number of blocks in $\mathcal{B}^{(s)}$ containing S.

On the other hand, for any possible set of shares S, we have

$$\begin{aligned} P(S) &= \sum_{s \in \Omega} P(S \cap \{K = s\}) \\ &= \sum_{s \in \Omega} P(K = s)P(S|K = s) \\ &= \frac{1}{m} \sum_{s \in \Omega} \frac{\lambda_S^{(s)}}{\binom{k}{u}|\mathcal{B}^{(s)}|}. \end{aligned}$$

Thus $P(S|K) = P(S)$ holds if and only if $\lambda_S^{(s)}/|\mathcal{B}^{(s)}|$ is a constant for any $s \in \Omega$.

Because of the condition that $\mu_S = \lambda_S^{(i)}/|\mathcal{B}^{(i)}|$ is a constant in a t-SEED, we have the following theorem:

Theorem 2.3.1. *There exists a perfect t-secure secret sharing scheme with m possible secret keys for distributing shares chosen from a v-set to k participants if and only if there exists a t-$(v, k; m)$ SEED.*

Note that Theorem 2.3.1 is satisfied whether a perfect t-secure secret sharing scheme is regular or non-regular.

A $(t, k, v; m)$-threshold scheme is a $(t-1)$-secure secret scheme for distributing shares chosen from V to k participants for which the secret $s \in \Omega$ can be recovered from t or more shares. Unfortunately, a t-SEED cannot provide a $(t+1, k, v; m)$-threshold scheme since, even when $t+1$ shares are obtained, we may not be able to indicate a single secret. Of course, it is clear that the secret key can be recovered when k shares are obtained.

Stinson and Vanstone [77] characterized that a perfect regular $(t, k, v; m)$-threshold scheme is a set of "m mutually t-compatible k-uniform hypergraphs." Let

$$\mathcal{B}_u^{(i)} = \left\{ T \in \binom{V}{u} : T \subset B \in \mathcal{B}^{(i)} \right\} = \sum_{T \in \binom{V}{u}} \lambda_T^{(i)} T$$

be a multiset of u-tuple T's with multiplicity $\lambda_T^{(i)}$. A family of designs $(V; \mathcal{B}^{(1)}, \mathcal{B}^{(2)}, \ldots, \mathcal{B}^{(m)})$ is said to be m mutually $(t+1)$-compatible k-uniform hypergraphs if the following two conditions are satisfied:

(i) $\mathcal{B}_t^{(i)} = \mathcal{B}_t^{(j)}$, i.e., $\sum_{T \in \binom{V}{t}} \lambda_T^{(i)} T = \sum_{T \in \binom{V}{t}} \lambda_T^{(j)} T$.

(ii) $\mathcal{B}_{t+1}^{(i)} \cap \mathcal{B}_{t+1}^{(j)} = \emptyset$ for any $i \neq j$.

In general, a set of m mutually $(t+1)$-compatible k-uniform hypergraphs is a t-$(v, k; m)$ SEED with $|\mathcal{B}^{(i)}|$ constant for any i. Therefore constructions of m mutually $(t+1)$-compatible k-uniform hypergraphs on V given in [14, 66, 77] are also available for t-SEEDs. However, it should be noted that (ii) does not hold in general for a t-SEED since two distinct blocks containing the same $(t+1)$-tuple can be included in different $\mathcal{B}^{(i)}$ and $\mathcal{B}^{(j)}$ unless $k = t+1$, even if every design $\mathcal{B}^{(i)}$ in a t-SEED has the same number of blocks. Moreover, in the case of a t-SEED,

(i)' $\sum_{T\in\binom{V}{t}} \frac{\lambda_T^{(i)}}{|\mathcal{B}^{(i)}|}T = \sum_{T\in\binom{V}{t}} \frac{\lambda_T^{(j)}}{|\mathcal{B}^{(j)}|}T$

is required instead of (i).

For a t-SEED, in the special case of $k = t+1$, since $\mathcal{B}^{(i)}$ and $\mathcal{B}^{(j)}$ are disjoint for any i and j, (ii) is trivially satisfied. Hence, a t-$(v, t+1; m)$ SEED with $|\mathcal{B}^{(i)}|$ constant for any i is a set of m mutually $(t+1)$-compatible $(t+1)$-uniform hypergraphs on V.

For example, an $LS_\lambda(2, 3, v)$ is a set of m mutually 3-compatible 3-uniform hypergraphs on V, and it is also a 2-$(v, 3; m)$ SEED. An $LS_1(2, 4, v)$ is a 2-$(v, 4; m)$ SEED. However, it is not a set of m mutually 3-compatible 4-uniform hypergraphs on V since, by noting $\lambda = 1$, distinct blocks B and B' containing a given 3-subset must belong to distinct designs, which implies that (ii) is not satisfied.

Stinson and Vanstone's assertion can be slightly extended for a perfect non-regular $(t, k, v; m)$-threshold scheme. By similar proofs to [77] and Theorem 2.3.1, we can say that a perfect (non-regular) $(t, k, v; m)$-threshold scheme is equivalent to a set of "generalized" m mutually t-compatible k-uniform hypergraphs $(V; \mathcal{B}^{(1)}, \ldots, \mathcal{B}^{(m)})$ satisfying the following conditions:

(i) $\frac{\mathcal{B}_{t-1}^{(i)}}{|\mathcal{B}^{(i)}|} = \frac{\mathcal{B}_{t-1}^{(j)}}{|\mathcal{B}^{(j)}|}$, where $\frac{\mathcal{B}_{t-1}^{(i)}}{|\mathcal{B}^{(i)}|} = \sum_{T\in\binom{V}{t-1}} \frac{\lambda_T^{(i)}}{|\mathcal{B}^{(i)}|}T$.

(ii) $\mathcal{B}_t^{(i)} \cap \mathcal{B}_t^{(j)} = \emptyset$ for any $i \neq j$.

According to these results, we illustrate the relation in Fig 2.3.1.

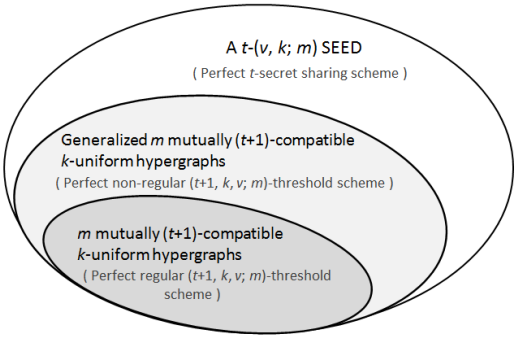

Figure 2.3.1: The relation between a t-SEED and m mutually $(t+1)$-compatible k-uniform hypergraphs.

In the case of $k = t + 1$, an optimal t-SEED corresponds to m mutually $(t + 1)$-compatible $(t + 1)$-uniform hypergraphs, which is an optimal perfect $(t+1, t+1, v; m)$-threshold scheme with $m = \frac{v-t+1}{k-t+1}$. For the case of $k > t+1$, though, a t-SEED can be used only in the case when the perfect t-secure property is required. Instead of this disadvantage, we can take a larger key space Ω for given v, k, t than a $(t + 1, k, v; m)$-threshold scheme.

Chapter 3

Conflict-avoiding codes

This chapter focuses on optimal equi-difference conflict avoiding codes, especially for the cases of weights three and four.

Firstly, in Section 3.1, we give several properties of the multiplicative order of a unit in $\mathbb{Z}_n$ for $n \geq 2$, which are needed in our discussion of determining the sizes $M^e(n,3)$ and $M^e(n,4)$ of optimal codes in $\mathrm{CAC}^e(n,3)$ and $\mathrm{CAC}^e(n,4)$, respectively.

Section 3.2 is devoted to equi-difference codes in $\mathrm{CAC}^e(n,3)$ for odd n. We first present some explicit series of odd code length n for which a "tight" equi-difference CAC exists. Next we establish a calculation formula for the size $M^e(n,3)$ of an optimal (not necessarily tight) equi-difference code in $\mathrm{CAC}^e(n,3)$.

In Section 3.3, optimal equi-difference codes in $\mathrm{CAC}^e(n,4)$ are considered for a general integer $n \geq 4$. As a tool for determining the size $M^e(n,4)$ of an optimal equi-difference CAC, we bring a directed graph representation to our discussion. Analyzing the graph structure, we obtain recurrence formulae for the sizes of subcodes in an optimal equi-difference code of weight four, which eventually allow us to compute the exact value of $M^e(n,4)$.

3.1 Multiplicative order and suborder

In subsequent sections, $\mathbb{N}$ is the set of positive integers. For $n \in \mathbb{N}$, let $\mathbb{Z}_n^+ = \mathbb{Z}_n \setminus \{0\}$, and for an equivalence relation $\sim$ on $\mathbb{Z}_n^+$ defined by $x \sim y$ if and only if $x \pm y \equiv 0 \pmod{n}$ for $x, y \in \mathbb{Z}_n^+$, let $\Omega_n = \mathbb{Z}_n^+ / \sim$, that is,

$\Omega_n = \{1, 2, \ldots, \lfloor \frac{n}{2} \rfloor\}$.

For $t \in \mathbb{Z}_n^+$ and a unit $\theta(\neq 1) \in \mathbb{Z}_n^+$, let $t(\theta)_n$ and $t\langle\theta\rangle_n$ be the orbits of distinct integers of form $(t\theta^i : i = 0, 1, 2, \ldots)$ in $\mathbb{Z}_n^+$ and Ω_n, respectively. In the case of $t = 1$, we simply write them as $(\theta)_n$ and $\langle\theta\rangle_n$. The *multiplicative order* of θ in $\mathbb{Z}_n^+$, denoted by $\mathrm{ord}_n(\theta)$, is the smallest positive integer ℓ such that $\theta^\ell \equiv 1 \pmod{n}$. The smallest positive integer κ such that $\theta^\kappa \equiv \pm 1 \pmod{n}$ is called the *multiplicative suborder* of θ in $\mathbb{Z}_n^+$, denoted by $\mathrm{sord}_n(\theta)$. Thus $\mathrm{ord}_n(\theta) = |(\theta)_n|$ and $\mathrm{sord}_n(\theta) = |\langle\theta\rangle_n|$. It is easy to see that, when $n \neq 2$, $\mathrm{sord}_n(\theta) = \mathrm{ord}_n(\theta)/2$ or $\mathrm{ord}_n(\theta)$, depending on whether $-1 \in (\theta)_n$ or not. Note that, for any t satisfying $\gcd(t, n) = 1$, $|t\langle\theta\rangle_n| = \mathrm{sord}_n(\theta)$ holds.

3.1.1 General properties of order and suborder of a unit

In this subsection, several properties of general units in $\mathbb{Z}_n$ are given, which are needed to find optimal equi-difference codes.

Lemma 3.1.1. *Let $n_1, n_2, \theta \in \mathbb{N} \setminus \{1\}$. If $n_1 \mid n_2$ and $\gcd(\theta, n_2) = 1$, then $\mathrm{ord}_{n_1}(\theta) \mid \mathrm{ord}_{n_2}(\theta)$ and $\mathrm{sord}_{n_1}(\theta) \mid \mathrm{sord}_{n_2}(\theta)$.*

Proof: Let $\ell_1 = \mathrm{ord}_{n_1}(\theta)$ and $\ell_2 = \mathrm{ord}_{n_2}(\theta)$. Since $\theta^{\ell_2} - 1 \equiv 0 \pmod{n_2}$, if $n_1 \mid n_2$, then $\theta^{\ell_2} - 1 \equiv 0 \pmod{n_1}$ holds. Hence $\ell_1 \mid \ell_2$. In a similar manner, $\mathrm{sord}_{n_1}(\theta) \mid \mathrm{sord}_{n_2}(\theta)$ can be proved. □

Lemma 3.1.2. *Let $n \geq 3$ be an integer and $\theta \in \mathbb{Z}_n^+$ be a unit. For any $t \in \mathbb{Z}_n^+$, $|t(\theta)_n| = \mathrm{ord}_{\frac{n}{d}}(\theta)$, $|t(\theta)_n|$ divides $\mathrm{ord}_n(\theta)$, and*

$$|t\langle\theta\rangle_n| = \begin{cases} \dfrac{|t(\theta)_n|}{2} & \text{if } -1 \in (\theta)_{\frac{n}{d}}, \\ |t(\theta)_n| & \text{if } -1 \notin (\theta)_{\frac{n}{d}}, \end{cases}$$

that is, $|t\langle\theta\rangle_n| = \mathrm{sord}_{\frac{n}{d}}(\theta)$, where $d = \gcd(t, n)$.

Proof: Let $\ell = |t(\theta)_n|$, that is, ℓ is the smallest positive integer satisfying $t\theta^\ell \equiv t \pmod{n}$ for $t \in \mathbb{Z}_n^+$. Then we have $\frac{t}{d}\theta^\ell \equiv \frac{t}{d} \pmod{\frac{n}{d}}$, which can be reduced to $\theta^\ell \equiv 1 \pmod{\frac{n}{d}}$ since $\gcd(\frac{t}{d}, \frac{n}{d}) = 1$. Thus $\ell = |t(\theta)_n| = |(\theta)_{\frac{n}{d}}|$, and it follows from Lemma 3.1.1 that $|t(\theta)_n|$ divides $\mathrm{ord}_n(\theta)$. Here let $k = |t\langle\theta\rangle_n|$, that is, $t\theta^k \equiv \pm t \pmod{n}$, which can be reduced to $\theta^k \equiv \pm 1 \pmod{\frac{n}{d}}$. Then it turns out that $k = \ell$ if $-1 \notin (\theta)_{\frac{n}{d}}$ and $k = \ell/2$ if $-1 \in (\theta)_{\frac{n}{d}}$. □

Lemma 3.1.3. *Let $n \geq 3$ be an integer and $\theta \in \mathbb{Z}_n^+$ be a unit. If $4 \mid \mathrm{ord}_p(\theta)$ for any prime factor p of n, then $|t\langle\theta\rangle_n|$ is even for any $t \in \mathbb{Z}_n^+$.*

Proof: For any $t \in \mathbb{Z}_n^+$, let $d = \gcd(t, n)$ and $k = |t\langle\theta\rangle_n|$, that is, k is the smallest positive integer satisfying $t\theta^k \equiv \pm t \pmod{n}$. Then we have $\frac{t}{d}\theta^k \equiv \pm\frac{t}{d} \pmod{\frac{n}{d}}$, which is reduced to $\theta^k \equiv \pm 1 \pmod{\frac{n}{d}}$. Therefore $\theta^k \equiv \pm 1 \pmod{p}$ holds for any prime factor p of $\frac{n}{d}$, and thus $\theta^{2k} \equiv 1 \pmod{p}$. If $4 \mid \mathrm{ord}_p(\theta)$ holds for any prime factor p of n, then $2k$ must be divisible by 4, which means k is even for any $t \in \mathbb{Z}_n^+$. □

Corollary 3.1.4. *For an odd integer $n \geq 3$ and a unit $\theta \in \mathbb{Z}_n^+$, suppose that $-1 \in (\theta)_n$. If $4 \mid \mathrm{ord}_n(\theta)$, then $|t\langle\theta\rangle_n|$ is even for any $t \in \mathbb{Z}_n^+$. If $\mathrm{ord}_n(\theta) \equiv 2 \pmod{4}$, then $|t\langle\theta\rangle_n|$ is odd for any $t \in \mathbb{Z}_n^+$.*

Proof: Note that $\mathrm{sord}_n(\theta) = \frac{\mathrm{ord}_n(\theta)}{2}$ follows from the assumption $-1 \in (\theta)_n$ and Lemma 3.1.2.

(i) If $\mathrm{ord}_n(\theta) = 4\ell$, then $\mathrm{sord}_n(\theta) = 2\ell$, that is, ℓ is the smallest positive integer satisfying $\theta^{2\ell} + 1 \equiv 0 \pmod{n}$. Thus, for any prime factor p of n, $\theta^{2\ell} + 1 \equiv 0 \pmod{p}$ holds. Let k be the smallest positive integer satisfying $\theta^k + 1 \equiv 0 \pmod{p}$. Then, $2\ell = rk$ holds for some odd integer r. In fact, if r is even, then $\theta^{rk} = \theta^{2\ell} \equiv 1 \pmod{p}$, a contradiction. Hence k must be even. Therefore, $4 \mid \mathrm{ord}_p(\theta)$. Then Lemma 3.1.3 shows the first assertion.

(ii) If $\mathrm{ord}_n(\theta) = 4\ell + 2$, then $\mathrm{sord}_n(\theta) = 2\ell + 1$. Since Lemma 3.1.1 implies that $|t\langle\theta\rangle_n|$ divides $\mathrm{sord}_n(\theta)$, $|t\langle\theta\rangle_n|$ must be odd. □

Note that if $4 \mid \mathrm{ord}_p(\theta)$ for any prime factor p of n, then n is indivisible by 3 since $4 \mid \mathrm{ord}_p(\theta) \mid (p-1)$ for any prime factor p of n.

Lemma 3.1.5. *Let $n = 3n_0$ be an odd integer and $\theta \in \mathbb{Z}_n^+$ be a unit. If $4 \mid \mathrm{ord}_p(\theta)$ for any prime factor p of n_0, then $|t\langle\theta\rangle_n|$ is even for any $t \in \mathbb{Z}_n^+ \setminus \{n_0, 2n_0\}$ and $|t\langle\theta\rangle_n| = 1$ for $t \in \{n_0, 2n_0\}$.*

Proof: If $t \not\equiv 0 \pmod{n_0}$, then it immediately follows from Lemma 3.1.3 that $|t\langle\theta\rangle_{n_0}|$ is even. Then Lemma 3.1.1 guarantees that $|t\langle\theta\rangle_n|$ is even. If $t \equiv 0 \pmod{n_0}$, then $3 \nmid t$ since $\gcd(n_0, 3) = 1$ follows from the assumption on each prime factor of n_0, and thus $|t\langle\theta\rangle_n| = |\langle 1\rangle_3| = |\langle 2\rangle_3| = 1$, which completes the proof. □

From Corollary 3.1.4 and Lemma 3.1.5, we can state the following.

Corollary 3.1.6. *For an odd integer $n = 3n_0$ and a unit $\theta \in \mathbb{Z}_n^+$, suppose that $4 \mid \mathrm{ord}_{n_0}(\theta)$ and $-1 \in (\theta)_{n_0}$. Then $|t\langle\theta\rangle_n|$ is even for any $t \in \mathbb{Z}_n^+ \setminus \{n_0, 2n_0\}$ and $|t\langle\theta\rangle_n| = 1$ for $t \in \{n_0, 2n_0\}$.*

Example 3.1.7. (1) The case when $\theta = 2$ and $n = 5 \times 13 = 65$. Since $\mathrm{ord}_5(2) = 4$ and $\mathrm{ord}_{13}(2) = 12$, Lemma 3.1.3 guarantees that $|t\langle 2\rangle_{65}|$ is even for any $t \in \mathbb{Z}_{65}^+$. This can also be verified from Corollary 3.1.4 since $-1 \equiv 64 \in (2)_{65} = (2^i : i = 0, 1, \ldots, 11) = (1, 2, 4, 8, 16, 32, 64, 63, 61, 57, 49, 33)$ and $\mathrm{ord}_{65}(2) = 12$. In fact, for any $t \in \mathbb{Z}_{65}^+$, $t\langle 2\rangle_{65}$ is congruent to any one of

$$\langle 2\rangle_{65} = (1, 2, 4, 8, 16, 32),\ 3\langle 2\rangle_{65} = (3, 6, 12, 24, 17, 31),$$
$$5\langle 2\rangle_{65} = (5, 10, 20, 25, 15, 30),\ 7\langle 2\rangle_{65} = (7, 14, 28, 9, 18, 29),$$
$$11\langle 2\rangle_{65} = (11, 22, 21, 23, 19, 27),\ 13\langle 2\rangle_{65} = (13, 26).$$

(2) The case when $\theta = 2$ and $n = 3 \times 17 = 51$. Since $\mathrm{ord}_{17}(2) = 8$, Lemma 3.1.5 guarantees that $|t\langle 2\rangle_{51}|$ is even for any $t \in \mathbb{Z}_{51}^+ \setminus \{17, 34\}$ and $|17\langle 2\rangle_{51}| = |34\langle 2\rangle_{51}| = 1$. This can also be verified from Corollary 3.1.6 since $\mathrm{ord}_{17}(2) = 8$ and $-1 \equiv 16 \in (2)_{17} = (2^i : i = 0, 1, \ldots, 7) = (1, 2, 4, 8, 16, 15, 13, 9)$. Actually, for any $t \in \mathbb{Z}_{51}^+$, $t\langle 2\rangle_{51}$ is congruent to any one of

$$\langle 2\rangle_{51} = (1, 2, 4, 8, 16, 19, 13, 25),\ 5\langle 2\rangle_{51} = (5, 10, 20, 11, 22, 7, 14, 23),$$
$$3\langle 2\rangle_{51} = (3, 6, 12, 24),\ 9\langle 2\rangle_{51} = (9, 18, 15, 21),\ 17\langle 2\rangle_{51} = (17).$$

Remark 3.1.8. Replacing n in Lemma 3.1.5 and Corollary 3.1.6 by $n = 3^e n_0$ with $e \geq 2$, we can no longer guarantee that $|t\langle\theta\rangle_n|$ is even or $|t\langle\theta\rangle_n| = 1$ for all $t \in \mathbb{Z}_n^+$. For example, when $t = n_0$, $|t\langle\theta\rangle_n| = |\langle\theta\rangle_{3^e}|$ is a divisor of $\varphi(3^e) = 3^{e-1}$, where φ is Euler's totient function. This means that $|n_0\langle\theta\rangle_n|$ could be odd depending on the choice of θ.

Lemma 3.1.9. *Let $n_1, n_2, \theta \in \mathbb{N} \setminus \{1\}$. If $\gcd(n_1, n_2) = 1$ and $\gcd(\theta, n_1 n_2) = 1$, then $\mathrm{ord}_{n_1 n_2}(\theta) = \mathrm{lcm}\,(\mathrm{ord}_{n_1}(\theta), \mathrm{ord}_{n_2}(\theta))$.*

Proof: Let $\ell_1 = \mathrm{ord}_{n_1}(\theta)$, $\ell_2 = \mathrm{ord}_{n_2}(\theta)$ and $\ell = \mathrm{lcm}\,(\ell_1, \ell_2)$. Then $\theta^\ell \equiv 1 \pmod{n_1}$ and $\theta^\ell \equiv 1 \pmod{n_2}$ hold. Since $\gcd(n_1, n_2) = 1$, we have $\theta^\ell \equiv 1 \pmod{n_1 n_2}$, which implies $\mathrm{ord}_{n_1 n_2}(a) \mid \ell$. Suppose that $\mathrm{ord}_{n_1 n_2}(\theta) \nmid \ell_1$. Then there exist integers s and r such that $\mathrm{ord}_{n_1 n_2}(\theta) = s\ell_1 + r$ for $0 < r < \ell_1$, which means that $\theta^{s\ell_1 + r} \equiv 1 \pmod{n_1 n_2}$ and thus $\theta^{s\ell_1 + r} \equiv 1 \pmod{n_1}$ holds, that is, $\theta^r \equiv 1 \pmod{n_1}$ holds. This contradicts $\ell_1 = \mathrm{ord}_{n_1}(\theta)$. Hence we have $\mathrm{ord}_{n_1 n_2}(\theta) \mid \ell_1$. By a similar argument, we have $\mathrm{ord}_{n_1 n_2}(\theta) \mid \ell_2$ as well. This concludes $\mathrm{ord}_{n_1 n_2}(\theta) = \mathrm{lcm}\,(\ell_1, \ell_2)$. □

Lemma 3.1.10. *Let p be an odd prime and $\theta \in \mathbb{Z}_p^+$. If there exists an integer $f \in \mathbb{N}$ such that $\mathrm{sord}_{p^e}(\theta) < \mathrm{sord}_{p^{e+1}}(\theta)$ for any $e \geq f$, then $\mathrm{sord}_{p^e}(\theta) = p^{e-f}\mathrm{sord}_{p^f}(\theta)$ holds for any $e \geq f \geq 1$. Moreover, if $-1 \in (\theta)_p$ and $f = v_p(\theta^{\mathrm{sord}_p(\theta)} + 1)$, or $-1 \notin (\theta)_p$ and $f = v_p(\theta^{\mathrm{sord}_p(\theta)} - 1)$, then $\mathrm{sord}_{p^e}(\theta) = p^{e-f}\mathrm{sord}_p(\theta)$ holds for any $e \geq f$, where $v_p(x)$ is the highest power of p in x.*

Proof: We prove the first assertion by mathematical induction on e. It is trivial for the case $e = f$. Suppose that the assertion is true for some $e > f$. Then we have $\mathrm{sord}_{p^e}(\theta) < \mathrm{sord}_{p^{e+1}}(\theta)$ and $\mathrm{sord}_{p^e}(\theta) = p^{e-f}\mathrm{sord}_{p^f}(\theta)$. Note that $\theta^{\mathrm{sord}_{p^e}(\theta)}$ can be written as $kp^e \pm 1$ for some $k \in \mathbb{N}$. If $p \mid k$, then $\theta^{\mathrm{sord}_{p^e}(\theta)} = kp^e \pm 1 \equiv \pm 1 \pmod{p^{e+1}}$, which implies that $\mathrm{sord}_{p^{e+1}}(\theta) \mid \mathrm{sord}_{p^e}(\theta)$. Thus we have $\mathrm{sord}_{p^e}(\theta) = \mathrm{sord}_{p^{e+1}}(\theta)$, however, this contradicts $\mathrm{sord}_{p^e}(\theta) < \mathrm{sord}_{p^{e+1}}(\theta)$. Hence $p \nmid k$. Since $\mathrm{sord}_{p^e}(\theta) \mid \mathrm{sord}_{p^{e+1}}(\theta)$, by letting $\mathrm{sord}_{p^{e+1}}(\theta) = u{\cdot}\mathrm{sord}_{p^e}(\theta)$ for some $u \in \mathbb{N}$, we have

$$\theta^{\mathrm{sord}_{p^{e+1}}(\theta)} = \theta^{u\cdot\mathrm{sord}_{p^e}(\theta)} = (kp^e \pm 1)^u = \sum_{i=0}^{u} \binom{u}{i} (kp^e)^i (\pm 1)^{u-i}.$$

Note that $2e \geq e + 1$ is satisfied for $e \geq 1$. Then

$$\theta^{\mathrm{sord}_{p^{e+1}}(\theta)} \equiv (\pm 1)^u + (\pm 1)^{u-1} ukp^e \equiv \pm 1 \pmod{p^{e+1}}, \tag{3.1.1}$$

and it is easily observed that the smallest positive integer u satisfying (3.1.1) is p since $p \nmid k$. Hence $\mathrm{sord}_{p^{e+1}}(\theta) = p{\cdot}\mathrm{sord}_{p^e}(\theta) = p^{e+1-f}\mathrm{sord}_{p^f}(\theta)$ holds, which proves the first assertion.

From Lemma 3.1.1, $\mathrm{sord}_p(\theta) \mid \mathrm{sord}_{p^i}(\theta)$ holds for any $i \geq 1$. Note that $f = v_p(\theta^{\mathrm{sord}_p(\theta)} \pm 1)$ implies that $\theta^{\mathrm{sord}_p(\theta)} \pm 1 \equiv 0 \pmod{p^f}$. Thus $\mathrm{sord}_{p^i}(\theta) = \mathrm{sord}_p(\theta)$ for any $1 \leq i \leq f$, which proves the second assertion. □

Lemma 3.1.11. *For an odd prime p and $\theta \in \mathbb{Z}_p^+$, $v_2(\mathrm{sord}_{p^e}(\theta)) = v_2(\mathrm{sord}_p(\theta))$ holds for any $e \geq 2$. If $-1 \notin (\theta)_p$, then $\mathrm{sord}_{p^e}(\theta)$ is odd for any $e \in \mathbb{N}$.*

Proof: Since $\mathrm{sord}_{p^e}(\theta) \mid \mathrm{sord}_{p^{e+1}}(\theta)$ for any $e \in \mathbb{N}$, $\mathrm{sord}_{p^e}(\theta) = \mathrm{sord}_{p^{e+1}}(\theta)$ holds unless $\mathrm{sord}_{p^e}(\theta) < \mathrm{sord}_{p^{e+1}}(\theta)$. Then, together with Lemma 3.1.10, we know that $\mathrm{sord}_{p^e}(\theta)$ is an odd multiple of $\mathrm{sord}_p(\theta)$ for any $e \geq 2$, which proves the first assertion.

For the second assertion, it is sufficient to prove the case $e = 1$. Suppose that $\mathrm{sord}_p(\theta)$ is even. Then $\mathrm{sord}_p(\theta) = \mathrm{ord}_p(\theta) = 2k$ for some $k \in \mathbb{N}$. Since $\theta^{2k} - 1 = (\theta^k - 1)(\theta^k + 1) \equiv 0 \pmod{p}$, $\theta^k - 1 \equiv 0 \pmod{p}$ or $\theta^k + 1 \equiv 0 \pmod{p}$ must hold. However, $\theta^k - 1 \equiv 0 \pmod{p}$ contradicts $-1 \notin (\theta)_p$, and $\theta^k + 1 \equiv 0 \pmod{p}$ contradicts $\mathrm{sord}_p(\theta) = 2k$. Hence $\mathrm{sord}_p(\theta)$ must be odd, which completes the proof since $\mathrm{sord}_{p^e}(\theta)$ is an odd multiple of $\mathrm{sord}_p(\theta)$. □

Lemma 3.1.12. *Let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of an odd integer n and for a unit $\theta \in \mathbb{Z}_n^+$, let $P = \{p_i : -1 \in (\theta)_{p_i}, 1 \le i \le r\}$ and $\bar{P} = \{p_i : -1 \notin (\theta)_{p_i}, 1 \le i \le r\}$. Then*

$$\mathrm{sord}_n(\theta) = \alpha \cdot \mathrm{lcm}\big(\mathrm{sord}_{p_1^{e_1}}(\theta), \mathrm{sord}_{p_2^{e_2}}(\theta), \ldots, \mathrm{sord}_{p_r^{e_r}}(\theta)\big)$$

holds, where

$$\alpha = \begin{cases} 1 & \text{if } P = \emptyset, \text{ or } \bar{P} = \emptyset \text{ and } v_2(\mathrm{sord}_{p_i}(\theta))\text{'s are the same for } 1 \le i \le r, \\ 2 & \text{otherwise.} \end{cases}$$

Proof: Let $\mathrm{sord}_{p_i^{e_i}}(\theta) = \ell_i$ and $\mathrm{lcm}(\ell_1, \ell_2, \ldots, \ell_r) = \ell$ (thus $\mathrm{sord}_n(\theta) = \alpha\ell$). By noting Lemma 3.1.9 and the fact that $\mathrm{sord}_{p_i^{e_i}}(\theta) \mid \mathrm{sord}_n(\theta)$ holds for each i, we have

$$\ell \mid \mathrm{sord}_n(\theta) \mid \mathrm{ord}_n(\theta) \mid 2\ell,$$

which means that $\alpha = 1$ or 2. We will prove the assertion by showing that the condition for $\alpha = 1$ is necessary and sufficient. Note that, by Lemma 3.1.11, $v_2(\ell_i) = v_2(\mathrm{sord}_{p_i}(\theta))$ holds for any i.

($\Rightarrow$) If $P = \emptyset$, that is, $\bar{P} = \{p_1, p_2, \ldots, p_r\}$, then $\ell_i = \mathrm{ord}_{p_i^{e_i}}(\theta)$ and thus $\alpha = 1$ since $\mathrm{ord}_n(\theta) = \ell$ follows from Lemma 3.1.9.

If $\bar{P} = \emptyset$, that is, $P = \{p_1, p_2, \ldots, p_r\}$, and $v_2(\mathrm{sord}_{p_i}(\theta))$'s (thus $v_2(\ell_i)$'s) are the same for all i, then ℓ/ℓ_i is odd for any i. Therefore $\theta^{\ell} = (\theta^{\ell_i})^{\frac{\ell}{\ell_i}} \equiv -1 \pmod{p_i^{e_i}}$ holds for any i. This means that $\alpha = 1$.

($\Leftarrow$) Suppose that $\alpha = 1$, that is, $\mathrm{sord}_n(\theta) = \ell$. If $-1 \in (\theta)_n$, then $\theta^{\ell} \equiv -1 \pmod{p_i^{e_i}}$ should hold for any i and thus $\theta^{\ell_i} \equiv -1 \pmod{p_i^{e_i}}$, which implies that $\bar{P} = \emptyset$ and ℓ/ℓ_i is odd for any i. In this case, $v_2(\ell_i)$'s must be the same for all i.

If $-1 \notin (\theta)_n$, then $n^{\ell} \equiv 1 \pmod{p_i^{e_i}}$ holds for any i. It follows from Lemma 3.1.11 that ℓ_i is an odd multiple of $\mathrm{sord}_{p_i}(\theta)$ for any $p_i \in P \cup \bar{P}$, and ℓ_i itself is odd especially for $p_i \in \bar{P}$. Let $\ell_P = \mathrm{lcm}(\ell_i : p_i \in P)$ and $\ell_{\bar{P}} = \mathrm{lcm}(\ell_i : p_i \in \bar{P})$. Then $\ell_{\bar{P}}$ is odd and $\ell = \mathrm{lcm}(\ell_P, \ell_{\bar{P}})$. By noting that

$$\theta^{\ell_P} \equiv -1 \pmod{\prod_{p_i \in P} p_i^{e_i}},$$

it is easy to see that ℓ_P/ℓ_i is odd for any $p_i \in P$. On the other hand, since $\theta^{\ell} \equiv 1 \pmod{p_i^{e_i}}$ holds for any $p_i \in P$, ℓ/ℓ_i must be even and thus ℓ_P/ℓ_i must be even for any $p_i \in P$, a contradiction. Therefore, if $\alpha = 1$ and $-1 \notin (\theta)_n$,

then $P = \emptyset$. $\square$

The following lemma can be easily shown using the uniqueness of prime factorization.

Lemma 3.1.13. *For any multiplicative function ψ of $n \in \mathbb{N}$,*

$$\sum_{d|n} \psi(d) = \prod_{p|n} \big(1 + \psi(p) + \psi(p^2) + \cdots + \psi(p^{v_p(n)})\big)$$

holds, where the product runs through all the prime factors of n.

Lemma 3.1.14. *Let n be an odd integer and $\theta \in \mathbb{Z}_n^+$ be a unit. If $\mathrm{sord}_n(\theta)$ is a multiplicative function with respect to n, then the number of disjoint cycles $t\langle\theta\rangle_n$ in Ω_n is*

$$N(n) = \frac{1}{2}\Big\{\prod_{p|n}\Big(1 + \frac{1}{\mathrm{sord}_p(\theta)}\big(p^{f_p} - 1 + p^{f_p-1}(p-1)(v_p(n) - f_p)\big)\Big) - 1\Big\},$$

where the product runs through all the prime factors of n, and $f_p = v_p(\theta^{\mathrm{sord}_p(\theta)} + 1)$ or $v_p(\theta^{\mathrm{sord}_p(\theta)} - 1)$ depending on $-1 \in (\theta)_p$ or not.

Proof: Recall that for a given d, $|t\langle\theta\rangle_n| = \mathrm{sord}_{\frac{n}{d}}(\theta)$ for any $t \in \mathbb{Z}_n^+$ such that $d = \gcd(t, n)$ (see Lemma 3.1.2). Then the number of disjoint cycles $t\langle\theta\rangle_n$ of length $\mathrm{sord}_{\frac{n}{d}}(\theta)$ with $d = \gcd(t, n)$ in Ω_n is $\frac{\varphi(\frac{n}{d})}{2\cdot\mathrm{sord}_{\frac{n}{d}}(\theta)}$. Thus

$$N(n) = \sum_{1<d|n} \frac{\varphi(d)}{2\cdot\mathrm{sord}_d(\theta)} = \frac{1}{2}\sum_{d|n} \frac{\varphi(d)}{\mathrm{sord}_d(\theta)} - \frac{1}{2}. \tag{3.1.2}$$

Applying Lemma 3.1.13, we have

$$N(n) = \frac{1}{2}\prod_{p|n}\Big(1 + \frac{\varphi(p)}{\mathrm{sord}_p(\theta)} + \cdots + \frac{\varphi(p^{f_p})}{\mathrm{sord}_{p^{f_p}}(\theta)} + \frac{\varphi(p^{f_p+1})}{\mathrm{sord}_{p^{f_p+1}}(\theta)} + \cdots + \frac{\varphi(p^{v_p(n)})}{\mathrm{sord}_{p^{v_p(n)}}(\theta)}\Big) - \frac{1}{2}.$$

Then it follows from Lemma 3.1.11 that

$$\begin{aligned} N(n) &= \frac{1}{2}\prod_{p|n}\Big(1 + \frac{p-1}{\mathrm{sord}_p(\theta)}\big(1 + p + p^2 + \cdots + p^{f_p-1} + p^{f_p-1} + \cdots + p^{f_p-1}\big)\Big) - \frac{1}{2} \\ &= \frac{1}{2}\Big\{\prod_{p|n}\Big(1 + \frac{1}{\mathrm{sord}_p(\theta)}\big(p^{f_p} - 1 + p^{f_p-1}(p-1)(v_p(n) - f_p)\big)\Big) - 1\Big\}. \end{aligned}$$

$\square$

Lemma 3.1.15. *Let n be an odd integer and $\theta \in \mathbb{Z}_n^+$ be a unit. If $\mathrm{sord}_n(\theta)$ is odd and $\gcd(\varphi(p^e), \varphi(q^f))$ is a power of 2 for any distinct prime factors p, q of n, where $e = v_p(n)$ and $f = v_q(n)$, then $\mathrm{sord}_n(\theta)$ is a multiplicative function with respect to n.*

Proof: It follows from Euler's theorem and Lemma 3.1.11 that, if $\gcd(\varphi(p^e), \varphi(q^f))$ is a power of 2, then so is $\gcd(\mathrm{sord}_{p^i}(\theta), \mathrm{sord}_{q^j}(\theta))$ for $1 \le i \le e$ and $1 \le j \le f$. Meanwhile, since $\mathrm{sord}_d(\theta) \mid \mathrm{sord}_n(\theta)$ for any divisor d of n, if $\mathrm{sord}_n(\theta)$ is odd, then $\mathrm{sord}_d(\theta)$ should be odd. This implies that $\gcd(\mathrm{sord}_{p^i}(\theta), \mathrm{sord}_{q^j}(\theta)) = 1$ for any pair of distinct primes p, q in n, $1 \le i \le e$ and $1 \le j \le f$. Hence $\mathrm{sord}_{d_1 d_2}(\theta) = \mathrm{sord}_{d_1}(\theta)\mathrm{sord}_{d_2}(\theta)$ holds for any coprime divisors d_1, d_2 of n, which completes the proof. □

From Lemmas 3.1.10 and 3.1.12, $|t\langle\theta\rangle_n|$ is odd if and only if $\mathrm{sord}_p(\theta)$ is odd for any prime factor p of $\frac{n}{\gcd(t,n)}$. Then we have the following theorem.

Theorem 3.1.16. *Let $n = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of an odd integer n, and for a unit $\theta \in \mathbb{Z}_n^+$, let $P_1 = \{p_i : -1 \notin (\theta)_{p_i}, 1 \le i \le r\}$, $P_2 = \{p_i : -1 \in (\theta)_{p_i}, 2 \nmid \mathrm{sord}_{p_i}(\theta), 1 \le i \le r\}$, $P_3 = \{p_i : -1 \in (\theta)_{p_i}, 2 \mid \mathrm{sord}_{p_i}(\theta), 1 \le i \le r\}$, and*

$$n_j = \prod_{p_i \in P_j} p_i^{e_i} \quad \text{for } j = 1, 2, 3,$$

where $n_j = 1$ if $P_j = \emptyset$. Thus $n = n_1 n_2 n_3$. If $\mathrm{sord}_{n_j}(\theta)$ is a multiplicative function with respect to n_j ($j \in \{1, 2\}$), then the number of disjoint odd cycles $t\langle\theta\rangle_n$ in Ω_n is

$$N(n_1) + N(n_2).$$

Proof: Note that (3.1.2) shows that the number of disjoint odd cycles $t\langle\theta\rangle_n$ in Ω_n is represented by the sum of $\frac{\varphi(d)}{\mathrm{sord}_d(\theta)}$'s for the divisors d of n for which $\mathrm{sord}_d(\theta)$ is odd. From Lemma 3.1.12, $\mathrm{sord}_d(\theta)$ is odd for any divisor d of n_j ($j \in \{1, 2\}$). Thus, by applying Lemma 3.1.14, the number of disjoint odd cycles is

$$\frac{1}{2}\Big(\sum_{d \mid n_1} \frac{\varphi(d)}{\mathrm{sord}_d(\theta)} + \sum_{d \mid n_2} \frac{\varphi(d)}{\mathrm{sord}_d(\theta)}\Big) - 1 = N(n_1) + N(n_2).$$

□

3.1.2 Order and suborder of 2 and 3

In this subsection, it is shown that, for specific units $\theta = 2$ and 3, it is impossible to determine the exact values of their multiplicative order and suborder.

By Euler's criterion and the second supplementary law of quadratic reciprocity, the following lemma is clear.

Lemma 3.1.17. *Let p be an odd prime. Then*

$$2^{\frac{p-1}{2}} \equiv \begin{cases} 1 \pmod{p} & \text{if } p \equiv 1 \text{ or } 7 \pmod{8} \\ -1 \pmod{p} & \text{if } p \equiv 3 \text{ or } 5 \pmod{8} \end{cases}$$

Corollary 3.1.18. *Let $n \geq 3$ be an odd integer. Then*

(i) *If $p \equiv 3 \pmod 8$ for any prime factor p of n, then $\mathrm{sord}_n(2)$ is odd.*

(ii) *If $p \equiv 7 \pmod 8$ for any prime factor p of n, then $\mathrm{sord}_n(2)$ is odd.*

(iii) *If n has a prime factor $p \equiv 5 \pmod 8$, then $\mathrm{sord}_n(2)$ is even.*

(iv) *If n has prime factors both $p \equiv 3 \pmod 8$ and $p \equiv 7 \pmod 8$, then $\mathrm{sord}_n(2)$ is even.*

Proof: (i) & (ii) By noting that $2^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$, we have $\mathrm{sord}_p(2) \mid \frac{p-1}{2}$. If $p \equiv 3$ or $7 \pmod 8$, then $\frac{p-1}{2}$ is odd. Thus $\mathrm{sord}_p(2)$ is odd. By Lemma 3.1.17, $-1 \in (2)_p$ and $v_2(\mathrm{sord}_p(2)) = 0$ if $p \equiv 3 \pmod 8$, and $-1 \notin (2)_p$ if $p \equiv 7 \pmod 8$. From Lemmas 3.1.11 and 3.1.12, $\mathrm{sord}_n(2)$ is odd.
(iii) If $p \equiv 5 \pmod 8$, then $\mathrm{sord}_p(2) \mid \frac{p-1}{2} = 2(2k+1)$ holds for some integer k. Suppose that $\mathrm{sord}_p(\theta)$ is odd (thus $\mathrm{sord}_p(\theta) \mid 2k+1$). Then $\theta^{\frac{p-1}{4}} \equiv -1 \pmod p$ since $\frac{p-1}{4} = 2k+1$ is odd. Thus $\theta^{\frac{p-1}{2}} \equiv 1 \pmod p$ holds, but this contradicts $2^{\frac{p-1}{2}} \equiv -1 \pmod p$ in Lemma 3.1.17. Hence $\mathrm{sord}_p(2)$ must be even. By Lemmas 3.1.11 and 3.1.12, if n has a prime factor p such that $\mathrm{sord}_p(2)$ is even, then $\mathrm{sord}_{p^e}(2)$ is even, and thus $\mathrm{sord}_n(2)$ is even since $\mathrm{sord}_{p^e}(2) \mid \mathrm{sord}_n(2)$.
(iv) By Lemma 3.1.17, $-1 \in (2)_p$ if $p \equiv 3 \pmod 8$, and $-1 \notin (2)_p$ if $p \equiv 7 \pmod 8$. Then it immediately follows from Lemma 3.1.12 that $\mathrm{sord}_n(2)$ is even. □

A *Wieferich prime* is a prime satisfying $2^{p-1} \equiv 1 \pmod{p^2}$. It is known due to Dorais [19] that there is no Wieferich prime $p < 6.7 \times 10^{15}$ other than

$p = 1093, 3511$ (see also [73]). Note that if p is a non-Wieferich prime, then $2^{p-1} + 1 \not\equiv 0 \pmod{p^2}$ since $2^{p-1} + 1 \equiv 2 \not\equiv 0 \pmod{p}$. Therefore, for a non-Wieferich prime p, $2^{\mathrm{sord}_p(2)} \not\equiv \pm 1 \pmod{p^2}$ holds, which implies that $v_p(2^{\mathrm{sord}_p(2)} \pm 1) = 1$.

Corollary 3.1.19. *Let N_1 and N_2 be multisets of odd non-Wieferich primes $p \equiv 3 \pmod 8$ and $p \equiv 7 \pmod 8$, respectively, and N_3 be a multiset of odd primes p with $p \equiv 5 \pmod 8$. Further let*

$$n_j = \prod_{p \in N_j} p \quad \text{for } j = 1, 2, 3$$

and $n = n_1 n_2 n_3$, where $n_j = 1$ if $N_j = \emptyset$. Assume that

(i) $\gcd(\varphi(p^e), \varphi(q^f))$ *is a power of 2 for any distinct prime factors p, q of n_j ($j \in \{1, 2\}$), where $e = v_p(n_j)$ and $f = v_q(n_j)$, and*

(ii) $\Omega_p = \langle 2 \rangle_p$ *for any prime factor p of $n_1 n_2$.*

Then the number of disjoint odd cycles $t\langle 2 \rangle_n$ in Ω_n for $t \in \mathbb{Z}_n^+$ is

$$N(n_1) + N(n_2) = \frac{1}{2}\Big\{\prod_{p|n_1}\big(1 + 2v_p(n_1)\big) + \prod_{p|n_2}\big(1 + 2v_p(n_2)\big)\Big\} - 1.$$

Proof: It follows from Corollary 3.1.18(i) and (ii) that both of $\mathrm{sord}_{n_1}(2)$ and $\mathrm{sord}_{n_2}(2)$ are odd. Then, from Lemma 3.1.15, we know that $\mathrm{sord}_{n_j}(2)$ is a multiplicative function with respect to n_j ($j \in \{1, 2\}$). Note that $v_p(2^{\mathrm{sord}_p(2)} \pm 1) = 1$ for any non-Wieferich prime p. Since the assumption $\Omega_p = \langle 2 \rangle_p$ for any prime factor p of $n_1 n_2$ implies that $\mathrm{sord}_p(2) = \frac{p-1}{2}$, the assertion can be immediately proved by Theorem 3.1.16. □

Example 3.1.20. The case when $n = 11 \cdot 7^2 = 539$. For any $t \in \mathbb{Z}_{539}^+$, $t\langle 2 \rangle_{539}$ is congruent to one of $\langle 2 \rangle_{539}$, $7\langle 2 \rangle_{539}$, $11\langle 2 \rangle_{539}$, $49\langle 2 \rangle_{539}$ and $77\langle 2 \rangle_{539}$. In this case, the lengths of the cycles are as follows:

$$\begin{aligned}
&|\langle 2 \rangle_{539}| = \mathrm{sord}_{539}(2) = 210, \ |7\langle 2 \rangle_{539}| = \mathrm{sord}_{77}(2) = 30, \\
&|11\langle 2 \rangle_{539}| = \mathrm{sord}_{49}(2) = 21, \ |49\langle 2 \rangle_{539}| = \mathrm{sord}_{11}(2) = 5, \\
&|77\langle 2 \rangle_{539}| = \mathrm{sord}_{7}(2) = 3.
\end{aligned}$$

It is readily verified that the number of disjoint odd cycles $t\langle 2 \rangle_{539}$ is consistent with $N(11) + N(7^2) = \frac{1}{2}(3 + 5) - 1 = 3$ in Corollary 3.1.19.

Corollary 3.1.21. *Under the same assumption as in Corollary 3.1.19, if N_1 and N_2 are non-multisets, then*

$$N(n_1) + N(n_2) = \frac{1}{2}\big(3^{e_1} + 3^{e_2}\big) - 1$$

holds, where $e_j = |N_j|$ for $j = 1, 2$.

Example 3.1.22. The case when $n = 3{\cdot}7{\cdot}5 = 105$. For any $t \in \mathbb{Z}^+_{105}$, $t\langle 2\rangle_{105}$ is congruent to one of $\langle 2\rangle_{105}$, $3\langle 2\rangle_{105}$, $11\langle 2\rangle_{105}$, $5\langle 2\rangle_{105}$, $7\langle 2\rangle_{105}$, $15\langle 2\rangle_{105}$, $21\langle 2\rangle_{105}$ and $35\langle 2\rangle_{99}$. In this case, the lengths of the cycles are as follows:

$$\begin{aligned}
&|\langle 2\rangle_{105}| = \mathrm{sord}_{105}(2) = 12,\ |3\langle 2\rangle_{105}| = \mathrm{sord}_{35}(2) = 12,\\
&|11\langle 2\rangle_{105}| = \mathrm{sord}_{105}(2) = 12,\ |5\langle 2\rangle_{105}| = \mathrm{sord}_{21}(2) = 6,\\
&|7\langle 2\rangle_{105}| = \mathrm{sord}_{15}(2) = 4,\ |15\langle 2\rangle_{105}| = \mathrm{sord}_{7}(2) = 3,\\
&|21\langle 2\rangle_{105}| = \mathrm{sord}_{5}(2) = 2,\ |35\langle 2\rangle_{99}| = \mathrm{sord}_{3}(2) = 1.
\end{aligned}$$

Then it turns out that the number of disjoint odd cycles $t\langle 2\rangle_{105}$ is consistent with $N(3) + N(7) = \frac{1}{2}(3+3) - 1 = 2$ in Corollary 3.1.21.

Corollary 3.1.23. *Let $m = \prod_{i=1}^{r} p_i^{e_i}$ be the prime factorization of an odd integer m indivisible by 3. Let $P = \{p_i : -1 \in (2)_{p_i}, 1 \le i \le r\}$ and $\bar{P} = \{p_i : -1 \notin (2)_{p_i}, 1 \le i \le r\}$. Then*

$$\mathrm{sord}_{3m}(2) = \begin{cases} 2\mathrm{sord}_m(2) & \text{if } P = \emptyset, \text{ or } \bar{P} = \emptyset \text{ and } v_2(\mathrm{sord}_{p_i}(2)) \text{ is} \\ & \text{a non-zero constant for any } 1 \le i \le r, \\ \mathrm{sord}_m(2) & \text{otherwise.} \end{cases}$$

Proof: Note that $\mathrm{sord}_3(2) = 1$ and $-1 \in (2)_3$. Applying Lemma 3.1.12, we have

$$\begin{aligned}
\mathrm{sord}_{3m}(2) &= \alpha_1 \,\mathrm{lcm}\big(\mathrm{sord}_3(2), \mathrm{sord}_{p_1^{e_1}}(2), \mathrm{sord}_{p_2^{e_2}}(2), \ldots, \mathrm{sord}_{p_r^{e_r}}(2)\big)\\
&= \alpha_1 \,\mathrm{lcm}\big(\mathrm{sord}_{p_1^{e_1}}(2), \mathrm{sord}_{p_2^{e_2}}(2), \ldots, \mathrm{sord}_{p_r^{e_r}}(2)\big)
\end{aligned}$$

and

$$\mathrm{sord}_m(2) = \alpha_2 \,\mathrm{lcm}\big(\mathrm{sord}_{p_1^{e_1}}(2), \mathrm{sord}_{p_2^{e_2}}(2), \ldots, \mathrm{sord}_{p_r^{e_r}}(2)\big),$$

where

$$\alpha_1 = \begin{cases} 1 & \text{if } \bar{P} = \emptyset \text{ and } v_2(\mathrm{sord}_{p_i}(2)) = 0 \text{ for any } 1 \le i \le r, \\ 2 & \text{otherwise,} \end{cases}$$

and

$$\alpha_2 = \begin{cases} 1 & \text{if } P = \emptyset, \text{ or } \bar{P} = \emptyset \text{ and } v_2(\mathrm{sord}_{p_i}(2))\text{'s are the same for } 1 \le i \le r, \\ 2 & \text{otherwise.} \end{cases}$$

By noting $\mathrm{sord}_{3m}(2) = \frac{\alpha_1}{\alpha_2}\mathrm{sord}_m(2)$, then the assertion can be proved. $\square$

In the rest of this section, we consider the case: $\theta = 3$.

Lemma 3.1.24. *For $k \geq 0$, $\mathrm{sord}_{2^{k+2}}(3) = 2^k$ holds. Further, if $k \geq 1$, then $\mathrm{sord}_{2^{k+2}}(3) = \mathrm{ord}_{2^{k+2}}(3)$ holds.*

Proof: Since $3 \equiv -1 \pmod{2^2}$ and $3^2 \equiv 1 \pmod{2^2}$, the assertion is true when $k = 0$. For $k \geq 1$, we first show by induction that

$$3^{2^k} - 1 = 2^{k+2} h_k \tag{3.1.3}$$

holds for $k \geq 1$, where $h_1 = 1$ and

$$h_k = h_{k-1}(2^k h_{k-1} + 1) \quad \text{for } k \geq 2.$$

When $k = 1$, it is obvious that (3.1.3) is true. Now, suppose that (3.1.3) holds for some $k \geq 1$. Then, it follows that

$$\begin{aligned} 3^{2^{k+1}} - 1 &= (3^{2^k} - 1)^2 + 2(3^{2^k} - 1) = (2^{k+2} h_k)^2 + 2(2^{k+2} h_k) \\ &= 2^{2k+4} h_k^2 + 2^{k+3} h_k = 2^{k+3} h_k \left(2^{k+1} h_k + 1\right) \\ &= 2^{k+3} h_{k+1}, \end{aligned}$$

which shows that (3.1.3) holds for $k+1$ and thus (3.1.3) is true for any $k \geq 1$.

Note that (3.1.3) implies that $s = \mathrm{sord}_{2^{k+2}}(3)$ is a divisor of 2^k. Let $s = 2^i$ for some positive integer $i < k$. Since it is easy to see that h_i is odd for any $i \geq 1$, $3^{2^i} - 1 = 2^{i+2} h_i$ cannot be divided by 2^{k+2}. Thus, $3^{2^i} \not\equiv 1 \pmod{2^{k+2}}$ for any $1 \leq i < k$, which implies that $\mathrm{ord}_{2^{k+2}}(3) = 2^k$ holds for $k \geq 1$.

Here, let $h_i = 2^{k-i} q_i + r_i$ for $1 \leq r_i \leq 2^{k-i} - 1$. Then we have

$$3^{2^i} + 1 = 3^{2^i} - 1 + 2 = 2^{i+2} h_i + 2 \equiv 2^{i+2} r_i + 2 \pmod{2^{k+2}}.$$

Since $1 < 2^{i+2} r_i + 2 \leq 2^{k+2} - 2^{i+2} + 2 < 2^{k+2} - 1$ for $1 \leq i < k$, $3^{2^i} + 1 \not\equiv 0 \pmod{2^{k+2}}$ holds for any $1 \leq i < k$. This shows that $s = \mathrm{sord}_{2^{k+2}}(3) = \mathrm{ord}_{2^{k+2}}(3) = 2^k$ for any $k \geq 1$. □

Lemma 3.1.25. *For $k \geq 0$ and $m \geq 5$ with $\gcd(m, 6) = 1$, let $t_k = \mathrm{sord}_{2^k m}(3)$. Then $t_1 = t_0$,*

$$t_2 = \begin{cases} t_0 & \text{if } v_2(\mathrm{ord}_m(3)) = 1, \text{ or } v_2(\mathrm{ord}_m(3)) \geq 2 \text{ and } -1 \notin (3)_m, \\ 2t_0 & \text{otherwise,} \end{cases}$$

and for $k \geq 3$,

$$t_k = \begin{cases} t_{k-1} & \text{if } k = 3 \text{ and } t_2 \text{ is even, or } 4 \leq k \leq v_2(\mathrm{ord}_m(3)) + 2, \\ 2t_{k-1} & \text{otherwise.} \end{cases}$$

Proof: It is obvious that $3^{t_0} \equiv \pm 1 \pmod 2$. Since $\gcd(m, 2) = 1$, we have $3^{t_0} \equiv \pm 1 \pmod{2m}$, which implies that $t_1 = t_0$.

Next, we consider the relation between t_0 and t_2 in three cases.

(i) The case when $v_2(\mathrm{ord}_m(3)) = 0$. Then $-1 \notin (3)_m$ and $t_0 = \mathrm{ord}_m(3)$ is odd. Note that

$$t_0 \mid t_2 \mid \mathrm{ord}_{4m}(3) = \mathrm{lcm}(\mathrm{ord}_4(3), \mathrm{ord}_m(3)) = 2\,\mathrm{ord}_m(3) = 2t_0.$$

If $-1 \in (3)_{4m}$, then $3^{t_0} \equiv -1 \pmod{4m}$, which implies that $3^{t_0} \equiv -1 \pmod m$ must hold. However, this contradicts $-1 \notin (3)_m$. Thus $-1 \notin (3)_{4m}$. Then we have $t_2 = 2t_0$.

(ii) The case when $v_2(\mathrm{ord}_m(3)) = 1$. If $-1 \in (3)_m$, then t_0 is odd since $\mathrm{ord}_m(3) = 2t_0$. Since $3 \equiv -1 \pmod 4$, $3^{t_0} \equiv -1 \pmod 4$ holds if t_0 is odd. Thus $3^{t_0} \equiv -1 \pmod{4m}$, which implies that $t_2 = t_0$ is odd. If $-1 \notin (3)_m$, then $t_0 = \mathrm{ord}_m(3)$ is even. Thus $t_2 = t_0$ is even since $t_0 \mid t_2 \mid \mathrm{ord}_{4m}(3) = \mathrm{ord}_m(3)$.

(iii) The case when $v_2(\mathrm{ord}_m(3)) \geq 2$. Since

$$t_0 \mid t_2 \mid \mathrm{ord}_{4m}(3) = \mathrm{lcm}(\mathrm{ord}_4(3), \mathrm{ord}_m(3)) = \mathrm{ord}_m(3)$$

and $v_2(t_0) \geq v_2(\mathrm{ord}_m(3)) - 1$, t_2 must be even. Note that $3^{t_2} \equiv -1 \pmod 4$ holds only if t_2 is odd. Then $-1 \notin (3)_{4m}$ since t_2 is even. Thus $t_2 = \mathrm{ord}_{4m}(3) = \mathrm{ord}_m(3)$ holds. Obviously $\mathrm{ord}_m(3) = t_0$ or $2t_0$ depending on whether $-1 \notin (3)_m$ or not. Thus

$$t_2 = \begin{cases} t_0 & \text{if } -1 \notin (3)_m, \\ 2t_0 & \text{if } -1 \in (3)_m. \end{cases}$$

Finally, we consider the relation between t_k and t_{k-1} for $k \geq 3$. If $-1 \in (3)_{2^k m}$, then $3^{t_k} \equiv -1 \pmod{2^k m}$ holds, and thus $3^{t_k} \equiv -1 \pmod{2^k}$, which contradicts Lemma 3.1.24, that is, $-1 \notin (3)_{2^k}$ for $k \geq 3$. Therefore $-1 \notin (3)_{2^k m}$ for $k \geq 3$, and it follows from Lemmas 3.1.24 and 3.1.9 that

$$t_k = \mathrm{sord}_{2^k m}(3) = \mathrm{ord}_{2^k m}(3) = \mathrm{lcm}(2^{k-2}, \mathrm{ord}_m(3)).$$

Then, for $k \geq 4$,

$$t_k = \begin{cases} t_{k-1} & \text{if } v_2(\mathrm{ord}_m(3)) \geq k - 2, \\ 2t_{k-1} & \text{otherwise.} \end{cases}$$

From the preceding discussion, we know that $t_3 = \mathrm{lcm}(2, \mathrm{ord}_m(3))$. If $-1 \in (3)_{4m}$, then we have

$$2t_2 = \mathrm{ord}_{4m}(3) = \mathrm{lcm}(\mathrm{ord}_4(3), \mathrm{ord}_m(3)) = \mathrm{lcm}(2, \mathrm{ord}_m(3)) = t_3,$$

$3^{t_2} \equiv -1 \pmod{4m}$ and thus $3^{t_2} \equiv -1 \pmod 4$, which implies that t_2 is odd since $\mathrm{sord}_4(3) = 1$. Meanwhile, if $-1 \notin (3)_{4m}$, then

$$t_2 = \mathrm{sord}_{4m}(3) = \mathrm{ord}_{4m}(3) = \mathrm{lcm}(2, \mathrm{ord}_m(3)) = t_3,$$

which is even. Hence the proof is completed. □

Corollary 3.1.26. *For $m \geq 5$ with $\gcd(m, 6) = 1$, let $t_k = \mathrm{sord}_{2^k m}(3)$ and $u = v_2(t_2) + 2$. Then, for $k \geq 3$,*

$$t_k = \begin{cases} t_{k-1} & \text{if } k \leq u, \\ 2t_{k-1} & \text{if } k > u. \end{cases}$$

Proof: By Lemma 3.1.25, the following holds.

(i) When $v_2(\mathrm{ord}_m(3)) = 0$, we have $t_2 = 2t_0$ and $v_2(t_2) = 1$. Thus

$$t_0 = t_1 < t_2 = t_3 < t_4 < t_5 < \cdots < 2^{-a+2}t_a,$$

that is, $t_0 = t_1 = 2^{-1}t_2 = 2^{-1}t_3 = 2^{-2}t_4 = 2^{-3}t_5 = \cdots = 2^{-a+2}t_a$.

(ii) When $v_2(\mathrm{ord}_m(3)) = 1$, if $-1 \in (3)_m$, then $t_2 = t_0$ is odd and $v_2(t_2) = 0$. Thus

$$t_0 = t_1 = t_2 < t_3 < t_4 < t_5 < \cdots < t_a,$$

that is, $t_0 = t_1 = t_2 = 2^{-1}t_3 = 2^{-2}t_4 = 2^{-3}t_5 = \cdots = 2^{-a+2}t_a$. If $-1 \notin (3)_m$, then $t_2 = t_0$ is even and $v_2(t_2) = 1$. Thus

$$t_0 = t_1 = t_2 = t_3 < t_4 < t_5 < \cdots < t_a,$$

that is, $t_0 = t_1 = t_2 = t_3 = 2^{-1}t_4 = 2^{-2}t_5 = \cdots = 2^{-a+3}t_a$.

(iii) When $v_2(\mathrm{ord}_m(3)) \geq 2$, we have $v_2(\mathrm{ord}_m(3)) = v_2(t_2)$ and for $u = v_2(t_2) + 2$,

$$\begin{cases} t_0 = t_1 < t_2 = t_3 = \cdots = t_u < t_{u+1} < \cdots < t_a & \text{if } -1 \in (3)_m, \\ t_0 = t_1 = t_2 = t_3 = \cdots = t_u < t_{u+1} < \cdots < t_a & \text{if } -1 \notin (3)_m \end{cases}$$

holds, that is, $t_0 = t_1 = 2^{-1}t_2 = 2^{-1}t_3 = \cdots = 2^{-1}t_u = 2^{-2}t_{u+1} = \cdots = 2^{-a+u-1}t_a$ or $t_0 = t_1 = t_2 = t_3 = \cdots = t_u = 2^{-1}t_{u+1} = \cdots = 2^{-a+u}t_a$ holds, respectively.

Then the assertion follows from (i)–(iii). □

3.1.3 Order and suborder of units in $\mathbb{Z}_n$ for n defined by cyclotomic polynomials

For a given unit $\theta(\neq 1) \in \mathbb{Z}_n^+$, finding $\mathrm{ord}_n(\theta)$ is a challenging problem in general. In this subsection, we will show that if n is defined by cyclotomic polynomials, then it is possible to determine $\mathrm{ord}_n(\theta)$.

For $m \in \mathbb{N}$, let $\Phi_m(x)$ be the mth cyclotomic polynomial, defined by

$$\Phi_m(x) = \prod_{d|m} (x^d - 1)^{\mu(\frac{m}{d})},$$

where $\mu(n)$ is the Möbius function, that is, the minimal polynomial over $\mathbb{Q}$ having exactly the primitive mth roots of unity as its roots. It is known that the coefficients of the cyclotomic polynomials are integers and

$$x^m - 1 = \prod_{d|m} \Phi_d(x)$$

holds.

In order to present a relation between cyclotomic polynomials and multiplicative order, we revisit a couple of basic results on cyclotomic polynomials.

Proposition 3.1.27. *For $m \in \mathbb{N}$ and a prime p,*

$$\Phi_m(x^p) = \begin{cases} \Phi_{pm}(x) & \text{if } p \mid m, \\ \Phi_{pm}(x)\Phi_m(x) & \text{if } p \nmid m. \end{cases}$$

Lemma 3.1.28. *For $m \in \mathbb{N} \setminus \{1\}$ and $k \in \mathbb{N}$, let k' be the maximum divisor of k satisfying $\gcd(k', m) = 1$, and let $s = \frac{k}{k'}$. Then*

$$\Phi_m(x^k) = \Phi_{sm}(x^{k'}) = \prod_{t|k'} \Phi_{tsm}(x).$$

Proof: Let $s = \prod_{i=1}^{u} p_i$, where p_i's are not necessarily distinct primes. Applying the first case of Proposition 3.1.27 recursively to $p_1, p_2, \ldots, p_u$, the first equality can be proved. Furthermore, let $k' = \prod_{i=1}^{v} q_i$, where q_i's are not necessarily distinct primes. Since $\gcd(k', sm) = 1$, by applying the second case of Proposition 3.1.27 recursively to $q_1, q_2, \ldots, q_v$, we have the last equality. □

Proposition 3.1.29 ([17, p. 388]). *Let $n \in \mathbb{N}$ and $m, \theta \in \mathbb{N} \setminus \{1\}$. Then $\Phi_m(\theta)$ has a prime factor not dividing $\theta^n - 1$ for any $n < m$ except in the cases $(m, \theta) = (6, 2), (2, 2^f - 1)$ for $f \in \mathbb{N}$; whence $\theta^m - 1$ has a prime factor not dividing $\theta^n - 1$ for any $n < m$ except in those cases.*

Proposition 3.1.29 implies that, for $m, \theta \in \mathbb{N} \setminus \{1\}$, $\Phi_m(\theta)$ has a prime factor p such that $\mathrm{ord}_p(\theta) = m$ except in the cases $(m, \theta) = (6, 2), (2, 2^f - 1)$ for $f \geq 1$. Then we can state the following:

Theorem 3.1.30. *Let $k \in \mathbb{N}$ and $m, \theta \in \mathbb{N} \setminus \{1\}$ with $(k, m, \theta) \neq (1, 6, 2)$. Then*

$$\mathrm{ord}_{\Phi_{km}(\theta)}(\theta) = \mathrm{ord}_{\Phi_m(\theta^k)}(\theta) = km$$

holds. If m is even, then

$$\mathrm{sord}_{\Phi_{km}(\theta)}(\theta) = \mathrm{sord}_{\Phi_m(\theta^k)}(\theta) = \frac{km}{2}$$

holds. In the case of $(k, m, \theta) = (1, 6, 2)$, $\mathrm{ord}_{\Phi_6(2)}(2) = 2$ and $\mathrm{sord}_{\Phi_6(2)}(2) = 1$ hold.

Proof: Since $\Phi_{km}(x) \mid \Phi_m(x^k) \mid (x^{km} - 1)$, for any prime factor p in $\Phi_{km}(\theta)$,

$$p \mid \Phi_{km}(\theta) \mid \Phi_m(\theta^k) \mid \theta^{km} - 1$$

holds, which implies that

$$\mathrm{ord}_p(\theta) \mid \mathrm{ord}_{\Phi_{km}(\theta)}(\theta) \mid \mathrm{ord}_{\Phi_m(\theta^k)}(\theta) \mid km.$$

Proposition 3.1.29 claims that $\Phi_{km}(\theta)$ has a prime factor p such that $\mathrm{ord}_p(\theta) = km$ if $(k, m, \theta) \notin \{(1, 6, 2), (2, 3, 2), (3, 2, 2)\} \cup \{(1, 2, 2^f - 1) : f \geq 1\}$. Thus we have

$$\mathrm{ord}_{\Phi_{km}(\theta)}(\theta) = \mathrm{ord}_{\Phi_m(\theta^k)}(\theta) = km.$$

If m is even, then $\Phi_m(\theta^k) \mid (\theta^{\frac{km}{2}} - 1)$ or $\Phi_m(\theta^k) \mid (\theta^{\frac{km}{2}} + 1)$ must hold since $\Phi_m(\theta^k) \mid (\theta^{km} - 1) = (\theta^{\frac{km}{2}} - 1)(\theta^{\frac{km}{2}} + 1)$. Noting that, for $(k, m, \theta) \notin \{(1, 6, 2), (2, 3, 2), (3, 2, 2)\} \cup \{(1, 2, 2^f - 1) : f \geq 1\}$, $\Phi_m(\theta^k)$ does not divide $\theta^{\frac{km}{2}} - 1$ since $\mathrm{ord}_{\Phi_m(\theta^k)}(\theta) = km$, we have $\Phi_m(\theta^k) \mid (\theta^{\frac{km}{2}} + 1)$, that is, $\theta^{\frac{km}{2}} \equiv -1 \pmod{\Phi_m(\theta^k)}$. Thus $-1 \in (\theta)_{\Phi_m(\theta^k)}$. Then the second assertion of the lemma is proved by Lemma 3.1.2.

Now we examine the case $(k, m, \theta) \in \{(1, 6, 2), (2, 3, 2), (3, 2, 2)\} \cup \{(1, 2, 2^f - 1) : f \geq 1\}$.

If $(k,m,\theta) \in \{(1,2,2^f-1) : f \geq 1\}$, then we have $\Phi_m(\theta^k) = \Phi_2(2^f-1) = (2^f-1)+1 = 2^f$ and $\mathrm{ord}_{\Phi_m(\theta^k)}(\theta) = \mathrm{ord}_{2^f}(2^f-1) = 2 = m$ since $(2^f-1)^2 \equiv 1 \pmod{2^f}$.

If $(k,m,\theta) \in \{(2,3,2),(3,2,2)\}$, then from Lemma 3.1.28 and the fact that $\Phi_6(2) = \Phi_2(2) = 3$, we have $\Phi_3(2^2) = \Phi_3(2)\Phi_6(2) = \Phi_3(2)\Phi_2(2) = 21$ and $\Phi_2(2^3) = \Phi_2(2)\Phi_6(2) = \Phi_2(2)^2 = 9$, respectively. Note that $\mathrm{ord}_{21}(2) = \mathrm{sord}_{21}(2) = 6 = km$, $\mathrm{ord}_9(2) = 6 = km$ and $\mathrm{sord}_9(2) = 3 = \frac{km}{2}$. Then, from the argument above, it turns out that the case $(k,m,\theta) \in \{(2,3,2),(3,2,2)\} \cup \{(1,2,2^f-1) : f \geq 1\}$ is consistent with the assertion of the lemma.

As for the case when $(k,m,\theta) = (1,6,2)$, $\Phi_m(\theta^k)$ can be directly computed as $\Phi_6(2) = 2^2-2+1 = 3$. Since $\mathrm{ord}_{\Phi_6(2)}(2) = \mathrm{ord}_3(2) = 2$ and $\mathrm{sord}_{\Phi_6(2)}(2) = \mathrm{sord}_3(2) = 1$, this completes the proof. □

The following theorem is useful for giving a series of optimal (not necessarily tight) codes in $\mathrm{CAC}^e(n,3)$ for odd n.

Theorem 3.1.31. *For mutually distinct $m_i \in \mathbb{N} \setminus \{1\}$, $1 \leq i \leq r$, and $\theta \in \mathbb{N} \setminus \{1\}$, let $n = \prod_{i=1}^r \Phi_{m_i}(\theta)$ and $m = \mathrm{lcm}(m_1, m_2, \ldots, m_r)$. Then, $\mathrm{ord}_n(\theta) = \delta m$, where*

$$\delta = \begin{cases} \frac{1}{3} & \text{if } m_j = 6 \text{ for some } j,\ 3 \nmid \prod_{i=1, i\neq j}^r m_i \text{ and } \theta = 2, \\ 1 & \text{otherwise.} \end{cases}$$

Moreover, if all m_i's are even and $v_2(m_i)$'s are the same, then $\mathrm{sord}_n(\theta) = \frac{\delta m}{2}$.

Proof: The proof of the first assertion is divided into two cases: (i) $m_i \neq 6$ for any i or $\theta \neq 2$, and (ii) $m_j = 6$ for some j and $\theta = 2$. Let $\ell = \mathrm{ord}_n(\theta)$ and $m = \mathrm{lcm}(m_1, m_2, \ldots, m_r)$.

(i) Since $\theta^m - 1 = \prod_{d|m} \Phi_d(\theta) = nq(\theta)$, where $q(\theta) = \frac{\prod_{d|m} \Phi_d(\theta)}{n}$, we have $\theta^m \equiv 1 \pmod{n}$ and then $\ell \mid m$. Suppose that $\ell < m$. That is, there is at least one m_i such that $m_i \nmid \ell$. Let $\ell = s_i m_i + r_i$ for $0 < r_i < m_i$. Then $1 \equiv \theta^\ell = \theta^{s_i m_i} \theta^{r_i} \equiv \theta^{r_i} \pmod{\Phi_{m_i}(\theta)}$, which contradicts Theorem 3.1.30, that is, $\mathrm{ord}_{\Phi_{m_i}(\theta)}(\theta) = m_i$. Hence $\ell = m$.

(ii) Without loss of generality, suppose that $m_1 = 6$. Since $\Phi_6(2) = 3 = \Phi_2(2)$, $n = \Phi_6(2) \prod_{i=2}^r \Phi_{m_i}(2) = \Phi_2(2) \prod_{i=2}^r \Phi_{m_i}(2)$ holds. Then $\mathrm{ord}_n(2) = \mathrm{lcm}(2, m_2, \ldots, m_r)$ follows from the case (i) and it is easy to see that

$$\mathrm{lcm}(2, m_2, \ldots, m_k) = \begin{cases} \frac{1}{3}\mathrm{lcm}(m_1 = 6, m_2, \ldots, m_k) & \text{if } 3 \nmid \prod_{i=2}^r m_i, \\ \mathrm{lcm}(m_1 = 6, m_2, \ldots, m_k) & \text{otherwise.} \end{cases}$$

Hence, the first assertion is proved.

Now we will prove the second assertion. In what follows, if $\theta = 2$ and n has $\Phi_6(2)$ as its factor, then $\Phi_6(2)$ is replaced by $\Phi_2(2)$ for simplicity (thus we may consider $\delta = 1$ invariably). If $\mathrm{sord}_n(\theta) = \frac{m}{2}$, then $\theta^{\frac{m}{2}} + 1 \equiv 0 \pmod{n}$ must hold, which implies that

$$\theta^{\frac{m}{2}} + 1 \equiv 0 \pmod{\Phi_{m_i}(\theta)} \tag{3.1.4}$$

for $1 \leq i \leq r$. On the other hand, m_i must be even for

$$\theta^{\frac{m_i}{2}} + 1 \equiv 0 \pmod{\Phi_{m_i}(\theta)} \tag{3.1.5}$$

to hold. Let $m = m_i L_i$, that is, let $L_i = \mathrm{lcm}(m_1, m_2, \ldots, m_r)/m_i$. Note that, if m_i is even, then the exponent of θ in (3.1.4) is factorized as

$$\frac{m}{2} = \frac{m_i}{2} \cdot L_i.$$

For (3.1.4) and (3.1.5) to hold simultaneously, L_i needs to be odd for any i. This implies that $v_2(m_i)$'s must be the same, which proves the second assertion of the theorem. It should be noted that if $\theta = 2$ and n has $\Phi_6(2)$ as its factor, then m in the proof of the second assertion should be read as $\frac{m}{3}$. □

Example 3.1.32. (1) The case when $\theta = 2$, $r = 3$ and $(m_1, m_2, m_3) = (6, 2, 10)$ in Theorem 3.1.31. Since $\Phi_6(2) = \Phi_2(2) = 3$ and $\Phi_{10}(2) = 11$, we have $n = \Phi_2(2)\Phi_6(2)\Phi_{10}(2) = 99$. It is straightforward to check that $\mathrm{ord}_{99}(2) = 30 = \mathrm{lcm}(m_1, m_2, m_3)$ and $-1 \in (2)_{99}$. In fact, $v_2(m_1) = v_2(m_2) = v_2(m_3) = 2$ and $\mathrm{sord}_{99}(2) = 15$.

(2) The case when $\theta = 2$, $r = 2$ and $(m_1, m_2) = (3, 9)$ in Theorem 3.1.31. Since $\Phi_3(2) = 7$ and $\Phi_9(2) = 73$, we have $n = \Phi_3(2)\Phi_9(2) = 511$. By a short calculation, it is verified that $\mathrm{ord}_{511}(2) = 9 = \mathrm{lcm}(m_1, m_2)$ and $-1 \notin (2)_{511}$. Thus $\mathrm{sord}_{511}(2) = \mathrm{ord}_{511}(2) = 9$.

(3) The case when $\theta = 2$, $r = 3$ and $(m_1, m_2, m_3) = (3, 5, 8)$ in Theorem 3.1.31. Since $\Phi_3(2) = 7$, $\Phi_5(2) = 31$ and $\Phi_8(2) = 17$, we have $n = \Phi_3(2)\Phi_5(2)\Phi_8(2) = 3689$. In this case, $\mathrm{ord}_{3689}(2) = 120 = \mathrm{lcm}(m_1, m_2, m_3)$ and $-1 \notin (2)_{3689}$. Thus $\mathrm{sord}_{3689}(2) = 120$.

3.2 Optimal equi-difference conflict-avoiding codes of odd length and weight three

In this section, we present some explicit series of tight equi-difference CACs of odd length and weight three by using the properties of the multiplicative suborder obtained in Section 3.1 and the recursive construction due to Momihara et al. [60].

Before presenting the main theorems, we clarify the reason why the multiplicative order of 2 modulo n is concerned in the existence of tight/optimal codes in $\mathrm{CAC}^e(n,3)$ in Subsection 3.2.1. Applying the properties of the multiplicative order, some series of code lengths of tight equi-difference CAC are given in Subsection 3.2.2. In Subsection 3.2.3, we derive a calculation formula for $M^e(n,4)$ in the case when an optimal equi-difference CAC is not necessarily tight.

3.2.1 Graph representation for codes in $\mathbf{CAC}^e(n,3)$

Let $G(\Omega_n)$ be a graph with the vertex set $\Omega_n = \{1,2,\ldots,\lfloor \frac{n}{2} \rfloor\}$ and the edge set $E = \{(x,y) \in \Omega_n^2 : y \equiv \pm 2x \pmod{n}\}$. It is known due to Fu et al. [29] that, if n is odd, then the graph $G(\Omega_n)$ can be decomposed into disjoint cycles $t\langle 2\rangle_n$ for some distinct integers $t \in \Omega_n$.

Theorem 3.2.1 ([29, Lemma 2(iii)]). *Let $n \geq 3$ be an odd integer and $s_d = \mathrm{sord}_d(2)$. Then $G(\Omega_n)$ is decomposed into*

$$\sum_{\substack{d \mid n \\ d \neq 1}} \frac{\varphi(d)}{2s_d}$$

disjoint cycles including a loop if it exists, where for each divisor $d \neq 1$ of n, the number of s_d-cycles is $\frac{\varphi(d)}{2s_d}$.

When $3 \mid n$, $G(\Omega_n)$ contains the single loop $\frac{n}{3}\langle 2\rangle_n = (\frac{n}{3})$. Since any codeword in $\mathcal{C} \in \mathrm{CAC}^e(n,3)$ is of form $\{0,i,2i\}$,

$$|\Delta_2(\{0,i,2i\})| = \begin{cases} 2 & \text{if } i \neq \frac{n}{3}, \\ 1 & \text{if } 3 \mid n \text{ and } i = \frac{n}{3} \end{cases}$$

holds. Thus $\mathcal{C}$ is a tight code if and only if any cycle in $G(\Omega_n)$ is an even cycle or the loop $(\frac{n}{3})$.

In fact, it can be seen in [29] that the conditions for $|t\langle\theta\rangle_n|$ to be even in Lemmas 3.1.3 and 3.1.5 are necessary and sufficient for the existence of a tight code in $\mathrm{CAC}^e(n,3)$ since $4 \mid \mathrm{ord}_p(\theta)$ implies $p \equiv 1 \pmod 4$ for a prime p.

Theorem 3.2.2 ([29, Theorem 4]). *A tight code $\mathcal{C} \in \mathrm{CAC}^e(n,3)$ exists if and only if $n(\geq 3)$ is of form $n = 3^f n_0$ for $f \in \{0,1\}$ and any prime factor p of n_0 satisfies $p \equiv 1 \pmod 4$.*

Example 3.2.3. (1) The case when $n = 5{\cdot}13 = 65$. As in Example 3.1.7(1), $G(65)$ is decomposed into the six cycles

$$\begin{aligned}&\langle 2\rangle_{65} = (1,2,4,8,16,32),\ 3\langle 2\rangle_{65} = (3,6,12,24,17,31),\\ &5\langle 2\rangle_{65} = (5,10,20,25,15,30),\ 7\langle 2\rangle_{65} = (7,14,28,9,18,29),\\ &11\langle 2\rangle_{65} = (11,22,21,23,19,27),\ 13\langle 2\rangle_{65} = (13,26).\end{aligned}$$

From these cycles, a tight equi-difference CAC of length 65 and weight 3 is derived as the set of codewords

$$\begin{aligned}\big\{&\{0,1,2\},\ \{0,4,8\},\ \{0,16,32\},\ \{0,3,6\},\ \{0,12,24\},\ \{0,17,34\},\\ &\{0,5,10\},\ \{0,20,40\},\ \{0,15,30\},\ \{0,7,14\},\ \{0,28,56\},\ \{0,18,36\},\\ &\{0,11,22\},\ \{0,21,42\},\ \{0,19,38\},\ \{0,13,26\}\big\}.\end{aligned}$$

(2) The case when $n = 3{\cdot}17 = 51$. As in Example 3.1.7(2), $G(51)$ is decomposed into the five cycles

$$\begin{aligned}&\langle 2\rangle_{51} = (1,2,4,8,16,19,13,25),\ 5\langle 2\rangle_{51} = (5,10,20,11,22,7,14,23),\\ &3\langle 2\rangle_{51} = (3,6,12,24),\ 9\langle 2\rangle_{51} = (9,18,15,21),\ 17\langle 2\rangle_{51} = (17).\end{aligned}$$

Then, a tight equi-difference CAC of length 51 and weight 3 is given as

$$\begin{aligned}\big\{&\{0,1,2\},\ \{0,4,8\},\ \{0,16,32\},\ \{0,13,26\},\\ &\{0,5,10\},\ \{0,20,40\},\ \{0,22,44\},\ \{0,14,28\},\\ &\{0,3,6\},\ \{0,12,24\},\ \{0,9,18\},\ \{0,15,30\},\ \{0,17,34\}\big\}.\end{aligned}$$

Remark 3.2.4. In general, if $X = (x_1, x_2, \ldots, x_s)$ is a cycle in $G(\Omega_n)$, then for any odd $t \in \mathbb{N}$, $tX = (tx_1, tx_2, \ldots, tx_s)$ is also a cycle of the same length in $G(t\Omega_n)$. This means that there is an injection from each cycle in $G(\Omega_n)$ to an cycle in $G(t\Omega_n)$ (see [29]).

3.2.2 Tight codes in $\mathrm{CAC}^e(n,3)$

Now we are ready to give explicit series of tight codes in $\mathrm{CAC}^e(n,3)$, which can be seed codes for Corollary 3.2.10.

Theorem 3.2.5. *There exists a tight code in* $\mathrm{CAC}^e(n,3)$ *in the following two cases:*

(1) $n = 2^{2k-1} - 2^k + 1$ *for* $k \in \mathbb{N} \setminus \{1\}$.

(2) $n = 2^{2k-1} + 2^k + 1$ *for* $k \in \mathbb{N}$.

Proof: Let $n_1 = 2^{2k-1} - 2^k + 1$ and $n_2 = 2^{2k-1} + 2^k + 1$ for $k \geq 2$. Then, we have

$$n_1 n_2 = (2^{2k-1}-2^k+1)(2^{2k-1}+2^k+1) = (2^{2k-1}+1)^2-2^{2k} = 2^{4k-2}+1. \quad (3.2.1)$$

On the other hand, since $n_2 - n_1 = 2^{k+1}$,

$$\gcd(n_1, n_2) = \gcd(n_1, n_2 - n_1) = 1.$$

holds. Therefore it follows from (3.2.1) that

$$2^{4k-2} \equiv -1 \pmod{n_i} \quad \text{for } i = 1, 2, \qquad (3.2.2)$$

which implies that $\mathrm{sord}_{n_i}(2) \mid (4k-2)$ and thus $\mathrm{ord}_{n_i}(2) \mid (8k-4)$. Meanwhile, since $n_2 > n_1 > 2^{2k-2}$, $\mathrm{ord}_{n_i}(2) > 2k-2$ must hold for $i = 1, 2$. Therefore, there is a possibility that $\mathrm{ord}_{n_i}(2) = h(2k-1)$ for each $h = 1, 2, 4$, and $h = \frac{4}{3}$ as well if $3 \mid (2k-1)$, that is, $k \equiv 2 \pmod 3$.

It is rather obvious that $h = 1, 2$ is impossible since $2^{2k-1} \equiv (-1)^{i-1}2^k - 1 \not\equiv 1 \pmod{n_i}$ and (3.2.2) holds for $i = 1, 2$ and $k \geq 2$. Thus, if $3 \nmid (2k-1)$, then $h = 4$ is the only choice, that is, $\mathrm{ord}_{n_i}(2) = 8k-4$ and $\mathrm{sord}_{n_i}(2) = 4k-2$. If $3 \mid (2k-1)$, then the possibility of $h = \frac{4}{3}$ should be further examined. Let $u = h(2k-1) = \frac{8k-4}{3}$. Since $2^u \equiv 1 \pmod{n_i}$, by noting (3.2.2), we have $2^{4k-2-u} \equiv 2^{\frac{8k-4}{6}} \equiv -1 \pmod{n_i}$, which contradicts the fact that $2^{\frac{8k-4}{6}} < n_i - 1 = 2^{2k-1} + (-1)^i 2^k$ if $i = 1$ and $k \geq 3$, or $i = 2$ and $k \geq 2$.

Note that for n_1 with $k = 2$ and n_2 with $k = 1$, that is, $n_1 = n_2 = 5$, we have $\mathrm{sord}_5(2) = 2$ and $\mathrm{ord}_5(2) = 4$, which guarantees that $4 \mid \mathrm{ord}_n(2)$ and $-1 \in (2)_n$ for each of the cases (1) and (2).

Then, for each case, it follows from Corollary 3.1.4 that $|t\langle\theta\rangle_n|$ is even for any $t \in \mathbb{Z}_n^+$. This means that there exists a tight code in $\mathrm{CAC}^e(n,3)$. $\square$

Theorem 3.2.6. *For $m \in \mathbb{N} \setminus \{1\}$, let $n = \Phi_m(2)$, where $\Phi_m(x)$ is the nth cyclotomic polynomial. If $4 \mid m$ or $m \in \{2, 6\}$, then there exists a tight code in $\mathrm{CAC}^e(n, 3)$.*

Proof: Theorem 3.1.30 claims that

$$\mathrm{ord}_n(2) = \begin{cases} 2 & \text{if } m = 6, \\ n & \text{otherwise,} \end{cases}$$

and if m is even, then $-1 \in (2)_n$. Thus the assertion follows from Corollary 3.1.4 for the case when $4 \mid m$. If $m \in \{2, 6\}$, then $\Phi_2(2) = \Phi_6(2) = 3$ and $\mathrm{CAC}^e(3, 3)$ consists of a unique tight code $\{\{0, 1, 2\}\}$. □

Since $2^{2^f s}+1 = \prod_{d|s} \Phi_{2^{f+1}d}(2)$ holds for $f \in \mathbb{N}$ and an odd integer s, applying Corollary 3.2.10 recursively to tight codes obtained in Theorem 3.2.6 with $n = \Phi_{2^{f+1}d}(2)$ for $d \mid s$, we have one of the two series of odd n in [87] for which a tight equi-difference CAC of weight 3 exists.

Corollary 3.2.7 ([87, Theorem 1.1(1)])**.** *For $k \in \mathbb{N}$, let $n = 2^{2k} + 1$. Then there exists a tight code in $\mathrm{CAC}^e(n, 3)$.*

Note that $2^{2^k} - 1 = \prod_{i=0}^{k} \Phi_{2^i}(2) = \prod_{i=1}^{k} \Phi_{2^i}(2)$ for any $k \in \mathbb{N}$ and $\Phi_2(2) = \Phi_6(2) = 3$. Then, applying Corollary 3.2.10 recursively to tight codes obtained in Theorem 3.2.6 with $n = \Phi_{2^i}(2)$ for $1 \le i \le k$, we have the other series of odd n in [87].

Corollary 3.2.8 ([87, Theorem 1.1(2)])**.** *For $k \in \mathbb{N}$, let $n = 2^{2^k} - 1$. Then there exists a tight code in $\mathrm{CAC}^e(n, 3)$.*

The following is a recursive construction of an equi-difference CAC for general weight $w \ge 3$ given in [60] (see also Proposition 3.1 in [59]).

Theorem 3.2.9 ([60, Theorem 6.1])**.** *Let w, n_1, n_2 and s be positive integers such that $\gcd(n_2, \ell) = 1$ for all ℓ, $1 \le \ell \le w - 1$. Let $\mathcal{C}_1 \in \mathrm{CAC}^e(sn_1, w)$ with $|\mathcal{C}_1|$ non-exceptional codewords satisfying $n_1\mathbb{Z}_{sn_1} \subseteq \mathbb{Z}_{sn_1} \setminus \Delta(\mathcal{C}_1)$ and let $\mathcal{C}_2 \in \mathrm{CAC}^e(sn_2, w)$ with $|\mathcal{C}_2|$ codewords. Then there exists a code $\mathcal{C} \in \mathrm{CAC}^e(sn_1n_2, w)$ with $|\mathcal{C}| = n_2|\mathcal{C}_1| + |\mathcal{C}_2|$.*

For the definition of 'exceptional/non-exceptional' codewords, see [60]. If $w = 3$ and $3 \mid n$, then a code in $\mathrm{CAC}^e(n, 3)$ may contain $\{0, \frac{n}{3}, \frac{2n}{3}\}$ as the only exceptional codeword. Reading Theorem 3.2.9 as a recursive construction for a tight equi-difference CAC of odd length and weight 3, we have the following.

Corollary 3.2.10. *Let n_1 and n_2 be odd integers such that $3 \nmid n_1$. If there exist a tight code $\mathcal{C}_1 \in \mathrm{CAC}^e(n_1, 3)$ and a tight/optimal code $\mathcal{C}_2 \in \mathrm{CAC}^e(n_2, 3)$, then there exists a tight/optimal code $\mathcal{C} \in \mathrm{CAC}^e(n_1 n_2, 3)$ with $|\mathcal{C}| = n_2|\mathcal{C}_1| + |\mathcal{C}_2|$.*

Proof: It follows from Theorem 3.2.9 that the resulting code $\mathcal{C}$ is in $\mathrm{CAC}^e(n_1 n_2, 3)$; we prove it tight by checking the number of codewords. Let $\nu(n)$ be the number of odd cycles in $G(\Omega_n)$. If a code $\mathcal{C} \in \mathrm{CAC}^e(n, 3)$ is optimal, then

$$|\mathcal{C}| = \frac{n-1}{4} - \frac{\nu(n)}{2} + \epsilon(n)$$

holds, where $\epsilon(n) = 1$ or 0 depending on whether $3 \mid n$ or not. From the assumption that $\mathcal{C}_1$ is a tight code and $3 \nmid n_1$, we have $\nu(n_1) = 0$, $\epsilon(n_1) = 0$ and

$$\begin{aligned} |\mathcal{C}| &= n_2|\mathcal{C}_1| + |\mathcal{C}_2| \\ &= \frac{n_2(n_1-1)}{4} + \frac{n_2-1}{4} - \frac{\nu(n_2)}{2} + \epsilon(n_2) \\ &= \frac{n_1 n_2 - 1}{4} - \frac{\nu(n_2)}{2} + \epsilon(n_2), \end{aligned}$$

which implies that the code $\mathcal{C}$ is optimal since

$$\nu(n) = \nu(n_1 n_2) \geq \max\{\nu(n_1), \nu(n_2)\}$$

(see Remark 3.2.4). If $\mathcal{C}_2$ is a tight code, then $\nu(n_2) = 1$ or 0 depending on whether $3 \mid n_2$ or not. This means that $\mathcal{C}$ will also be a tight code. □

Applying Corollary 3.2.10 recursively with the tight codes given in Theorems 3.2.5 and 3.2.6, we can establish the following theorem.

Theorem 3.2.11. *Let $N = \{2^{2k-1} - 2^k + 1 : k \in \mathbb{N} \setminus \{1\}\} \cup \{2^{2k-1} + 2^k + 1 : k \in \mathbb{N}\} \cup \{\Phi_{4m}(2) : m \in \mathbb{N}\}$. For $f \in \{0, 1\}$, $n_i \in N$ and $e_i \in \mathbb{N}$, $1 \leq i \leq r$, let*

$$n = 3^f \prod_{i=1}^{r} n_i^{e_i}$$

for $r \in \mathbb{N}$. Then there exists a tight code in $\mathrm{CAC}^e(n, 3)$.

For $n < 5000$, tight codes in $\mathrm{CAC}^e(n, 3)$ obtained by Theorems 3.2.5, 3.2.6 and 3.2.11 are tabulated in 3.2.1, where "*" (in the table) means that the same result also can be found in [87].

Table 3.2.1: Tight codes in $\mathrm{CAC}^e(n,3)$ for $n < 5000$

n	Detail	$M(n,3)$	Ref. Thm.	n	Detail	$M(n,3)$	Ref. Thm.
5	2^3-2^2+1	1	3.2.5*	1105	$5{\cdot}13{\cdot}17$	276	3.2.11
	$\Phi_4(2)$		3.2.6	1205	$5{\cdot}241$	301	3.2.11
13	2^3+2^2+1	3	3.2.5	1275	$3{\cdot}5^2{\cdot}17$	319	3.2.11
	$\Phi_{12}(2)$		3.2.6	1285	$5{\cdot}257$	321	3.2.11
15	$3{\cdot}5$	4	3.2.11*	1443	$3{\cdot}481$	361	3.2.11
17	$\Phi_8(2)$	4	3.2.6*	1445	$5{\cdot}17^2$	361	3.2.11
25	2^5-2^3+1	6	3.2.5	1469	$13{\cdot}113$	367	3.2.11
	5^2		3.2.11	1599	$3{\cdot}13{\cdot}41$	400	3.2.11
39	$3{\cdot}13$	10	3.2.11	1625	$13{\cdot}5^3$	406	3.2.11
41	2^5+2^3+1	10	3.2.5	1635	$3{\cdot}545$	409	3.2.11
51	$3{\cdot}17$	13	3.2.11	1681	41^2	420	3.2.11
65	$5{\cdot}13$	16	3.2.11*	1695	$3{\cdot}5{\cdot}113$	424	3.2.11
75	$3{\cdot}5^2$	19	3.2.11	1875	$3{\cdot}5^4$	469	3.2.11
85	$5{\cdot}17$	21	3.2.11	1885	$13{\cdot}145$	471	3.2.11
113	2^7-2^4+1	28	3.2.5	1921	$17{\cdot}113$	480	3.2.11
123	$3{\cdot}41$	31	3.2.11	1985	$2^{11}-2^6+1$	496	3.2.5
125	5^3	31	3.2.11	2091	$3{\cdot}17{\cdot}41$	523	3.2.11
145	2^7+2^4+1	36	3.2.5	2113	$2^{11}+2^6+1$	528	3.2.5
169	13^2	42	3.2.11	2125	$5^3{\cdot}17$	531	3.2.11
195	$3{\cdot}5{\cdot}13$	49	3.2.11	2175	$3{\cdot}5{\cdot}145$	544	3.2.11
205	$\Phi_{20}(2)$	51	3.2.6	2197	13^3	549	3.2.11
221	$13{\cdot}17$	55	3.2.11	2405	$5{\cdot}481$	601	3.2.11
241	$\Phi_{24}(2)$	60	3.2.6	2465	$17{\cdot}145$	616	3.2.11
255	$3{\cdot}5{\cdot}17$	64	3.2.11*	2535	$3{\cdot}5{\cdot}13^2$	634	3.2.11
257	$\Phi_{16}(2)$	64	3.2.6*	2665	$5{\cdot}13{\cdot}41$	666	3.2.11
289	17^2	72	3.2.11	2725	$5{\cdot}545$	681	3.2.11
325	$5^2{\cdot}13$	81	3.2.11	2825	$5^2{\cdot}113$	706	3.2.11
339	$3{\cdot}113$	85	3.2.11	2873	$13^2{\cdot}17$	718	3.2.11
375	$3{\cdot}5^3$	94	3.2.11	3075	$3{\cdot}5^2{\cdot}41$	769	3.2.11
425	$5^2{\cdot}17$	106	3.2.11	3125	5^5	781	3.2.11
435	$3{\cdot}145$	109	3.2.11	3133	$13{\cdot}241$	783	3.2.11
481	2^9-2^5+1	120	3.2.5	3277	$\Phi_{28}(2)$	819	3.2.6
507	$3{\cdot}13^2$	127	3.2.11	3315	$3{\cdot}5{\cdot}13{\cdot}17$	829	3.2.11
533	$13{\cdot}41$	133	3.2.11	3485	$5{\cdot}17{\cdot}41$	871	3.2.11
545	2^9+2^5+1	136	3.2.5	3615	$3{\cdot}5{\cdot}241$	904	3.2.11
565	$5{\cdot}113$	141	3.2.11	3625	$5^2{\cdot}145$	906	3.2.11
615	$3{\cdot}5{\cdot}41$	154	3.2.11	3757	$13{\cdot}17^2$	939	3.2.11
625	5^4	156	3.2.11	3855	$3{\cdot}5{\cdot}257$	964	3.2.11
663	$3{\cdot}13{\cdot}17$	166	3.2.11	4033	$\Phi_{36}(2)$	1008	3.2.6
697	$17{\cdot}41$	174	3.2.11	4097	$17{\cdot}241$	1024	3.2.11*
723	$3{\cdot}241$	181	3.2.11	4225	$5^2{\cdot}13^2$	1056	3.2.11
725	$5{\cdot}145$	181	3.2.11	4335	$3{\cdot}5{\cdot}17^2$	1084	3.2.11
771	$3{\cdot}257$	193	3.2.11	4369	$17{\cdot}257$	1092	3.2.11
845	$5{\cdot}13^2$	211	3.2.11	4407	$3{\cdot}13{\cdot}113$	1102	3.2.11
867	$3{\cdot}17^2$	217	3.2.11	4633	$41{\cdot}113$	1158	3.2.11
975	$3{\cdot}5^2{\cdot}13$	244	3.2.11	4875	$3{\cdot}5^3{\cdot}13$	1219	3.2.11
1025	$5^2{\cdot}41$	256	3.2.11*	4913	17^3	1228	3.2.11

3.2.3 Optimal codes in $\mathrm{CAC}^e(n,3)$

In this subsection, we consider the case when $G(\Omega_n)$ contains some odd cycles $t\langle 2\rangle_n$ for $t \in \mathbb{Z}_n^+$, and determine $M^e(n,3)$.

We should mention that a tight code in $\mathrm{CAC}^e(n,3)$ is equivalent to a perfect 2-shift code in a finite abelian group (see [48]), and due to Levenshtein and Vinck [48], the necessary and sufficient condition for the existence of a tight code in $\mathrm{CAC}^e(n,3)$ is known. However if it is not a tight code, determining the size $M^e(n,3)$ of an optimal (not necessarily tight) code in $\mathrm{CAC}^e(n,3)$ for a given n is a challenging problem. In this subsection, we give a computation formula of $M^e(n,3)$ for odd n which does not have prime factor $p \equiv 1 \pmod 8$.

Theorem 3.2.12. *Let N_1 and N_2 be multisets of odd non-Wieferich primes $p \equiv 3 \pmod 8$ and $p \equiv 7 \pmod 8$, respectively, and N_3 be a multiset of odd primes p with $p \equiv 5 \pmod 8$. Further let*

$$n_j = \prod_{p \in M_j} p \quad \text{for } j = 1,2,3$$

and $n = n_1 n_2 n_3$, where $n_j = 1$ if $N_j = \emptyset$. Assume that

(i) $\gcd(\varphi(p^e), \varphi(q^f))$ *is a power of 2 for any distinct prime factors p, q of n_j ($j \in \{1,2\}$), where $e = v_p(n_j)$ and $f = v_q(n_j)$, and*

(ii) $\Omega_p = \langle 2\rangle_p$ *for any prime factor p of $n_1 n_2$.*

Then,

$$M^e(n,3) = \frac{1}{4}\Big\{n + 1 - \prod_{p|n_1}\big(1 + 2v_p(n_1)\big) - \prod_{p|n_2}\big(1 + 2v_p(n_2)\big)\Big\} + \epsilon(n),$$

where $\epsilon(n) = 1$ or 0 depending on whether $3 \mid n$ or not.

Proof: From Theorem 3.2.1, there exists an optimal (but not tight) code $\mathcal{C} \in \mathrm{CAC}^e(n,3)$ with

$$|\mathcal{C}| = \frac{1}{2}\Big(\frac{n-1}{2} - \nu(n)\Big) + \epsilon(n),$$

where $\nu(n)$ is the number of odd cycles in $G(\Omega_n)$. Thus the assertion can be immediately proved by Corollary 3.1.19. □

Corollary 3.2.13. *Under the same assumptions as in Theorem 3.2.12, if N_1 and N_2 are non-multisets, then*

$$M^e(n,3) = \frac{1}{4}\big(n+1-3^{e_1}-3^{e_2}\big)+\epsilon(n),$$

where $e_j = |N_j|$ for $j = 1, 2$.

By virtue of Theorem 3.1.31, we can state the following on $M^e(n,3)$, including the case when n contains a prime factor $p \equiv 1 \pmod 8$:

Theorem 3.2.14. *Let N_1, N_2, and N_3 be a set of odd integers, a set of singly even integers, and a set of doubly even integers, respectively. Further let*

$$n_j = \prod_{m\in N_j} \Phi_m(2) \quad \text{for } j = 1, 2, 3$$

and $n = n_1n_2n_3$, where $n_j = 1$ if $N_j = \emptyset$. If $\Phi_m(2)$ is a non-Wieferich prime for any $m \in N_1 \cup N_2$, and a prime for any $m \in N_3$, then

$$M^e(n,3) = \frac{n-1}{4} - \frac{1}{2}\big(N(n_1)+N(n_2)\big)+\epsilon(n).$$

Moreover, if (i) *$\Phi_m(2)$'s are distinct primes for all $m \in N_1 \cup N_2$, and* (ii) *$\gcd(m, m') = j$ for any pair of distinct integers $m, m' \in N_j$ ($j \in \{1, 2\}$), then*

$$M^e(n,3) = \frac{1}{4}\left\{n+1-\prod_{m\in N_1}\Big(1+\frac{1}{m}(\Phi_m(2)-1)\Big)-\mu\prod_{m\in N_2}\Big(1+\frac{2}{m}(\Phi_m(2)-1)\Big)\right\}+\epsilon(n),$$

where $\mu = \frac{9}{5}$ or 1 depending on whether $6 \in N_2$ or not.

Proof: Theorem 3.1.31 guarantees that both $\mathrm{sord}_{n_1}(2)$ and $\mathrm{sord}_{n_2}(2)$ are odd and $\mathrm{sord}_{n_3}(2)$ is even. Thus $|t\langle 2\rangle_{n_j}|$ is odd for any $t \in \mathbb{Z}^+_{n_j}$ ($j \in \{1, 2\}$). Noting that $\mathrm{ord}_{n_1}(2)$ is odd and $\mathrm{ord}_{n_2}(2) \equiv 2 \pmod 4$, we have that $-1 \notin (2)_{n_1}$ and $-1 \in (2)_{n_2}$. Applying Theorem 3.1.16, the number of odd cycles in $G(\Omega_n)$ can be obtained. Thus the first assertion can be proved by a similar calculation as in Theorem 3.2.12.

Now we will show the second assertion. Since $\Phi_m(2)$'s are distinct primes for all $m \in N_1 \cup N_2$, we know from Lemma 3.1.31 that $\mathrm{sord}_{n_j}(2)$ is a multiplicative function with respect to n_j ($j \in \{1, 2\}$). Note that for $j = 1, 2$,

$$\{p : p \text{ is a prime factor of } n_j\} = \{\Phi_m(2) : m \in N_j\}$$

and for $m \in N_j$, $\mathrm{sord}_{\Phi_m(2)}(2) = \frac{\delta m}{j}$ follows from Theorem 3.1.30, where $\delta = \frac{1}{3}$ or 1 depending on whether $j = 2$ and $m = 6$, or not. Since $v_p(2^{\mathrm{sord}_p(2)} \pm 1) = 1$ for any non-Wieferich prime p, it immediately follows from Lemma 3.1.14 that

$$N(n_j) = \frac{1}{2}\left\{ \prod_{m \in N_j} \left(1 + \frac{j}{\delta m}(\Phi_m(2) - 1)\right) - 1 \right\} \quad \text{for } j = 1, 2.$$

Thus,

$$N(n_1) + N(n_2) =$$
$$\frac{1}{2}\left\{ \prod_{m \in N_1} \left(1 + \frac{1}{m}(\Phi_m(2) - 1)\right) + \mu \prod_{m \in N_2} \left(1 + \frac{2}{m}(\Phi_m(2) - 1)\right) \right\} - 1,$$

where $\mu = \frac{9}{5}$ or 1 depending on whether $6 \in N_2$ or not. Hence the second assertion is proved. □

Example 3.2.15. (1) The case when $n = \Phi_3(2)\Phi_9(2) = 511 = 7{\cdot}73$. As in Example 3.1.32(2), all cycles in $G(511)$ are odd cycles. $G(511)$ is decomposed into the $\sum_{\substack{d|511 \\ d \neq 1}} \frac{\varphi(d)}{2 \cdot \mathrm{sord}_d(2)} (= 29)$ odd cycles. Thus the code $\mathcal{C} \in \mathrm{CAC}^e(511, 3)$ derived from the 29 cycles is optimal and $M^e(511, 3) = \frac{511-1}{4} - \frac{29}{2} = 113$.

(2) The case when $n = \Phi_3(2)\Phi_5(2)\Phi_8(2) = 3689 = 7{\cdot}17{\cdot}31$. Since $\Phi_3(2) = 7$, $\Phi_5(2) = 31$ and $\Phi_8(2) = 17$, we have $\mathrm{sord}_{\Phi_3(2)}(2) = 3$, $\mathrm{sord}_{\Phi_5(2)}(2) = 5$ and $\mathrm{sord}_{\Phi_8(2)}(2) = 4$. Let $n_1 = \Phi_3(2)\Phi_5(2)$ and $n_3 = \Phi_8(2)$. From Theorem 3.2.14, there are $N(n_1)$ odd cycles in $G(3689)$. By Lemma 3.1.31, we know that $\mathrm{sord}_{n_j}(2)$ is a multiplicative function with respect to n_j ($j \in \{1, 2\}$). Note that $v_{\Phi_3(2)}(2^3 - 1) = v_{\Phi_5(2)}(2^5 - 1) = 1$. Applying Lemma 3.1.14, we have the number of disjoint odd cycles in $G(3689)$ as

$$N(n_1) = \frac{1}{2}\left\{ \left(1 + \frac{\Phi_3(2) - 1}{\mathrm{sord}_{\Phi_3(2)}(2)}\right)\left(1 + \frac{\Phi_5(2) - 1}{\mathrm{sord}_{\Phi_5(2)}(2)}\right) - 1 \right\} = 10.$$

Thus the code $\mathcal{C} \in \mathrm{CAC}^e(3689, 3)$ is optimal and $M^e(3689, 3) = \frac{3689-1}{4} - \frac{10}{2} = 917$.

3.3 Optimal equi-difference conflict-avoiding codes of weight four

In this section, we develop optimal equi-difference conflict-avoiding codes of weight four. Without loss of generality, we write any integer n as $n = 2^a 3^b m$

with $\gcd(m, 6) = 1$. In Subsection 3.3.1, our notations and graph representation for an equi-difference CAC of weight four are given. In Subsection 3.3.2, we characterize the graph corresponding to an equi-difference CAC of weight four. In Subsection 3.3.3, the following recurrence formula for the size $M^e(n = 2^a3^bm, 4)$ of an optimal code in $\mathrm{CAC}^e(2^a3^bm, 4)$ is obtained with respect to $b \geq 2$.

$$M^e(2^a3^bm, 4) = \begin{cases} 2^{a-3}(3^b - 1)m + M^e(2^am) & \text{if } b \text{ is even,} \\ 2^{a-3}(3^b - 3)m + M^e(2^a3m) & \text{if } b \text{ is odd.} \end{cases} \tag{3.3.1}$$

In Subsection 3.3.4, we determine the maximum sizes of subcodes by using some properties of the multiplicative order shown in Section 3.1. By virtue of those properties of the multiplicative suborder, it is shown in Subsections 3.3.5 and 3.3.6 that the second terms $M^e(2^am)$ and $M^e(2^a3m)$ on the right-hand side of (3.3.1) can be represented as recurrence formulae with respect to a. We overview our results in the last section.

Note that a necessary and sufficient condition for the existence of a tight equi-difference CAC of weight four is equivalent to that of a perfect 3-shift code (see [61]). As is the case of weight three, we are interested in the size $M^e(n, 4)$ of an optimal (not necessarily tight) code in $\mathrm{CAC}^e(n, 4)$.

3.3.1 Graph representation for codes in $\mathbf{CAC}^e(n, 4)$

Let $C_x = \{0, x, 2x, 3x \pmod n\}$ for $x \in \mathbb{Z}_n^+$. Since $\Delta(C_x) = \Delta(C_{n-x}) = \{\pm x, \pm 2x, \pm 3x \pmod n\}$, at most one of C_x and C_{n-x} can be a codeword of a code $\mathcal{C} \in \mathrm{CAC}^e(n, 4)$. Therefore we identify C_x with C_{n-x} for $x \in \Omega_n$ throughout this thesis.

Recall that any integer $n \in \mathbb{N}$ can be written as $n = 2^a3^bm$ for $a, b \geq 0$ and $m \in \mathbb{N}$ with $\gcd(m, 6) = 1$. We use a directed graph to examine common differences among C_x's for all $x \in \Omega_n$. It should be noticed in advance that for consistency of the discussion, $C_{n/2}$ and/or $C_{n/3}$ come up in context if $2 \mid n$ and/or $3 \mid n$, but $C_{n/2}$ and $C_{n/3}$ can never be codewords since neither can be of weight 4.

Let $G(\Omega_n)$ be a directed graph with the vertex set Ω_n and the directed edge set $E = \{(x, y) \in \Omega_n^2 : y \equiv \pm 2x \text{ or } \pm 3x \pmod n\}$. It is not difficult to see that the outdegree of any vertex $x \in \Omega_n$ is 2, and that $\Delta(C_x) \cap \Delta(C_{2x}) = \{\pm 2x \pmod n\}$ and $\Delta(C_x) \cap \Delta(C_{3x}) = \{\pm 3x \pmod n\}$ hold for $x \in \Omega_n$.

Note that for our discussion of optimal equi-difference CACs of weight four, a directed graph representation is tractable since the indegree of each vertex is not constant. Meanwhile, for the discussion of optimal equi-difference CACs of odd length and weight three in Section 3.1, an undirected graph is easier to deal with since both the indegree and the outdegree of each vertex are exactly 1, and thus $G(\Omega_n)$ is partitioned into disjoint cycles.

Lemma 3.3.1. *For $x \neq y \in \Omega_n$, $\Delta(C_x) \cap \Delta(C_y) = \emptyset$ holds if and only if (i) $(x, y) \notin E$ and $(y, x) \notin E$ and (ii) there does not exist $z \in \Omega_n$ such that $(x, z), (y, z) \in E$.*

Proof: ($\Rightarrow$) Since $\Delta(C_x) \cap \Delta(C_y) = \emptyset$, we have (i) $x \not\equiv \pm 2y, \pm 3y \pmod{n}$ and $y \not\equiv \pm 2x, \pm 3x \pmod{n}$, and (ii) $2x \equiv \pm 2y \pmod{n}$, $2x \equiv \pm 3y \pmod{n}$, $3x \equiv \pm 2y \pmod{n}$ and $3x \equiv \pm 3y \pmod{n}$. It is clear that (i) implies $(y, x) \notin E$ and $(x, y) \notin E$. Note that if there exists $z \in \Omega_n$ such that $(x, z) \in E$ and $(y, z) \in E$, then $z \equiv \pm 2x$ or $\pm 3x \pmod{n}$, and $z \equiv \pm 2y$ or $\pm 3y \pmod{n}$ hold. Hence it follows from (ii) that such z does not exist.
($\Leftarrow$) The definition of an edge in the graph $G(\Omega_n)$ explains the sufficiency. $\square$

Let $\mathcal{C} = \mathcal{C}_X = \{C_x : x \in X \subset \Omega_n\}$ be a code in $\mathrm{CAC}^e(n, 4)$. Then for any $x \neq y \in X$, both (i) and (ii) hold in Lemma 3.3.1. Thus we may view a subset X of Ω_n as a code $\mathcal{C} \in \mathrm{CAC}^e(n, 4)$ by identifying x with C_x. Our purpose is to determine the maximum size $M^e(n, 4)$ of a code in $\mathrm{CAC}^e(n, 4)$. That is, our problem can be rephrased as follows.

Problem: Find a vertex set X in $G(\Omega_n)$ such that $\mathcal{C}_X$ is a code with maximum size in $\mathrm{CAC}^e(n, 4)$.

If $x \in X$, then $2x, 3x \notin X$. On the other hand, if $x \notin X$, then at most one of $2x$ and $3x$ can be in X since $2x$ and $3x$ are adjacent to $6x$. That is, at most one of x, $2x$ and $3x$ can be in X. Let $G'(\Omega_n)$ be an undirected graph with the vertex set Ω_n and the (undirected) edge set $E' = \{\{x, y\}, \{y, z\}, \{x, z\} : (x, z), (y, z) \in E\}$.

Lemma 3.3.2. *Finding a subset $X \subset \Omega_n$ satisfying conditions (i) and (ii) in Lemma 3.3.1 is equivalent to finding an independent vertex set in the graph $G'(\Omega_n)$.*

Using Lemma 3.3.2, our problem is translated to the familiar problem of finding an independent vertex set of $G'(\Omega_n)$. However, $G'(\Omega_n)$ has more edges than $G(\Omega_n)$ and thus tends to be messy to deal with. Hence we mainly use $G(\Omega_n)$ and consider an undirected graph $G'(\Omega_n)$ only when necessary.

For a positive integer $k = 2^i 3^j s$ with $\gcd(s, 6) = 1$, let

$$V_k^d = V_{2^i 3^j s}^d = \{x \in \Omega_k : \gcd(s, x) = d\}$$

and $tV_k^d = \{tx : x \in V_k^d\}$. When $d = 1$, we write just V_k instead of V_k^1. Note that $|V_k| = 2^{i-1}3^j\varphi(s)$, where φ is Euler's totient function. Then we can decompose Ω_n into disjoint vertex subsets as follows:

$$\Omega_n = \bigcup_{d'|m} V_n^{d'} = \bigcup_{d'|m} d' V_{2^a 3^b \frac{m}{d'}} = \bigcup_{d|m} \frac{m}{d} V_{2^a 3^b d}.$$

Lemma 3.3.3. *For integers $a, b \geq 0$ and $m \in \mathbb{N}$ with $\gcd(m, 6) = 1$, let $n = 2^a 3^b m$. The graph $G(\Omega_n)$ is decomposed into disconnected subgraphs $G(V_n^d)$ for all divisors d of m. Moreover, $G(V_n^d) \cong G(V_{2^a 3^b \frac{m}{d}})$.*

Proof: (i) Let $x_1 \in V_n^{d_1}$ and $x_2 \in V_n^{d_2}$ for distinct divisors d_1, d_2 of m. Thus $\gcd(m, x_1) = d_1$ and $\gcd(m, x_2) = d_2$. Clearly, $d_2 \nmid x_1$ or $d_1 \nmid x_2$ since $d_1 \neq d_2$. Suppose that $(x_1, x_2) \in E$. Then $x_2 \equiv \pm 2x_1 \pmod{n}$ or $x_2 \equiv \pm 3x_1 \pmod{n}$ must hold. If $x_2 \equiv \pm 2x_1 \pmod{n}$, then both $x_2 \equiv \pm 2x_1 \equiv 0 \pmod{d_1}$ and $x_2 \equiv \pm 2x_1 \equiv 0 \pmod{d_2}$ hold. This implies that $d_1 \mid x_2$ and $d_2 \mid x_1$, which contradicts the assumption. By a similar argument, $(x_1, x_2) \notin E$ if $x_2 \equiv \pm 3x_1 \pmod{n}$. Hence $G(V_n^{d_1})$ and $G(V_n^{d_2})$ are disconnected, which shows the first assertion.

(ii) For any $x \in V_n^d$, $\gcd(m, x) = d$ holds, which is reduced to $\gcd(\frac{m}{d}, \frac{x}{d}) = 1$. Hence we have $V_n^d \cong V_{n/d}^1$ by considering a bijection $f : x \to \frac{x}{d}$. Then it immediately follows from (i) that $G(V_n^d) \cong G(V_{n/d})$. □

Let $\mathrm{CAC}^e(V_n)$ be the class of equi-difference CACs of weight 4 derived from $G(V_n)$ and $M_\varphi^e(n, 4)$ be the maximum size of a code in $\mathrm{CAC}^e(V_n)$.

(1) For $m = 1$, $M^e(2^a 3^b, 4) = M_\varphi^e(2^a 3^b, 4)$ for $(a, b) \notin \{(0, 0), (1, 0), (0, 1)\}$.

(2) For $m \geq 5$ with $\gcd(m, 6) = 1$ and $a, b \geq 0$,

$$M^e(2^a 3^b m, 4) = \sum_{d|m} M_\varphi^e(2^a 3^b d, 4). \tag{3.3.2}$$

(3.3.2) implies that the problem of determining $M^e(2^a 3^b m, 4)$ can be reduced to the problem of determining $M_\varphi^e(2^a 3^b d, 4)$ for all divisors d of m. Therefore, it is sufficient to find $M_\varphi^e(2^a 3^b m, 4)$ for any m relatively prime to 6.

In order to do that, the structure of $G(V_n)$ needs to be clarified. For $n = 2^a 3^b m$ with $\gcd(m, 6) = 1$, let $U_{ij} = \{x \in V_n : \gcd(x, 2^a) = 2^i, \gcd(x, 3^b) = 3^j\}$ for $0 \le i \le a$ and $0 \le j \le b$. Then

$$V_n = \bigcup_{i=0}^{a} \bigcup_{j=0}^{b} U_{ij}.$$

By noting $|U_{ij}| = \frac{1}{2}\varphi(\frac{n}{2^i 3^j}) = \frac{1}{2}\varphi(2^{a-i}3^{b-j}m)$, the following can be easily observed.

(1) When $m = 1$, that is, $n = 2^a 3^b$, $U_{ab} = \emptyset$ and it can be easily verified that

$$|U_{ij}| = \begin{cases} 2^{a-1-i}3^{b-1-j} & \text{if } i < a \text{ and } j < b, \\ 2^{a-2-i} & \text{if } i < a-1 \text{ and } j = b, \\ 3^{b-1-j} & \text{if } i = a \text{ and } j < b, \\ 1 & \text{if } i = a-1 \text{ and } j = b, \\ 0 & \text{if } i = a \text{ and } j = b. \end{cases} \tag{3.3.3}$$

Note that $|U_{a-1,b-1}| = |U_{a,b-1}| = |U_{a-2,b}| = |U_{a-1,b}| = 1$. Indeed, $U_{a-1,b-1} = \{\frac{n}{6}\}$, $U_{a,b-1} = \{\frac{n}{3}\}$, $U_{a-2,b} = \{\frac{n}{4}\}$ and $U_{a-1,b} = \{\frac{n}{2}\}$.

(2) When $m \ge 5$ with $\gcd(m, 6) = 1$, for a given m,

$$|U_{ij}| = \begin{cases} 2^{a-1-i}3^{b-1-j}\varphi(m) & \text{if } i < a \text{ and } j < b, \\ 2^{a-2-i}\varphi(m) & \text{if } i < a \text{ and } j = b, \\ 3^{b-1-j}\varphi(m) & \text{if } i = a \text{ and } j < b, \\ \frac{1}{2}\varphi(m) & \text{if } i = a \text{ and } j = b. \end{cases} \tag{3.3.4}$$

Example 3.3.4. Let $n = 42 = 2{\cdot}3{\cdot}7$. A graph $G(\Omega_{42})$ consists of two disconnected subgraphs $G(V_{42})$ and $G(7V_6)$ (see Fig. 3.3.1). This implies that $M^e(42, 4)$ can be given as a sum of the maximum numbers of codewords derived from $G(V_{42})$ and $G(7V_6)$, that is, $M^e_\varphi(42) + M^e_\varphi(6)$.

3.3.2 Structure of $G(V_n)$

Write $n = 2^a 3^b m$ for an integer $m \in \mathbb{N}$ with $\gcd(m, 6) = 1$. For $x \in \Omega_n \cup \{0\}$, let σ_2 and σ_3 be mappings defined by

$$\sigma_2(x) = \begin{cases} 2x & \text{for } 0 \le x \le \frac{n}{4}, \\ n - 2x & \text{for } \frac{n}{4} \le x \le \frac{n}{2}, \end{cases} \quad \text{and} \quad \sigma_3(x) = \begin{cases} 3x & \text{for } 0 \le x \le \frac{n}{6}, \\ n - 3x & \text{for } \frac{n}{6} \le x \le \frac{n}{3}, \\ 3x - n & \text{for } \frac{n}{3} \le x \le \frac{n}{2}. \end{cases}$$

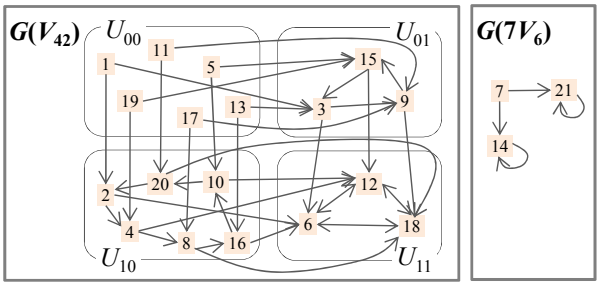

Figure 3.3.1: $G(\Omega_{42})$

Lemma 3.3.5. *By restricting the domain of the mapping σ_2 to U_{ij}, the followings hold for $0 \le j \le b$:*

(i) *For $0 \le i \le a-2$, $\sigma_2(U_{ij}) = U_{i+1,j}$, which is a 2-to-1 onto mapping.*

(ii) *For $i = a-1$ and $(j,m) \ne (b,1)$, $\sigma_2(U_{ij}) = U_{i+1,j}$, which is a bijection.*

(iii) *For $i = a$ and $(j,m) \ne (b,1)$, $\sigma_2(U_{ij}) = U_{ij}$, which is a bijection.*

Proof: Let $y = 2^{i+1}y' \in U_{i+1,j}$ for $0 \le i \le a-1$, and consider the two solutions $x = 2^i y'$ and $\frac{n}{2} - 2^i y'$ of the equation $y = \sigma_2(x)$ over $V_{2^a 3^b m}$.

(i) For $0 \le i \le a-2$, both of the two solutions are in U_{ij}. Hence σ_2 is an onto mapping from U_{ij} to $U_{i+1,j}$. It is clear that for $x, x' \in U_{ij}$ such that $x' \ne x, \frac{n}{2} - x$, $\sigma_2(x) \ne \sigma_2(x')$ holds. Meanwhile, it follows from (3.3.3) and (3.3.4) that $|U_{ij}| = 2|U_{i+1,j}|$ for $0 \le i \le a-2$. Thus σ_2 is a 2-to-1 onto mapping from U_{ij} to $U_{i+1,j}$.

(ii) & (iii) When $i = a-1$, that is, $y = 2^a y' \in U_{aj}$, we have two cases to consider:

$$\begin{array}{rr} 2^{a-1}y' \in U_{a-1,j}, & \frac{n}{2} - 2^{a-1}y' \in U_{aj} \quad \text{if } y' \text{ is odd,} \\ \frac{n}{2} - 2^{a-1}y' \in U_{a-1,j}, & 2^{a-1}y' \in U_{aj} \quad \text{if } y' \text{ is even.} \end{array}$$

Then a similar argument to case (i) with the fact that $|U_{a-1,j}| = |U_{aj}|$ for $(j,m) \ne (b,1)$ shows that, from $U_{a-1,j}$ to U_{aj} and U_{aj} to U_{aj}, σ_2 is a bijection. □

Lemma 3.3.6. *By restricting the domain of the mapping σ_3 to U_{ij}, the following hold for $0 \le i \le a$:*

(i) *For $0 \le j \le b-2$, $\sigma_3(U_{ij}) = U_{i,j+1}$, which is a 3-to-1 onto mapping.*

(ii) *For $j = b-1$ and $(i,m) \notin \{(a-1,1),(a,1)\}$, $\sigma_3(U_{ij}) = U_{i,j+1}$, which is a 2-to-1 onto mapping. In the case of $(i,j,m) = (a-1,b-1,1)$, we have $\sigma_3(U_{ij}) = U_{i,j+1}$, which is a bijection.*

(iii) *For $j = b$ and $(i,m) \neq (a,1)$, $\sigma_3(U_{ij}) = U_{ij}$, which is a bijection.*

Proof: Let $y = 3^{j+1}y' \in U_{i,j+1}$ for $0 \leq j \leq b-1$ and consider the three solutions $x = 3^j y', \frac{n}{3} \pm 3^j y'$ of the equation $y = \sigma_3(x)$ over $V_{2^a 3^b m}$.

(i) For $0 \leq j \leq b-2$, all three solutions are in U_{ij}. Hence σ_3 is an onto mapping from U_{ij} to $U_{i,j+1}$. Since $\sigma_3(x) \neq \sigma_3(x')$ for any $x, x' \in U_{ij}$ such that $x' \neq x, \frac{n}{3} \pm x$, and $|U_{ij}| = 3|U_{i,j+1}|$ for $0 \leq j \leq b-2$, σ_3 is a 3-to-1 onto mapping from U_{ij} to $U_{i,j+1}$ for $0 \leq j \leq b-2$.

(ii) & (iii) When $j = b-1$, that is, $y = 3^b y' \in U_{ib}$, and $(i,m) \notin \{(a,1),(a-1,1)\}$, we have three cases to consider:

$$\begin{array}{rll} \frac{n}{3} \pm 3^{b-1}y' \in U_{i,b-1}, & 3^{b-1}y' \in U_{ib} & \text{if } y' \equiv 0 \pmod 3, \\ 3^{b-1}y', \frac{n}{3} + 3^{b-1}y' \in U_{i,b-1}, & \frac{n}{3} - 3^{b-1}y' \in U_{ib} & \text{if } y' \equiv 2^a m \pmod 3, \\ 3^{b-1}y', \frac{n}{3} - 3^{b-1}y' \in U_{i,b-1}, & \frac{n}{3} + 3^{b-1}y' \in U_{ib} & \text{if } y' \equiv -2^a m \pmod 3. \end{array}$$

Since $|U_{i,b-1}| = 2|U_{ib}|$ for $(i,m) \notin \{(a-1,1),(a,1)\}$ and $\sigma_3(x) \neq \sigma_3(x')$ as long as $x' \neq x, \frac{n}{3} \pm x$, σ_3 is a 2-to-1 onto mapping from $U_{i,b-1}$ to U_{ib}. It is easy to see that σ_3 is a bijection from U_{ib} to U_{ib}. Note that when $m = 1$, $U_{a-1,b-1} = \{n/6\}$ and $\sigma_3(U_{a-1,b-1}) = \{n/2\} = U_{a-1,b}$. Thus σ_3 is a bijection from $U_{a-1,b-1}$ to $U_{a-1,b}$. □

Remark that, when $m = 1$, $U_{ab} = \emptyset$, $\sigma_2(U_{a-1,b}) = \sigma_2(\{n/2\}) = \{0\}$ and $\sigma_3(U_{a,b-1}) = \sigma_3(\{n/3\}) = \{0\}$. For a code $\mathcal{C} \in \mathrm{CAC}^e(V_n)$, let $\mathcal{C}_{ij} = \mathcal{C} \cap U_{ij}$ and $|\mathcal{C}_{ij}| = c_{ij}$. From Lemmas 3.3.5 and 3.3.6, and the definition of a CAC that any pair of codewords in $\mathcal{C}$ have no differences in common, we can state the following.

Lemma 3.3.7. *If $\sigma_2(U_{i'j}) = U_{ij}$ and $\sigma_3(U_{ij'}) = U_{ij}$, then $\sigma_2(\mathcal{C}_{i'j})$, $\sigma_3(\mathcal{C}_{ij'})$ and $\mathcal{C}_{ij}$ are disjoint. Moreover, $|\mathcal{C}_{ij}| = |\sigma_2(\mathcal{C}_{ij})| = |\sigma_3(\mathcal{C}_{ij})|$ holds.*

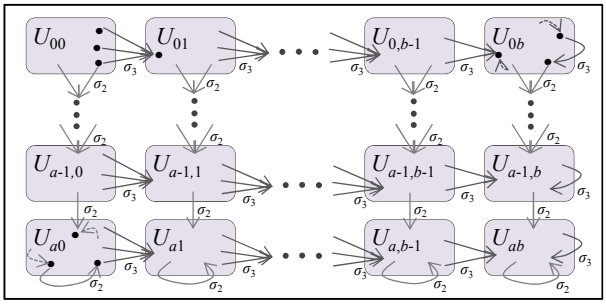

Figure 3.3.2: The adjacency relation of vertices in $G(V_n)$

3.3.3 The recurrence formula of $M^e_\varphi(2^a3^bm, 4)$ with respect to b

Note that any $x \in \bigcup_{j=b'}^{b}\bigcup_{i=0}^{a} U_{ij}$ is represented as $x = 3^{b'}y$ for some $y \in V_{2^a3^{b-b'}m}$. Thus we have

$$G\Big(\bigcup_{j=b'}^{b}\bigcup_{i=0}^{a} U_{ij}\Big) \cong 3^{b'}G(V_{2^a3^{b-b'}m}).$$

Lemma 3.3.8. *For $a \geq 0$, $b \geq 2$ and $m \geq 1$ with $\gcd(m, 6) = 1$,*

$$M^e_\varphi(2^a3^bm, 4) \leq 2^a3^{b-2}\varphi(m) + M^e_\varphi(2^a3^{b-2}m, 4)$$

holds.

Proof: For $b \geq 2$, we shall examine incoming edges for each vertex of U_{i1} in $G(V_{2^a3^bm})$. In the case when $a = 0$, it follows from Lemmas 3.3.5 and 3.3.6 that

$$\mathcal{C}_{01} \,\dot\cup\, \sigma_2(\mathcal{C}_{01}) \,\dot\cup\, \sigma_3(\mathcal{C}_{00}) \subset U_{01}.$$

This means that $2|\mathcal{C}_{01}| + |\mathcal{C}_{00}| \leq |U_{01}|$ since $|\mathcal{C}_{ij}| = |\sigma_2(\mathcal{C}_{ij})| = |\sigma_3(\mathcal{C}_{ij})|$ holds (see Lemma 3.3.7), which can be rewritten as

$$2c_{01} + c_{00} \leq 3^{b-2}\varphi(m). \tag{3.3.5}$$

In the case when $a \geq 1$, $\mathcal{C}_{01} \,\dot\cup\, \sigma_3(\mathcal{C}_{00}) \subset U_{01}$ holds from Lemmas 3.3.5, 3.3.6 and 3.3.7, which implies

$$c_{01} + c_{00} \leq |U_{01}| = 2^{a-1}3^{b-2}\varphi(m). \tag{3.3.6}$$

In a similar manner, we have $\mathcal{C}_{i1} \dot{\cup} \sigma_2(\mathcal{C}_{i-1,1}) \dot{\cup} \sigma_3(\mathcal{C}_{i0}) \subset U_{i1}$ for $1 \leq i \leq a-1$ and $\mathcal{C}_{a1} \dot{\cup} \sigma_2(\mathcal{C}_{a1}) \dot{\cup} \sigma_2(\mathcal{C}_{a-1,1}) \dot{\cup} \sigma_3(\mathcal{C}_{a0}) \subset U_{a1}$. This implies that

$$c_{i1} + c_{i0} + c_{i-1,1} \leq 2^{a-1-i}3^{b-2}\varphi(m) \quad \text{for } 1 \leq i \leq a-1 \tag{3.3.7}$$

and

$$2c_{a1} + c_{a0} + c_{a-1,1} \leq 3^{b-2}\varphi(m). \tag{3.3.8}$$

By adding up (3.3.6)–(3.3.8), we obtain

$$\sum_{i=0}^{a}(c_{i0} + 2c_{i1}) \leq 2^a 3^{b-2}\varphi(m) \tag{3.3.9}$$

for $a \geq 1$ and $b \geq 2$, which is consistent with (3.3.5), that is, the case when $a = 0$ and $b \geq 2$.

Since the elements in U_{ij} for $j \geq 2$ are multiples of 3^2, the codewords in $\bigcup_{i=0}^{a}\bigcup_{j=2}^{b} U_{ij}$ can be identified with those of a code in $\mathrm{CAC}^e(n = 2^a 3^{b-2}m)$. Hence,

$$\sum_{i=0}^{a}\sum_{j=2}^{b} c_{ij} \leq M_\varphi^e(2^a 3^{b-2}m) \tag{3.3.10}$$

holds. Thus, by (3.3.9) and (3.3.10), we obtain

$$\begin{aligned} M_\varphi^e(2^a 3^b m, 4) &= \sum_{i=0}^{a}\sum_{j=0}^{b} c_{ij} = \sum_{i=0}^{a}(c_{i0} + c_{i1}) + \sum_{i=0}^{a}\sum_{j=2}^{b} c_{ij} \\ &\leq \sum_{i=0}^{a}(c_{i0} + 2c_{i1}) + \sum_{i=0}^{a}\sum_{j=2}^{b} c_{ij} \\ &\leq 2^a 3^{b-2}\varphi(m) + M_\varphi^e(2^a 3^{b-2}m, 4). \end{aligned} \tag{3.3.11}$$

□

Remark that the equality of (3.3.11) holds if $\sum_{i=0}^{a}(c_{i0}+c_{i1}) = \sum_{i=0}^{a}(c_{i0}+2c_{i1})$, that is, if $c_{i1} = 0$ for any $0 \leq i \leq a$.

Theorem 3.3.9. *For $a \geq 0$, $b \geq 2$ and $m \geq 1$ with $\gcd(m, 6) = 1$,*

$$M_\varphi^e(2^a 3^b m, 4) = 2^a 3^{b-2}\varphi(m) + M_\varphi^e(2^a 3^{b-2}m, 4)$$

holds.

Proof: Firstly, we construct a subcode in $\bigcup_{i=0}^{a} U_{i0}$ attaining the upper bound (3.3.9). In this proof, to verify the differences which occur in a code/subcode, we utilize code notations instead of graph representation. Let

$$\Gamma = \{3t+1 : 0 \le t \le 2^a 3^{b-2} m - 1\}.$$

Thus $\mathcal{C}_\Gamma = \{C_x : x \in \Gamma\}$ is a set of $2^a 3^{b-2} m$ codewords. Let $\Delta(\Gamma)$ be the set of differences arising from $\mathcal{C}_\Gamma$, that is, $\Delta(\Gamma) = \bigcup_{x\in\Gamma} \Delta(C_x)$.

(i) Note that if $b \ge 2$, then $3^b m \equiv 3, 9 \pmod{12}$ and $3^b m \equiv 9 \pmod{18}$. Then, $\Delta(\Gamma)$ is reckoned to be a union of disjoint subsets:

$$\begin{aligned}
&\{3t+1 : 0 \le t \le 3^{b-2}m - 1\} = \{1, 4, \ldots, 3^{b-1}m - 2\},\\
&\{6t+2 : 0 \le t \le (3^{b-1}m + \gamma)/4 - 1\} = \Big\{2, 8, \ldots, \frac{3^b m + 3\gamma}{2} - 4\Big\},\\
&\{n - (6t+2) : (3^{b-1}m + \gamma)/4 \le t \le 3^{b-2}m - 1\}\\
&\quad = \{6t+1 : (3^{b-2}m + 1)/2 \le t \le (3^{b-1}m - \gamma - 2)/4\}\\
&\quad = \Big\{3^{b-1}m + 4, 3^{b-1}m + 10, \ldots, \frac{3^b m - 3\gamma}{2} - 2\Big\},\\
&\{9t+3 : 0 \le t \le (3^{b-2}m - 1)/2\} = \Big\{3, 12, \ldots, \frac{3^b m - 3}{2}\Big\},\\
&\{n - (9t+3) : (3^{b-2}m + 1)/2 \le t \le 3^{b-2}m - 1\}\\
&\quad = \{9t+6 : 0 \le t \le (3^{b-2}m - 1)/2 - 1\}\\
&\quad = \Big\{6, 15, \ldots, \frac{3^b m - 1}{2} - 7\Big\},
\end{aligned}$$

where $\gamma = -1$ or 1 depending on whether $3^b m \equiv 3$ or $9 \pmod{12}$. It is easily checked that the elements in each subset are mutually distinct.

(ii) When $a \ge 1$ and $b \ge 2$, $\Delta(\Gamma)$ is given as a union of disjoint subsets

$$\begin{aligned}
&\{3t+1 : 0 \le t \le 2^a 3^{b-2} m - 1\},\\
&\{6t+2 : 0 \le t \le 2^{a-2} 3^{b-1} m + \mu - 1\},\\
&\{n - (6t+2) : 2^{a-2} 3^{b-1} m + \mu \le t \le 2^a 3^{b-2} m - 1\}\\
&\quad = \{6t+4 : 2^{a-1} 3^{b-2} m \le t \le 2^{a-2} 3^{b-1} m - \mu - 1\},\\
&\{9t+3 : 0 \le t \le 2^{a-1} 3^{b-2} m - 1\},\\
&\{n - (9t+3) : 2^{a-1} 3^{b-2} m \le t \le 2^a 3^{b-2} m - 1\}\\
&\quad = \{9t+6 : 0 \le t \le 2^{a-1} 3^{b-2} m - 1\},
\end{aligned}$$

where $\mu = \frac{1}{2}$ or 0 depending on whether $a = 1$ or $a \geq 2$. A straightforward verification ensures that the elements in each subset are mutually distinct.

For $n = 2^a 3^b m$, let $X_0 = \Gamma \cap V_n$, where $V_n = \{x \in \Omega_n : \gcd(x, m) = 1\}$. By noting that

$$\Omega_n = \bigcup_{j=0}^{m-1} \bigcup_{i=0}^{2} \{x \in \Omega_n : x \equiv i \pmod 3,\ x \equiv j \pmod m\},$$

$|X_0| = 2^a 3^{b-2} \varphi(m)$ holds. Thus, in cases (i) or (ii), $\mathcal{C}_{X_0} = \{C_x : x \in X_0\}$ can be considered as a subcode satisfying the inequality of (3.3.9).

Let $\mathcal{C}_{X_0 \cup X'} = \mathcal{C}_{X_0} \cup \mathcal{C}_{X'}$ be a code in $\mathrm{CAC}^e(V_n)$ for some subset $X' \subset \bigcup_{i=0}^{a} \bigcup_{j=2}^{b} U_{ij}$. Recall that $c_{01} = c_{11} = \cdots = c_{a1} = 0$ is necessary for the equality of (3.3.11) to hold. If this is the case, then $\mathcal{C}_{X_0}$ never affects the choice of codewords in $\mathcal{C}_{X'}$. By noting $\bigcup_{i=0}^{a} \bigcup_{j=2}^{b} U_{ij} = 3^2 V_{2^a 3^{b-2} m}$, it is easy to see that a subcode $\mathcal{C}_{X'}$ with $|\mathcal{C}_{X'}| = M_\varphi^e(2^a 3^{b-2} m)$ can be obtained by multiplying all the codewords in an optimal code in $\mathrm{CAC}^e(V_{2^a 3^{b-2} m})$ by 3^2. Then $\mathcal{C}_{X_0 \cup X'}$ is an optimal code in $\mathrm{CAC}^e(V_n)$. □

Corollary 3.3.10. *For $a \geq 0$, $b \geq 2$ and $m \geq 1$ with $\gcd(m, 6) = 1$,*

$$M_\varphi^e(2^a 3^b m, 4) = \begin{cases} 2^{a-3}(3^b - 1)\varphi(m) + M_\varphi^e(2^a m, 4) & \text{if } b \text{ is even,} \\ 2^{a-3}(3^b - 3)\varphi(m) + M_\varphi^e(2^a 3m, 4) & \text{if } b \text{ is odd.} \end{cases}$$

Proof: By using the recurrence relation repeatedly in Theorem 3.3.9, the assertion can be proved. □

Noting (3.3.2) and $\sum_{d|m} \varphi(\frac{m}{d}) = m$, we have the following theorem:

Theorem 3.3.11. *For $a \geq 0$, $b \geq 2$ and $m \geq 1$ with $\gcd(m, 6) = 1$,*

$$M^e(2^a 3^b m, 4) = \begin{cases} 2^{a-3}(3^b - 1)m + M^e(2^a m, 4) & \text{if } b \text{ is even,} \\ 2^{a-3}(3^b - 3)m + M^e(2^a 3m, 4) & \text{if } b \text{ is odd.} \end{cases} \tag{3.3.12}$$

It turns out from Theorem 3.3.11 that the problem of finding $M^e(2^a 3^b m, 4)$ can be reduced to the problem of finding $M^e(2^a m, 4)$ and $M^e(2^a 3m, 4)$.

3.3.4 Subcodes in σ_2-orbits and σ_3-orbits

It follows from Lemma 3.3.5(iii) that the vertices in U_{aj} are partitioned into disjoint cycles by the action of σ_2. We call these cycles σ_2-*orbits*. Similarly, it follows from Lemma 3.3.6(iii) that the vertices in U_{ib} are partitioned into σ_3-*orbits*. Theorem 3.3.11 says that, in order to determine $M^e(2^a3^bm, 4)$, the evaluation of $M^e(2^am, 4)$ and $M^e(2^a3m, 4)$ is imperative. Thus it is necessary to know the lengths of the σ_2-orbits in each U_{aj} for $j = 0, 1$ and the σ_3-orbits in each U_{ib} for $0 \le i \le a$.

Lemma 3.3.12. *For $0 \le j \le b$ and $(j, m) \ne (b, 1)$, the vertices in U_{aj} are partitioned into σ_2-orbits of uniform length* $\mathrm{sord}_{3^{b-j}m}(2)$.

Proof: From Lemma 3.3.5(iii), for any $x = 2^a3^jy \in U_{aj}$, there exists the smallest positive integer κ such that $\sigma_2^\kappa(x) = 2^\kappa x \equiv \pm x \pmod n$, which can be reduced to $2^\kappa y \equiv \pm y \pmod{3^{b-j}m}$. Thus $|y\langle 2\rangle_{3^{b-j}m}| = \kappa$. On the other hand, $2^\kappa \equiv \pm 1 \pmod{3^{b-j}m}$ holds since $\gcd(y, 3^{b-j}m) = 1$. Hence $\kappa = |y\langle 2\rangle_{3^{b-j}m}| = |\langle 2\rangle_{3^{b-j}m}| = \mathrm{sord}_{3^{b-j}m}(2)$. □

Lemma 3.3.13. *For $0 \le i \le a$ and $(i, m) \ne (a, 1)$, the vertices in U_{ib} are partitioned into σ_3-orbits of uniform length* $\mathrm{sord}_{2^{a-i}m}(3)$.

Proof: The proof is almost the same as that of Lemma 3.3.12. □

Now we discuss the subcodes in each σ_2-orbit and σ_3-orbit.

Let $t_i = \mathrm{sord}_{2^im}(3)$ for $i \ge 0$. From Lemma 3.3.13, for $0 \le i \le a$, the vertices in U_{ib} are partitioned into σ_3-orbits of uniform length t_{a-i}. Let $T_{ib} = (x_0^{(i)}, x_1^{(i)}, \ldots, x_{t_{a-i}-1}^{(i)})$ be a σ_3-orbit in U_{ib} satisfying $\sigma_3(x_r^{(i)}) = x_{r+1}^{(i)}$ for $0 \le r \le t_{a-i}-2$ and $\sigma_3(x_{t_{a-i}-1}^{(i)}) = x_0^{(i)}$. Here we should remark that, although T_{ib} is defined as an ordered list, it is viewed as a set $\{x_0^{(i)}, x_1^{(i)}, \ldots, x_{t_{a-i}-1}^{(i)}\}$ depending on the context.

For $0 \le i \le a-2$, $\sigma_2(T_{ib}) = T_{i+1,b}$ is a bijection or a 2-to-1 onto mapping depending on whether $t_{a-i} = t_{a-i-1}$ or $2t_{a-i-1}$. If $\sigma_2(T_{ib}) = T_{i+1,b}$ is a bijection, that is, $t_{a-i} = t_{a-i-1}$, then there is a companion σ_3-orbit $\bar{T}_{ib} = (\bar{x}_0^{(i)}, \bar{x}_1^{(i)}, \ldots, \bar{x}_{t_{a-i}-1}^{(i)})$ in U_{ib} such that $\sigma_2(\bar{x}_r^{(i)}) = \sigma_2(x_r^{(i)}) = x_r^{(i+1)}$ and thus $\sigma_2(\bar{T}_{ib}) = \sigma_2(T_{ib}) = T_{i+1,b}$ (see Figure 3.3.3). If $\sigma_2(T_{ib}) = T_{i+1,b}$ is a 2-to-1 onto mapping, that is, $t_{a-i} = 2t_{a-i-1}$, then there are $t_{a-i}/2$ pairs of vertices $\{x_r^{(i)}, x_{\frac{t_{a-i}}{2}+r}^{(i)}\}$ in U_{ib} satisfying $\sigma_2(x_r^{(i)}) = \sigma_2(x_{\frac{t_{a-i}}{2}+r}^{(i)}) = x_r^{(i+1)}$ (see Figure 3.3.4).

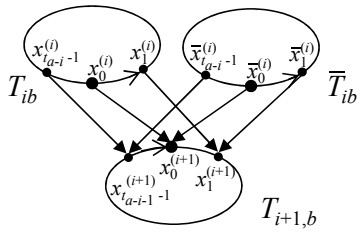

Figure 3.3.3: The adjacency relation between $T_{ib} \cup \bar{T}_{ib}$ and $T_{i+1,b}$ when $t_{a-i} = t_{a-i-1}$

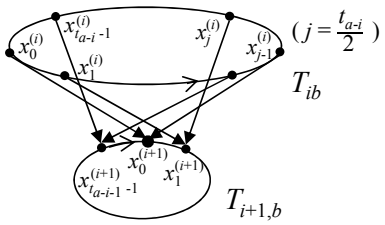

Figure 3.3.4: The adjacency relation between T_{ib} and $T_{i+1,b}$ when $t_{a-i} = 2t_{a-i-1}$

We consider a subcode on the vertex set of $\sigma_2^{-1}(T_{i+1,b}) \cup T_{i+1,b}$, where $\sigma_2^{-1}(T_{i+1,b}) = T_{ib} \cup \bar{T}_{ib}$ or T_{ib} depending on whether $t_{a-i} = t_{a-i-1}$ or $2t_{a-i-1}$. Let $S = \mathcal{C} \cap (\sigma_2^{-1}(T_{i+1,b}) \cup T_{i+1,b})$ be the subcode. We want to maximize the cardinality of S.

Lemma 3.3.14. *For $0 \leq i \leq a-2$, let $S = \mathcal{C} \cap (\sigma_2^{-1}(T_{i+1,b}) \cup T_{i+1,b})$ be a subcode. Then (i) $S \cap \sigma_2^{-1}(\sigma_3(S)) = \emptyset$ and $S \cap \sigma_3^{-1}(\sigma_2(S)) = \emptyset$ hold, and (ii) S, $\sigma_2^{-1}(S)$ and $\sigma_3^{-1}(S)$ are mutually disjoint.*

Proof: (i) Note that, for any $x \in U_{0j}$ and $y \in U_{i0}$, $G(\Omega_n) = (\Omega_n, E)$ does not have $\sigma_2^{-1}(x)$ and $\sigma_3^{-1}(y)$, respectively. For any vertex $x \in \Omega_n \setminus U_{0j}$, there exists a vertex $\sigma_3(x)$ such that $(x, \sigma_3(x)) \in E$ and $(\sigma_2^{-1}(\sigma_3(x)), \sigma_3(x)) \in E$. By Lemma 3.3.1(ii), if $x \in S$, then $\sigma_3(x) \notin S$ and $\sigma_2^{-1}(\sigma_3(x)) \notin S$. Thus $S \cap \sigma_2^{-1}(\sigma_3(S)) = \emptyset$. On the other hand, for any vertex $x \in \Omega_n \setminus U_{i0}$, there exists a vertex $\sigma_2(x)$ such that $(x, \sigma_2(x)) \in E$ and $(\sigma_3^{-1}(\sigma_2(x)), \sigma_2(x)) \in E$. Then, again from Lemma 3.3.1(ii), we have $S \cap \sigma_3^{-1}(\sigma_2(S)) = \emptyset$.

(ii) Since $(x, \sigma_2(x)) \in E$ and $(x, \sigma_3(x)) \in E$ for any vertex $x \in \Omega_n$, it is clear that S, $\sigma_2(S)$ and $\sigma_3(S)$ are mutually disjoint. As in the proof of (i), for any vertex $x \in \Omega_n$, either $\sigma_2^{-1}(x) \notin \Omega_n$ or $(\sigma_2^{-1}(x), x) \in E$, and

either $\sigma_3^{-1}(x) \notin \Omega_n$ or $(\sigma_3^{-1}(x), x) \in E$. Thus we have $S \cap \sigma_2^{-1}(S) = \emptyset$ and $S \cap \sigma_3^{-1}(S) = \emptyset$. Moreover, $\sigma_2^{-1}(S) \cap \sigma_3^{-1}(S) = \emptyset$ holds by Lemma 3.3.1(ii). □

Since T_{ib}, $\bar{T}_{ib}$ ($\bar{T}_{ib}$ exists only if $t_{a-i} = t_{a-i-1}$) and $T_{i+1,b}$ are mutually disjoint, we have

$$|S| = |S \cap \sigma_2^{-1}(T_{i+1,b})| + |S \cap T_{i+1,b}|. \tag{3.3.13}$$

In the rest of this section, we will give the maximum of $|S|$ in (3.3.13). In order to do that, we first define two specific types of graphs which appear in the undirected graph representation G' of $G(\Omega_n)$ defined in Section 3.3.1.

A *wheel* on $2w$ vertices is a graph consisting of a cycle of length $2w$ with edges as shown by Figure 3.3.5, and a *biwheel* on $2w$ vertices is a graph consisting of two vertex disjoint cycles of the same length w with edges as shown by Figure 3.3.6.

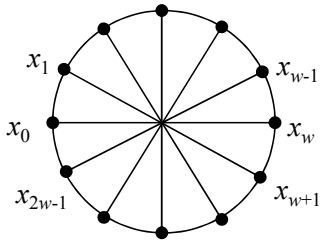

Figure 3.3.5: A wheel on $2w$ vertices

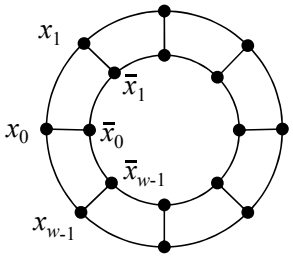

Figure 3.3.6: A biwheel on $2w$ vertices

By Lemma 3.3.2, σ_3-orbits T_{ib} and $\bar{T}_{ib}$ of $G(U_{ib})$ for $0 \leq i \leq a-2$ in Figures 3.3.3 and 3.3.4 correspond to a biwheel and a wheel in $G'(U_{ib})$, respectively. Then the following lemma is easily verified:

Lemma 3.3.15. *Let W_1 and W_2 be a wheel and a biwheel on $2w$ vertices, respectively, and S_i be a maximum independent set of W_i. Then*

$$|S_1| = \begin{cases} w-1 & \text{if } w \text{ is even,} \\ w & \text{if } w \text{ is odd,} \end{cases} \quad \text{and} \quad |S_2| = \begin{cases} w & \text{if } w \text{ is even,} \\ w-1 & \text{if } w \text{ is odd.} \end{cases}$$

Lemma 3.3.16. *For $0 \leq i \leq a-2$, let $S = \mathcal{C} \cap (\sigma_2^{-1}(T_{i+1,b}) \cup T_{i+1,b})$ be a subcode. Then*

$$\max\{|S|\} = \begin{cases} t_{a-i-1} & \text{for (A3) and (D3),} \\ t_{a-i-1} - 1 & \text{for (B3) and (C3),} \end{cases}$$

where (A3)–(D3) are the cases in Table 3.3.1 with $j = a - i$.

Table 3.3.1: Four cases for (t_{j-1}, t_j)

		t_j	
		t_{j-1}	$2t_{j-1}$
t_{j-1}	even	(A3)	(B3)
	odd	(C3)	(D3)

Proof: Firstly, we show the upper bound of $|S|$. In the cases of (A3) and (C3), we have $t_{a-i} = t_{a-i-1}$. For any $x_r^{(i+1)} \in T_{i+1,b}$ $(0 \leq r \leq t_{a-i} - 1)$, there exist $x_r^{(i)} \in T_{ib}$ and $\bar{x}_r^{(i)} \in \bar{T}_{ib}$ satisfying $\sigma_2(x_r^{(i)}) = \sigma_2(\bar{x}_r^{(i)}) = x_r^{(i+1)}$ as shown in Figure 3.3.3. In the cases of (B3) and (D3), we have $t_{a-i} = 2t_{a-i-1}$ and $\bar{T}_{ib} = \emptyset$. For any $x_r^{(i+1)} \in T_{i+1,b}$ $(0 \leq r \leq \frac{t_{a-i}}{2} - 1)$, there exist $x_r^{(i)}, x_{t_{a-i}/2+r}^{(i)} \in T_{ib}$ satisfying $\sigma_2(x_r^{(i)}) = \sigma_2(x_{t_{a-i}/2+r}^{(i)}) = x_r^{(i+1)}$ as shown in Figure 3.3.4.

By Lemma 3.3.14, for any vertex $x_r^{(i+1)} \in T_{i+1,b}$, at most one of $x_r^{(i+1)}$, $\sigma_2^{-1}(x_r^{(i+1)})$ and $\sigma_3^{-1}(x_r^{(i+1)})$ can belong to S. This implies that if $x_r^{(i+1)} \in S \cap T_{i+1,b}$, then

$$\begin{cases} S \cap \left(\{x_r^{(i)}, \bar{x}_r^{(i)}\} \cup \{x_{r-1}^{(i+1)}\}\right) = \emptyset & \text{for (A3) and (C3),} \\ S \cap \left(\{x_r^{(i)}, x_{t_{a-i}/2+r}^{(i)}\} \cup \{x_{r-1}^{(i+1)}\}\right) = \emptyset & \text{for (B3) and (D3)} \end{cases} \tag{3.3.14}$$

holds and since $S \cap \sigma_2^{-1}(\sigma_3(S)) = \emptyset$,

$$\begin{cases} S \cap \{x_{r+1}^{(i)}, \bar{x}_{r+1}^{(i)}\} = \emptyset & \text{for (A3) and (C3),} \\ S \cap \{x_{r+1}^{(i)}, x_{t_{a-i}/2+r+1}^{(i)}\} = \emptyset & \text{for (B3) and (D3)} \end{cases} \tag{3.3.15}$$

holds as well. Note that the distance between any two distinct vertices $x_r^{(i+1)}$, $x_{r'}^{(i+1)} \in S \cap T_{i+1,b}$ is at least 2, that is, $|r'-r| \geq 2$. From (3.3.14) and (3.3.15), if $x_r^{(i+1)} \in S \cap T_{i+1,b}$, then

$$\begin{cases} S \cap \{x_r^{(i)}, \bar{x}_r^{(i)}, x_{r+1}^{(i)}, \bar{x}_{r+1}^{(i)}\} = \emptyset & \text{for (A3) and (C3),} \\ S \cap \{x_r^{(i)}, x_{t_{a-i}/2+r}^{(i)}, x_{r+1}^{(i)}, x_{t_{a-i}/2+r+1}^{(i)}\} = \emptyset & \text{for (B3) and (D3).} \end{cases}$$

Thus the number of vertices in $\sigma_2^{-1}(T_{i+1,b})$ which can belong to S is

$$|\sigma_2^{-1}(T_{i+1,b})| - 4|S \cap T_{i+1,b}|.$$

Obviously, at most one of the two corresponding vertices in $\sigma_2^{-1}(x_r^{(i+1)}) \subset \sigma_2^{-1}(T_{i+1,b})$ can belong to S. Thus we have

$$|S \cap \sigma_2^{-1}(T_{i+1,b})| \leq \left\lfloor \frac{|\sigma_2^{-1}(T_{i+1,b})| - 4|S \cap T_{i+1,b}|}{2} \right\rfloor.$$

Let $|S \cap T_{i+1,b}| = k$. By noting (3.3.13) and substituting t_{a-i-1} for t_{a-i}, we have

$$\begin{aligned} |S| &\leq \begin{cases} \left\lfloor \frac{2t_{a-i}-4k)}{2} \right\rfloor + k & \text{for (A3) and (C3),} \\ \left\lfloor \frac{t_{a-i}-4k)}{2} \right\rfloor + k & \text{for (B3) and (D3),} \end{cases} \\ &\leq t_{a-i-1} - k. \end{aligned}$$

Then for $k \geq 0$, we have $|S| \leq t_{a-i-1}$. Note that $G'(\sigma_2^{-1}(T_{i+1,b}))$ is a biwheel on $2t_{a-i} (= 2t_{a-i-1})$ vertices for cases (A3) and (C3) with $j = a-i$, or a wheel on $t_{a-i} (= 2t_{a-i-1})$ vertices for cases (B3) and (D3) with $j = a-i$ (in this case $\bar{T}_{ib} = \emptyset$). Therefore, when $k = 0$, the problem of maximizing $|S|$ is equivalent to that of finding a maximum independent vertex set in $G'(T_{ib} \cup \bar{T}_{ib})$. Then Lemma 3.3.15 shows the assertion. □

Next, we discuss the subcodes derived from σ_2-orbits in the graph $G(U_{a,b-1} \cup U_{ab})$.

Let $d_i = \mathrm{sord}_{3^i m}(2)$ for $i \geq 0$. From Lemma 3.3.12, for $0 \leq i \leq b$, the vertices in U_{ai} are partitioned into σ_2-orbits of uniform length d_{b-i}. Let $D_{ai} = (x_0^{(i)}, x_1^{(i)}, \ldots, x_{d_{b-i}-1}^{(i)})$ be a σ_2-orbit in U_{ai} satisfying $\sigma_2(x_r^{(i)}) = x_{r+1}^{(i)}$ for $0 \leq r \leq d_{b-i} - 2$ and $\sigma_2(x_{d_{b-i}-1}^{(i)}) = x_0^{(i)}$. We will view D_{ai} also as a set $\{x_0^{(i)}, x_1^{(i)}, \ldots, x_{d_{b-i}-1}^{(i)}\}$ depending on the context.

Note that $\sigma_3(D_{a,b-1}) = D_{ab}$ is a bijection or a 2-to-1 onto mapping depending on whether $d_1 = d_0$ or $2d_0$. If $\sigma_3(D_{a,b-1}) = D_{ab}$ is a bijection, that is, $d_1 = d_0$, then there is a companion σ_2-orbit $\bar{D}_{a,b-1} = (\bar{x}_0^{(b-1)}, \bar{x}_1^{(b-1)}, \ldots, \bar{x}_{d_1-1}^{(b-1)})$ in $U_{a,b-1}$ satisfying $\sigma_3(\bar{x}_r^{(b-1)}) = \sigma_3(x_r^{(b-1)}) = x_r^{(b)}$ such that $\sigma_3(\bar{D}_{a,b-1}) = \sigma_3(D_{a,b-1}) = D_{ab}$ (see Figure 3.3.7). If $\sigma_3(D_{a,b-1}) = D_{ab}$ is a 2-to-1 onto mapping, that is, $d_1 = 2d_0$, then there are $d_1/2$ pairs of vertices $\{x_r^{(b-1)}, x_{\frac{d_1}{2}+r}^{(b-1)}\}$ in $U_{a,b-1}$ satisfying $\sigma_3(x_r^{(b-1)}) = \sigma_3(x_{\frac{d_1}{2}+r}^{(b-1)}) = x_r^{(b)}$ (see Figure 3.3.8).

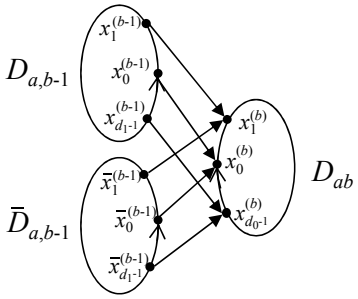

Figure 3.3.7: The adjacency relation between $D_{a,b-1} \cup \bar{D}_{a,b-1}$ and D_{ab} when $d_1 = d_0$

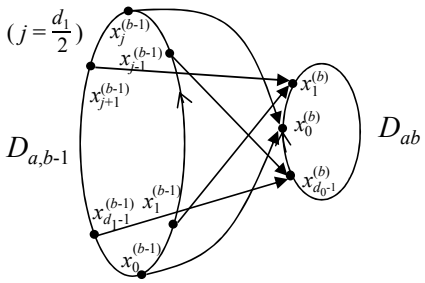

Figure 3.3.8: The adjacency relation between $D_{a,b-1}$ and D_{ab} when $d_1 = 2d_0$

Let $S = \mathcal{C} \cap (\sigma_3^{-1}(D_{ab}) \cup D_{ab})$. Since $D_{a,b-1}$, $\bar{D}_{a,b-1}$ ($\bar{D}_{a,b-1}$ exists only if $d_1 = d_0$) and D_{ab} are disjoint, we have

$$|S| = |S \cap \sigma_3^{-1}(D_{ab})| + |S \cap D_{ab}|. \tag{3.3.16}$$

Lemma 3.3.17. *Let $S = \mathcal{C} \cap (\sigma_3^{-1}(D_{ab}) \cup D_{ab})$ be a subcode. Then*

$$\max\{|S|\} = \begin{cases} d_0 & \textit{for (A2) and (D2),} \\ d_0 - 1 & \textit{for (B2) and (C2),} \end{cases}$$

where (A2)–(D2) are the cases in Table 3.3.2.

Table 3.3.2: Four cases for (d_0, d_1)

		d_1	
		d_0	$2d_0$
d_0	even	(A2)	(B2)
	odd	(C2)	(D2)

Proof: The proof can be shown in a way similar to that of Lemma 3.3.16 by considering σ_2-orbits instead of σ_3-orbits. □

3.3.5 The recurrence formula of $M_\varphi^e(2^a m)$ with respect to a

In this subsection, we consider the case $n = 2^a m$ with $a \geq 2$ and $\gcd(m, 6) = 1$.

Let $\tau_{i0} = |\mathcal{C} \cap \sigma_2^{-1}(T_{i+1,0})| = |\mathcal{C} \cap (T_{i0} \cup \bar{T}_{i0})|$, where $\bar{T}_{i0}$ does not exist if $t_{a-i} = 2t_{a-i-1}$ or $i \geq a-1$. Then, the size of a code $\mathcal{C} \in \mathrm{CAC}^e(V_n)$ is given by

$$|\mathcal{C}| = \sum_{i=0}^{a} c_{i0} = \sum_{i=0}^{a-1} \frac{|U_{i0}|}{2t_{a-i-1}} \tau_{i0} + c_{a0},$$

where $c_{ij} = |\mathcal{C} \cap U_{ij}|$.

Lemma 3.3.18. *For $a \geq 2$ and $m \geq 1$ with $\gcd(m, 6) = 1$ and $(a, m) \neq (2, 1)$,*

$$c_{00} + c_{10} \leq |U_{10}|$$

holds and there exists an optimal code in $\mathrm{CAC}^e(V_{2^a m})$ satisfying $c_{10} = 0$ and

$$c_{00} = \begin{cases} |U_{10}| & \text{for (A3) and (D3),} \\ |U_{10}| - \dfrac{|U_{10}|}{t_{a-1}} & \text{for (B3) and (C3),} \end{cases}$$

where (A3)–(D3) are the cases in Table 3.3.1 with $j = a$.

Proof: When $(a, m) \neq (2, 1)$, it follows from Lemmas 3.3.5 and 3.3.6 that

$$\mathcal{C}_{10} \,\dot\cup\, \sigma_2(\mathcal{C}_{00}) \,\dot\cup\, \sigma_3(\mathcal{C}_{10}) \subset U_{10},$$

which implies that $c_{00} + 2c_{10} \le |U_{10}|$. Then we have

$$\begin{cases} \frac{|U_{00}|}{2t_{a-1}}\tau_{00} + \frac{|U_{10}|}{t_{a-1}}\tau_{10} \le |U_{10}| & \text{if } t_{a-1} = t_{a-2}, \\ \frac{|U_{00}|}{2t_{a-1}}\tau_{00} + \frac{2|U_{10}|}{t_{a-1}}\tau_{10} \le |U_{10}| & \text{if } t_{a-1} = 2t_{a-2}. \end{cases}$$

Thus

$$\begin{cases} \tau_{00} + \tau_{10} \le t_{a-1} & \text{if } t_{a-1} = t_{a-2}, \\ \tau_{00} + 2\tau_{10} \le t_{a-1} & \text{if } t_{a-1} = 2t_{a-2}. \end{cases} \tag{3.3.17}$$

Note that the maximum value of $c_{00} + c_{10}$ can be derived by maximizing $\tau_{00} + \tau_{10}$. It follows from Lemma 3.3.16 with $i = 0$ that the equality of (3.3.17) holds when $\tau_{00} = t_{a-1}$ and $\tau_{10} = 0$ for cases (A3) and (D3). That is, the equality of $c_{00} + c_{10} \le |U_{10}|$ also holds when $c_{00} = |U_{10}|$ and $c_{10} = 0$. In fact, if (t_{a-1}, t_a) is case (A3) or (D3) and there exists an optimal code in $\mathrm{CAC}^e(V_{2^a m}, 4)$ with $\boldsymbol{c}^* = (c^*_{00}, c^*_{10}, c^*_{20}, \ldots, c^*_{a0})$, then there also exists an optimal code with $\boldsymbol{c}^{**} = (c^{**}_{00}, c^{**}_{10}, c^*_{20}, \ldots, c^*_{a0})$ such that $c^{**}_{00} = |U_{10}|$ and $c^{**}_{10} = 0$ since $c^*_{00} + c^*_{10} \le |U_{10}| = c^{**}_{00}$ and any vertex in U_{00} is never adjacent to vertices in $\bigcup_{i=2}^{a} U_{i0}$.

By Lemma 3.3.16, for cases (B3) and (C3), (3.3.17) has no solutions which attain the equality since $\tau_{00} \le t_{a-1} - 1$. In this case, $\tau_{00} = t_{a-1} - 1$ and $t_{10} = 0$ maximize $c_{00} + c_{10}$, that is, an optimal solution of $c_{00} + c_{10} \le |U_{10}|$ is

$$c_{00} = \frac{|U_{10}|}{t_{a-1}}(t_{a-1} - 1) \quad \text{and} \quad c_{10} = 0, \tag{3.3.18}$$

and then there exists an optimal code in $\mathrm{CAC}^e(V_{2^a m})$ satisfying (3.3.18).

When $(a, m) = (2, 1)$, that is, $n = 4$,

$$U_{00} = \{1\},\ U_{10} = \{2\},\ U_{20} = \emptyset$$

and thus $\mathrm{CAC}^e(4, 4) = \{\{0, 1, 2, 3\}\}$ and $M^e(4) = M^e_\varphi(4, 1) = 1$. □

For a code $\mathcal{C} \in \mathrm{CAC}^e(V_n)$, let $X = \{x : C_x \in \mathcal{C}\}$. Then c_{ij} can be viewed as $c_{ij} = |X \cap U_{ij}|$. Since any element in $V' = \sum_{i=2}^{a} U_{i0}$ is a multiple of 2^2, a subcode $\mathcal{C}_{X \cap V'}$ can be considered as a code in $\mathrm{CAC}^e(2^2 V_{2^{a-2} m})$ and thus $|\mathcal{C}_{X \cap V'}| = M^e_\varphi(2^{a-2} m, 4)$. Together with Lemma 3.3.18, we have the following:

Theorem 3.3.19. *For $a \geq 2$, $m \geq 1$ with $\gcd(m,6) = 1$ and $(a,m) \neq (2,1)$,*

$$M_\varphi^e(2^a m, 4) = \begin{cases} 2^{a-3}\varphi(m) + M_\varphi^e(2^{a-2}m, 4) & \text{for (A3) and (D3),} \\ 2^{a-3}\Big(1 - \dfrac{1}{t_{a-1}}\Big)\varphi(m) + M_\varphi^e(2^{a-2}m, 4) & \text{for (B3) and (C3),} \end{cases}$$

where (A3)–(D3) are the cases in Table 3.3.1 with $j = a$.

Recall that $M_\varphi^e(2^a, 4) = M^e(2^a, 4)$ for $a \geq 2$ and $M^e(4,4) = 1$. It follows from Lemma 3.1.24 that, if $a \geq 4$ and $m = 1$, then, for any $4 \leq i \leq a$, the relation between $t_{i-1} = \mathrm{sord}_{2^{i-1}}(3) = 2^{i-3}$ and $t_i = \mathrm{sord}_{2^i}(3) = 2^{i-2}$ falls into case (C3), and the relation between $t_3 = 1$ and $t_4 = 2$ falls into case (A3) in Table 3.3.1. Then we have the following as corollaries of Theorem 3.3.19:

Corollary 3.3.20 ([49, Lemma 2])**.** *For any $a \geq 2$,*

$$M^e(2^a, 4) = \begin{cases} \frac{1}{6}(2^a - 3a + 7) & \text{if } a \text{ is odd,} \\ \frac{1}{6}(2^a - 3a + 8) & \text{if } a \text{ is even.} \end{cases}$$

Corollary 3.3.21. *For $a \geq 2$ and $m \geq 5$ with $\gcd(m,6) = 1$, let $t_i = \mathrm{sord}_{2^i m}(3)$ $(0 \leq i \leq a)$, $u = v_2(t_2) + 2$, and $\beta_u^+ = \max\{0, \lceil \frac{a-u}{2} \rceil\}$. Then*

$$M_\varphi^e(2^a m, 4) = \begin{cases} \frac{\varphi(m)}{6}(2^a - 2) - \frac{\varphi(m)}{2t_2}(a-3) + M_\varphi^e(2m, 4) \\ \qquad \text{if } a \text{ is odd and } u = 2, \\ \frac{\varphi(m)}{6}(2^a - 2) - \frac{\varphi(m)}{t_2}2^{u-2}\beta_u^+ + M_\varphi^e(2m, 4) \\ \qquad \text{if } a \text{ is odd and } u \geq 3, \\ \frac{\varphi(m)}{6}(2^a - 1) - \frac{\varphi(m)}{2t_2}(a-1) + M_\varphi^e(m, 4) \\ \qquad \text{if } a \text{ is even and } u = 2, \\ \frac{\varphi(m)}{6}(2^a - 1) - \frac{\varphi(m)}{t_2}2^{u-2}\beta_u^+ + M_\varphi^e(m, 4) \\ \qquad \text{if } a \text{ is even, } u \geq 3 \text{ and } -1 \notin (3)_m, \\ \frac{\varphi(m)}{6}(2^a - 1) - \frac{\varphi(m)}{t_2}\big(2^{u-2}\beta_u^+ + 1\big) + M_\varphi^e(m, 4) \\ \qquad \text{if } a \text{ is even, } u \geq 4 \text{ and } -1 \in (3)_m. \end{cases}$$

Proof: Note that, if $u = 3$, that is, $v_2(t_2) = 1$, then $-1 \notin (3)_m$. From Corollary 3.1.26, we can tell the relation between t_i and t_{i-1} for $1 \leq i \leq a$ as in Table 3.3.3, where the cases (A3)–(D3) are in Table 3.3.1.

Table 3.3.3: The relation between t_i and t_{i-1}

		(t_i, t_{i-1})				
		$i=1$	$i=2$	$i=3$	$i \in [4,u]$	$i \in [u+1,a]$
$u=2$		(C3)		(D3)	(B3)	
$u=3$	t_0: even	(A3)		(A3)	(B3)	
	t_0: odd	(C3)	(D3)			
$u \geq 4$	$-1 \in (3)_m$	(A3)	(B3)	(A3)		(B3)
	$-1 \notin (3)_m$		(A3)			

Let $\alpha = \lfloor \frac{a}{2} \rfloor$ and $\beta_u = \lceil \frac{a-u}{2} \rceil$. By applying Theorem 3.3.19 repeatedly together with (3.3.4), we have

$$M_\varphi^e(2^a m) = \begin{cases} \sum_{i=1}^{\alpha} |U_{2i-1,0}| - \sum_{j=1}^{\beta_u} \frac{|U_{2j-1,0}|}{t_{a-2j+1}} + \mu & \text{if } \beta_u \geq 1, \\ \sum_{i=1}^{\alpha} |U_{2i-1,0}| + \mu & \text{if } \beta_u \leq 0, \end{cases} \tag{3.3.19}$$

where

$$\mu = \begin{cases} \frac{\varphi(m)}{t_2} + M_\varphi^e(2m,4) & \text{if } a \text{ is odd and } u=2, \\ M_\varphi^e(2m,4) & \text{if } a \text{ is odd and } u \geq 3, \\ -\frac{\varphi(m)}{2t_2} + M_\varphi^e(m,4) & \text{if } a \text{ is even and } u=2, \\ M_\varphi^e(m,4) & \text{if } a \text{ is even, } u \geq 3 \text{ and } -1 \notin (3)_m. \\ -\frac{\varphi(m)}{t_2} + M_\varphi^e(m,4) & \text{if } a \text{ is even, } u \geq 4 \text{ and } -1 \in (3)_m. \end{cases}$$

This completes the proof. □

Example 3.3.22. (1) The case when $n = 2^a m = 2^4 = 16$. Then we have

$$M^e(16,4) = M_\varphi^e(16,4) = \frac{1}{3}(2^3+4) - \frac{4}{2} = 2$$

from Corollary 3.3.20. For example, $\mathcal{C}_1 = \{\{0,1,2,3\},\{0,4,8,12\}\}$, which is an optimal code in $\mathrm{CAC}^e(16,4)$.

(2) The case when $n = 2^a m = 2^4 7 = 112$. Note that $t_2 = \mathrm{sord}_{112}(3) = 3$, $u = v_2(t_2)+2 = 2$, $\varphi(7) = 6$ and $M_\varphi^e(7,4) = 1$. Then from (3.3.2) and Corollary 3.3.21, we have

$$\begin{aligned} M^e(112,4) &= \sum_{d|7} M_\varphi^e(2^4 d) = M_\varphi^e(16) + M_\varphi^e(112,4) \\ &= M_\varphi^e(16,4) + \frac{\varphi(7)}{6}(2^4-1) - \frac{\varphi(7)}{6}(4-1) + M_\varphi^e(7,4) \\ &= 2 + 15 - 3 + 1 = 15. \end{aligned}$$

In this case, $V_{112} = \bigcup_{i=0}^{4} U_{i0}$ and the following are the σ_3-orbits

$$\begin{aligned}
&T_{00} = (1, 3, 9, 27, 31, 19, 55, 53, 47, 29, 25, 37),\\
&T'_{00} = (5, 15, 45, 23, 43, 17, 51, 41, 11, 33, 13, 39),\\
&T_{10} = (2, 6, 18, 54, 50, 38),\ \ T'_{10} = (10, 30, 22, 46, 26, 34),\\
&T_{20} = (4, 12, 36),\ \ T'_{20} = (20, 52, 44),\\
&T_{30} = (8, 24, 40),\ \ T_{40} = (16, 48, 32),
\end{aligned}$$

such that $U_{i0} = T_{i0} \cup T'_{i0}$ for $i = 0, 1, 2$, $T_{30} = U_{30}$ and $T_{40} = U_{40}$.

Since the relation between $t_4 = |T_{00}| = |T'_{00}|$ and $t_3 = |T_{10}| = |T'_{10}|$ is case (B3) in Table 3.3.1 with $j = 4$, we can choose $t_3 - 1 = 5$ vertices (as codewords) each from T_{00} and T'_{00}, and no vertex from T_{10} and T'_{10} (see Lemma 3.3.16 and its proof). Similarly, since the relation between $t_2 = |T_{20}| = |T'_{20}|$ and $t_1 = |T_{30}|$ is case (C3) in Table 3.3.1 with $j = 2$, we can choose $t_1 - 1 = 2$ vertices from $T_{20} \cup T'_{20}$ and no vertex from T_{30}. It is obvious that only one vertex can be chosen from $T_{40} = U_{40}$, since $U_{40} = 2^4 V_7$ and $M^e_\varphi(7, 4) = 1$. Hence, in total, we can get $13 (= 5 + 5 + 2 + 1)$ codewords. For example,

$$\begin{aligned}
\mathcal{C}_2 = \big\{&\{0, 1, 2, 3\}, \{0, 9, 18, 27\}, \{0, 31, 64, 93\}, \{0, 53, 106, 47\},\\
&\{0, 29, 58, 87\}, \{0, 5, 10, 15\}, \{0, 45, 90, 23\}, \{0, 43, 86, 17\},\\
&\{0, 41, 82, 2\}, \{0, 33, 66, 99\}, \{0, 4, 8, 12\}, \{0, 52, 104, 44\}, \{0, 16, 32, 48\}\big\}
\end{aligned}$$

is an optimal code in $\mathrm{CAC}^e(V_{112})$.

By noting $G(\Omega_{112}) = G(7V_{16} \cup V_{112})$, we have $\mathcal{C} = 7\mathcal{C}_1 \cup \mathcal{C}_2$ as an optimal code in $\mathrm{CAC}^e(112, 4)$.

So far, we have not found formulae for $M^e_\varphi(m, 4)$ and $M^e_\varphi(2m, 4)$ for general m with $\gcd(m, 6) = 1$, which means that we cannot develop the last step of calculating $M^e(2^a 3^b m, 4)$. However, if m is small, those values can be obtained by directly examining $G(\Omega_m)$ and $G(\Omega_{2m})$, and accordingly similar formulae to Corollary 3.3.20 (for the case of $m = 1$) can be established for even $b \geq 2$. The following theorem shows just two examples for such small m:

Theorem 3.3.23. *For any $a \geq 2$ and even $b \geq 2$,*

$$M^e(2^a 3^b 5, 4) = \frac{1}{6}\big\{5{\cdot}2^{a-2}(3^{b+1} + 1) - 15a + \varepsilon_5\big\},$$

and

$$M^e(2^a 3^b 7, 4) = \frac{1}{6}\big\{7{\cdot}2^{a-2}(3^{b+1} + 1) - 9a + \varepsilon_7\big\},$$

hold, where

$$\varepsilon_5 = \begin{cases} 22 & \text{if } a = 2, \\ 41 & \text{if } a \geq 3 \text{ is odd}, \\ 46 & \text{if } a \geq 4 \text{ is even}, \end{cases} \quad \text{and} \quad \varepsilon_7 = \begin{cases} 19 & \text{if } a \text{ is odd}, \\ 14 & \text{if } a \text{ is even}. \end{cases}$$

Proof: Since $t_2 = \mathrm{sord}_{2^2 5}(3) = 4$, $u = v_2(t_2)+2 = 4$ and $\beta_4^+ = \max\{0, \lceil \frac{a-4}{2} \rceil\}$. Note that $-1 \in (3)_5$, $\varphi(5) = 4$, $M_\varphi^e(5,4) = 0$ and $M_\varphi^e(10,4) = 1$. From Corollary 3.3.21, we have

$$M_\varphi^e(2^a 5, 4) = \begin{cases} \frac{1}{3}(2^{a+1} - 1) - 4\beta_4^+ & \text{if } a \text{ is odd}, \\ \frac{1}{3}(2^{a+1} - 5) - 4\beta_4^+ & \text{if } a \text{ is even}. \end{cases}$$

It follows from (3.3.2) that $M^e(2^a 5, 4) = M^e(2^a, 4) + M_\varphi^e(2^a 5, 4)$. Thus the formula for $M^e(2^a 3^b 5, 4)$ can be proved by applying Corollary 3.3.20 and Theorem 3.3.11.

By noting $t_2 = \mathrm{sord}_{2^2 7}(3) = 3$, $u = v_2(t_2) + 2 = 2$, $\varphi(7) = 6$ and $M_\varphi^e(7,4) = M_\varphi^e(14,4) = 1$, we can prove the formula for $M^e(2^a 3^b 7, 4)$ similarly to that for $M^e(2^a 3^b 5, 4)$ above. □

3.3.6 The recurrence formula of $M_\varphi^e(2^a 3m)$ with respect to a

Firstly, we consider the case of $a \geq 4$. Suppose that $0 \leq i \leq a-2$ and $m \geq 1$ with $(i,m) \neq (a-2,1)$. We examine the vertices on all the paths leading to a vertex $x_{\bullet\bullet} \in U_{i+1,1}$ in common. Then each vertex $x_{\bullet\bullet} \in U_{i+1,1}$ has an adjacency relation as Figure 3.3.9 shows, that is, $\sigma_3^{-1}(x_{\bullet\bullet}) = \{x_{0\bullet}, x_{1\bullet}\} \subseteq U_{i+1,0}$, $\sigma_2^{-1}(x_{\bullet\bullet}) = \{x_{\bullet 0}, x_{\bullet 1}\} \subseteq U_{i1}$, $\sigma_2^{-1}(x_{i\bullet}) = \{x_{i0}, x_{i1}\} \subseteq U_{i0}$, $\sigma_3^{-1}(x_{\bullet j}) = \{x_{0j}, x_{1j}\} \subseteq U_{i0}$, where $i, j \in \{0,1\}$.

Note that, for the case $(i,m) = (a-2,1)$, $U_{i+1,1} = \{2^{a-1}3\}$, $U_{i1} = \{2^{a-2}3\}$ and $U_{i+1,0} = \{2^{a-1}\}$. This means that on the paths with $x_{\bullet\bullet}(= 2^{a-1}3) \in U_{i+1,1}$ as one of the end vertices, we have $x_{\bullet 0}(= x_{\bullet 1} = 2^{a-2}3) \in U_{i1}$ and $x_{0\bullet}(= x_{1\bullet} = 2^{a-1}) \in U_{i+1,0}$, and two vertices $x_{00}(= x_{11})$, $x_{10}(= x_{01}) \in U_{i0}$ satisfying $\sigma_2(x_{rj}) = x_{r\bullet}$ and $\sigma_3(x_{rj}) = x_{\bullet j}$, where $r, j \in \{0,1\}$.

Lemma 3.3.24. *Let $a \geq 2$ and $m \geq 1$ with $\gcd(m,6) = 1$. Any code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a 3m})$ satisfies*

$$c_{i0} + c_{i1} + c_{i+1,0} \leq 2^{a-2-i}\varphi(m)$$

for all $0 \leq i \leq a-2$, where $c_{ij} = |\mathcal{C} \cap U_{ij}|$.

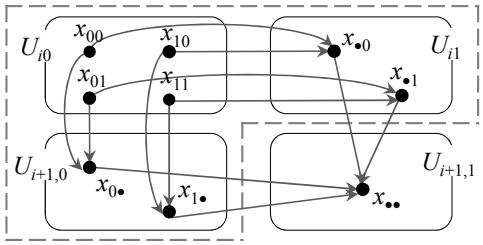

Figure 3.3.9: All paths from U_{i0} to a vertex $x_{\bullet\bullet} \in U_{i+1,1}$ when $a \geq 2$ and $b = 1$

Proof: Let $(a, m) \neq (2, 1)$ and consider the connectivity between the vertices in $U_{i0}, U_{i+1,0}, U_{i1}$ and $U_{i+1,1}$ by tracking back the incoming edges of the vertices in $U_{i+1,1}$ until reaching vertices in U_{i0}. As an implication of Fig. 3.3.9, for each vertex $x_{\bullet\bullet} \in U_{i+1,1}$, the following five inequalities should hold.

$$\begin{aligned} \delta_{\bullet\bullet} + \delta_{0\bullet} + \delta_{1\bullet} + \delta_{\bullet 0} + \delta_{\bullet 1} &\leq 1, \\ \delta_{0\bullet} + \delta_{00} + \delta_{01} &\leq 1, \\ \delta_{1\bullet} + \delta_{10} + \delta_{11} &\leq 1, \\ \delta_{\bullet 0} + \delta_{00} + \delta_{10} &\leq 1, \\ \delta_{\bullet 1} + \delta_{01} + \delta_{11} &\leq 1, \end{aligned}$$

where $\delta_{rj} = \delta(x_{rj}) = 1$ or 0 depending on whether $x_{rj} \in \mathcal{C}$ or not.

By summing these inequalities and considering the integrality of δ, we have

$$\sum_{\substack{r,j \in \{0,1,\bullet\} \\ (r,j) \neq (\bullet,\bullet)}} \delta_{rj} \leq 2,$$

regardless of whether $\delta_{\bullet\bullet} = 0$ or 1. Therefore, for $0 \leq i \leq a-2$ and $m \geq 1$ with $(a, m) \neq (2, 1)$,

$$\begin{aligned} c_{i0} + c_{i+1,0} + c_{i1} &= \sum_{x_{\bullet\bullet} \in U_{i+1,1}} \left(\sum_{\substack{r,j \in \{0,1,\bullet\} \\ (r,j) \neq (\bullet,\bullet)}} \delta_{rj} \right) \\ &\leq 2|U_{i+1,1}| = 2^{a-2-i}\varphi(m) \end{aligned} \tag{3.3.20}$$

holds.

When $(a, m) = (2, 1)$, that is, $n = 2^2 3 = 12$, $U_{00} = \{1, 5\}, U_{01} = \{3\}, U_{10} = \{2\}, U_{11} = \{6\}, U_{20} = \{4\}, U_{21} = \emptyset$. Then it turns out that

$$c_{00} + c_{10} + c_{01} = \delta(1) + \delta(2) + \delta(3) + \delta(5) \leq 1 = \frac{|U_{00}|}{2} = 2^{a-2},$$

which is consistent with (3.3.20). □

Lemma 3.3.25. *For $a \geq 2$ and $m \geq 1$ with $\gcd(m, 6) = 1$, there exists an optimal code in $\mathrm{CAC}^e(V_{2^a 3m})$ satisfying*

$$c_{00} = \frac{|U_{00}|}{2} = 2^{a-2}\varphi(m) \quad \textit{and} \quad c_{01} = c_{10} = 0.$$

Proof: It follows from Lemma 3.3.24 with $i = 0$ that

$$c_{00} + c_{01} + c_{10} \leq 2^{a-2}\varphi(m). \tag{3.3.21}$$

Let $(a, m) \neq (2, 1)$. For each $x_{\bullet\bullet} \in U_{11}$, by choosing two corresponding vertices $x_{ij}, x_{i'j'} \in U_{00}$ such that $i \oplus i' = 1$ and $j \oplus j' = 1$, where $\oplus$ is a bitwise exclusive-or operation, we have a code in $\mathrm{CAC}^e(V_{2^a 3m})$ with

$$c^{**}_{00} = \frac{|U_{00}|}{2} = 2^{a-2}\varphi(m) \quad \text{and} \quad c^{**}_{01} = c^{**}_{10} = 0,$$

which achieves the equality of (3.3.21) and never affects the choice of vertices from $U_{11}, U_{20}, U_{21}, \ldots, U_{a0}, U_{a1}$. This means that, if there exists an optimal code in $\mathrm{CAC}^e(V_{2^a 3m})$ with $\boldsymbol{u}^* = (c^*_{00}, c^*_{01}, c^*_{10}, c^*_{11}, \ldots, c^*_{a0}, c^*_{a1})$, then an optimal code with $\boldsymbol{u}^{**} = (c^{**}_{00}, c^{**}_{01}, c^{**}_{10}, c^*_{11}, \ldots, c^*_{a0}, c^*_{a1})$ also exists.

When $(a, m) = (2, 1)$, that is, $n = 2^2 3 = 12$, by choosing $1 \in U_{00}$, we have $\{\{0, 1, 2, 3\}\}$ as an optimal code in $\mathrm{CAC}^e(12, 4)$ (thus $M^e(12) = M^e_\varphi(12, 4) = 1$). □

Lemma 3.3.26. *Let $a \geq 1$ and $m \geq 1$ with $\gcd(m, 6) = 1$. Any code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a 3m})$ satisfies*

$$c_{i1} + c_{i+1,0} + c_{i+1,1} \leq |U_{i+1,1}| \tag{3.3.22}$$

for all $0 \leq i \leq a - 1$.

Proof: The proof is divided into two cases: (i) $0 \leq i \leq a - 2$, and (ii) $i = a - 1$.

(i) In the case when $(i, m) = (a - 2, 1)$, each of $U_{a-2,1}$, $U_{a-1,1}$, $U_{a-1,0}$ and U_{a0} consists of a single vertex. Clearly

$$|\mathcal{C} \cap (U_{a-2,1} \cup U_{a-1,1} \cup U_{a-1,0})| \leq |\mathcal{C} \cap (U_{a-2,1} \cup U_{a-1,1} \cup U_{a-1,0} \cup U_{a0})| \leq 1.$$

By choosing the vertex from $U_{a-1,0}$, we have

$$c_{a-2,1} + c_{a-1,1} + c_{a-1,0} \leq |U_{a-1,0}| = |U_{a-1,1}| = 1.$$

In the case when $0 \leq i \leq a-2$ and $(i,m) \neq (a-2,1)$, let $T_{i+1,1}$ be a σ_3-orbit in $U_{i+1,1}$. Then $|T_{i+1,1}| = t_{a-i-1}$. In a similar argument to Section 3.3.4 (focusing on the subcodes in σ_3-orbits), we have the corresponding σ_3-orbit(s) in $\sigma_2^{-1}(T_{i+1,1})$, that is, $\sigma_2^{-1}(T_{i+1,1}) = T_{i1} \cup \bar{T}_{i1}$, where $\bar{T}_{i1} = \emptyset$ if $t_{a-i} = 2t_{a-i-1}$. Let $S_t = \mathcal{C} \cap (T_{i+1,1} \cup \sigma_2^{-1}(T_{i+1,1}) \cup \sigma_3^{-1}(T_{i+1,1}))$ and $S = \mathcal{C} \cap (T_{i+1,1} \cup \sigma_2^{-1}(T_{i+1,1}))$. Obviously $|S| \leq |S_t| \leq |T_{i+1,1}|$. Then, from Lemma 3.3.16, we know that

$$\begin{aligned} &\max\{|S_t|\} = t_{a-i-1} && \text{for (A3) and (D3),} \\ &t_{a-i-1} - 1 \leq \max\{|S_t|\} \leq t_{a-i-1} && \text{for (B3) and (C3),} \end{aligned}$$

where (A3)–(D3) are the cases in Table 3.3.1 with $j = a-i$. Here, recall that for cases (B3) and (C3), there is exactly one vertex y in $T_{i+1,1}$, to which any of $t_{a-i-1}-1$ vertices in $\sigma_2^{-1}(T_{i+1,1})$ are not adjacent. So $\sigma_3^{-1}(y) \subseteq \sigma_3^{-1}(T_{i+1,1})$ and one of the two vertices in $\sigma_3^{-1}(y)$ can belong to S_t, and thus we can obtain $|S_t| = t_{a-i-1}$. Therefore, $\max\{|S_t|\} = t_{a-i-1}$ holds if S_t consists of t_{a-i-1} vertices in $\sigma_2^{-1}(T_{i+1,1})$ for cases (A3) and (D3), or $t_{a-i-1}-1$ vertices in $\sigma_2^{-1}(T_{i+1,1})$ and a uniquely determined vertex in $\sigma_3^{-1}(T_{i+1,1})$ for cases (B3) and (C3). By noting that $U_{i+1,1}$ is partitioned into σ_3-orbits of length t_{a-i-1}, we have

$$\max\{c_{i+1,1} + c_{i+1,0} + c_{i1}\} = \max\{|S_t|\}\frac{|U_{i+1,1}|}{t_{a-i-1}} = |U_{i+1,1}|.$$

That is, an optimal subcode $\mathcal{C} \cap (U_{i+1,0} \cup U_{i+1,1} \cup U_{i1})$ of size $|U_{i+1,1}|$ can be obtained by taking a maximum independent vertex set of a wheel/biwheel on $T_{i1} \cup \bar{T}_{i1}$ and for cases (B3) and (C3), a uniquely determined vertex in $\sigma_3^{-1}(T_{i+1,1})$ additionally with respect to each σ_3-orbit $T_{i+1,1}$, where $\bar{T}_{i1} = \emptyset$ if $t_{a-i} = 2t_{a-i-1}$. Thus, in total, we have $c_{i+1,1} = c_{i+1,0} = 0$ and $c_{i1} = |U_{i+1,1}|$ for cases (A3) and (D3), or $c_{i+1,1} = 0$, $c_{i+1,0} = \frac{|U_{i+1,1}|}{t_{a-i-1}}$ and $c_{i1} = \frac{|U_{i+1,1}|}{t_{a-i-1}}(t_{a-i-1}-1)$ for cases (B3) and (C3).

(ii) In the case when $(i,m) = (a-1,1)$, it is clear that $c_{a-1,1} + c_{a0} + c_{a1} = 0$ since $U_{a1} = \emptyset$, $U_{a-1,1} = \{\frac{n}{2}\}$ and $U_{a0} = \{\frac{n}{3}\}$, where $n = 2^a 3m$.

As for the case when $i = a-1$ and $m \geq 5$, let D_{a1} be a σ_2-orbit of length d_0 in U_{a1}, where $d_i = \mathrm{sord}_{3^i m}(2)$. Then $|D_{a1}| = d_0$. As seen in Section 3.3.4 (focusing on the subcodes in σ_2-orbits), D_{a1} has the corresponding σ_2-orbit(s) D_{a0} (and $\bar{D}_{a0}$) in U_{a0}, that is, $\sigma_3^{-1}(D_{a1}) = D_{a0} \cup \bar{D}_{a0}$, where $\bar{D}_{a0} = \emptyset$ if $d_1 = 2d_0$. Let $S_d = \mathcal{C} \cap (D_{a1} \cup \sigma_3^{-1}(D_{a1}) \cup \sigma_2^{-1}(D_{a1}))$ and $S = \mathcal{C} \cap (D_{a1} \cup \sigma_3^{-1}(D_{a1}))$. Since $|S| \leq |S_d| \leq |D_{a1}|$, it follows from Lemma 3.3.17 that

$$\begin{aligned} &\max\{|S_d|\} = d_0 && \text{for (A2) and (D2),} \\ &d_0 - 1 \leq \max\{|S_d|\} \leq d_0 && \text{for (B2) and (C2),} \end{aligned}$$

where (A2)–(D2) are the cases in Table 3.3.2. By a further examination of cases (B2) and (C2), similar to that of cases (B3) and (C3) in the case (i), we have $\max\{|S_d|\} = d_0$ for any of the cases (A2)–(D2), which leads to the completion of the proof. □

We already know, from Lemma 3.3.25, that there exists an optimal code in $\mathrm{CAC}^e(V_{2^a3m})$ satisfying

$$c_{00} = \frac{|U_{00}|}{2} = 2^{a-2}\varphi(m) \quad \text{and} \quad c_{01} = c_{10} = 0.$$

As for c_{11}, c_{20} and c_{21}, we can state the following:

Lemma 3.3.27. *Let $a \geq 3$ and $m \geq 1$ with $\gcd(m, 6) = 1$. If condition (A3) or (D3) in Table 3.3.1 with $j = a-1$ is satisfied, then there exists an optimal code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a3m})$ satisfying*

$$c_{11} = |U_{21}| \quad \textit{and} \quad c_{20} = c_{21} = 0.$$

Proof: It follows from the proof of (i) of Lemma 3.3.26 that, for cases (A3) and (D3), $\mathcal{C} \cap (U_{11} \cup U_{20} \cup U_{21})$ is an optimal subcode with $c_{11} = |U_{21}|$ and $c_{20} = c_{21} = 0$, which never affects the choice of codewords from $\bigcup_{i=3}^{a} \bigcup_{j=0}^{1} U_{ij}$. Then, together with Lemma 3.3.25, the assertion can be proved. □

We have a similar lemma for case (B3) in Table 3.3.1 with $j = a - 1$.

Lemma 3.3.28. *Let $a \geq 5$, $m \geq 1$ with $\gcd(m, 6) = 1$. If condition (B3) in Table 3.3.1 with $j = a - 1$ is satisfied, then there exists an optimal code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a3m})$ satisfying*

$$c_{11} = \frac{|U_{21}|}{t_{a-2}}(t_{a-2} - 1), \quad c_{20} = \frac{|U_{21}|}{t_{a-2}} \quad \textit{, and} \quad c_{21} = 0,$$

such that, for $V' = \bigcup_{i=3}^{a} \bigcup_{j=0}^{1} U_{ij}$, $\mathcal{C} \cap V'$ is also an optimal code in $\mathrm{CAC}^e(V')$.

Proof: (i) For the case when $(a, m) \neq (5, 1)$, recall that each vertex $x_{\bullet\bullet\bullet} \in U_{41}$ has an adjacency relation as Figure 3.3.10 shows, that is,

$$\begin{aligned}
&\sigma_3^{-1}(x_{\bullet\bullet\bullet}) = \{x_{0\bullet\bullet}, x_{1\bullet\bullet}\} \subseteq U_{40},\ \sigma_2^{-1}(x_{\bullet\bullet\bullet}) = \{x_{\bullet0\bullet}, x_{\bullet1\bullet}\} \subseteq U_{31},\\
&\sigma_2^{-1}(x_{i\bullet\bullet}) = \{x_{i0\bullet}, x_{i1\bullet}\} \subseteq U_{30},\ \sigma_3^{-1}(x_{\bullet j\bullet}) = \{x_{0j\bullet}, x_{1j\bullet}\} \subseteq U_{30},\\
&\sigma_2^{-1}(x_{\bullet j\bullet}) = \{x_{\bullet j0}, x_{\bullet j0}\} \subseteq U_{21},
\end{aligned} \tag{3.3.23}$$

where $i, j \in \{0, 1\}$, and so on. Hence the vertices in U_{20} are partitioned into $|U_{41}|$ subsets of size 8 which lead to distinct vertices in U_{41}, respectively, by a mapping $\sigma_3\sigma_2^2$.

For a σ_3-orbit T_{41} in U_{41}, let $T_{21}^{(i)}$, $1 \le i \le \ell$, be the σ_3-orbits satisfying $\sigma_2^2(T_{21}^{(i)}) = T_{41}$ (conversely $\sigma_2^{-2}(T_{41}) = \dot{\bigcup}_{i=1}^{\ell} T_{21}^{(i)}$). For each $T_{21}^{(i)}$, if $\mathcal{C} \cap (T_{21}^{(i)} \cup \sigma_2^{-1}(T_{21}^{(i)}) \cup \sigma_3^{-1}(T_{21}^{(i)}))$ is an optimal subcode just as S_t of maximum size t_{a-2} in the proof of (i) in Lemma 3.3.26, where $\mathcal{C}$ is a code in $\mathrm{CAC}^e(V_{2^a3m})$, then each $T_{21}^{(i)}$ has a uniquely determined vertex, say $y^{(i)}$, for which there is a vertex $y_0^{(i)} \in \mathcal{C} \cap \sigma_3^{-1}(T_{21}^{(i)}) \subseteq U_{20}$ satisfying $\sigma_3(y_0^{(i)}) = y^{(i)}$ (thus $y^{(i)} \notin \mathcal{C}$). Note that $\ell = \frac{4t_{a-4}}{t_{a-2}}$ since $|U_{21}| = 4|U_{41}|$, $|T_{i1}| = t_{a-i}$, and U_{21} and U_{41} are partitioned into $\frac{|U_{21}|}{t_{a-2}}$ and $\frac{|U_{41}|}{t_{a-4}}$ σ_3-orbits, respectively. So if $|T_{41}| = t_{a-4} \ge \ell$, that is, $t_{a-2} \ge 4$, then for any σ_3-orbit T_{41} in U_{41}, we can always take a set of ℓ distinct codewords

$$Y_0 = \{y_0^{(i)} \in \sigma_3^{-1}(T_{21}^{(i)}) : \sigma_3\sigma_2^2(y_0^{(i)}) \ne \sigma_3\sigma_2^2(y_0^{(i')}) \in T_{41}, 1 \le i \ne i' \le \ell\} \subset \mathcal{C} \cap U_{20},$$

that is, $Y_0 = \mathcal{C} \cap \left(\bigcup_{i=1}^{\ell} \sigma_3^{-1}(T_{21}^{(i)})\right) = \mathcal{C} \cap \sigma_3^{-1}\sigma_2^{-2}(T_{41})$. In fact, it is easily verified by Lemma 3.1.12 that $t_{a-2} \ge 4$ holds for any $a \ge 5$ and $m \ge 1$ except when $(a, m) = (5, 1)$, and thus there exists a code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a3m})$ such that, for any σ_3-orbit T_{41} in U_{41}, $\mathcal{C} \cap (T_{21}^{(i)} \cup \sigma_2^{-1}(T_{21}^{(i)}) \cup \sigma_3^{-1}(T_{21}^{(i)}))$, $1 \le i \le \ell$, are optimal subcodes such that $|\mathcal{C} \cap \sigma_2^{-1}(T_{21}^{(i)})| = t_{a-2} - 1$, $|\mathcal{C} \cap \sigma_3^{-1}(T_{21}^{(i)})| = 1$ and $|\mathcal{C} \cap T_{21}^{(i)}| = 0$. This means $\mathcal{C} \cap (U_{11} \cup U_{20} \cup U_{21})$ can be an optimal subcode satisfying $c_{11} = \frac{|U_{21}|}{t_{a-2}}(t_{a-2} - 1)$, $c_{20} = \frac{|U_{21}|}{t_{a-2}}$ and $c_{21} = 0$.

In order to complete the proof for $(a, m) \ne (5, 1)$, it remains to show that for any T_{41}, $\sigma_2(Y_0)$ does not change the size of $\mathcal{C} \cap V'$, which implies that $\mathcal{C} \cap V'$ can be supposed to be an optimal code in $\mathrm{CAC}^e(V')$. For a σ_3-orbit T_{41} in U_{41}, consider $Y_0 = \mathcal{C} \cap \sigma_3^{-1}\sigma_2^{-2}(T_{41})$. By letting $\sigma_3\sigma_2^2(y_0) = x_{\bullet\bullet\bullet}$ for an arbitrary $y_0 \in Y_0$, its related vertices $x_{ij\bullet}, x_{i\bullet\bullet}$ and $x_{\bullet j\bullet}$, where $i, j \in \{0, 1\}$, are determined as in (3.3.23) by mappings $\sigma_3^{-1}\sigma_2^{-1}$, σ_2^{-1} and σ_3^{-1}, respectively. By noting that $(\mathcal{C} \cap V') \cap \{x_{00\bullet}, x_{11\bullet}\} = \emptyset$ or $(\mathcal{C} \cap V') \cap \{x_{01\bullet}, x_{10\bullet}\} = \emptyset$ holds for any code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a3m})$, we can always assume $\sigma_2(y_0) \notin \mathcal{C} \cap V'$ for any $y_0 \in Y_0$, since the roles of the pairs $\{x_{00\bullet}, x_{11\bullet}\}$ and $\{x_{01\bullet}, x_{10\bullet}\}$ can be swapped if $\sigma_2(y_0) \in \mathcal{C} \cap V'$ originally. This completes the proof for the case when $(a, m) \ne (5, 1)$.

(ii) For the case when $(a, m) = (5, 1)$ (see Figure 3.3.11),

$$\mathcal{C} = \{1, 5, 7, 11, 13, 17, 23, 29, 6, 20, 8\}$$

is an instance of an optimal code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a3m})$ with $c_{00} = 2^3$, $c_{11} = \frac{|U_{21}|}{2}(2 - 1) = 1$, $c_{20} = \frac{|U_{21}|}{2} = 1$ and $c_{01} = c_{10} = c_{21} = 0$. In this case,

$\mathcal{C} \cap U_{00} = \{1, 5, 7, 11, 13, 17, 23, 29\}$, $\mathcal{C} \cap U_{11} = \{6\}$, $\mathcal{C} \cap U_{20} = \{20\}$, $\mathcal{C} \cap U_{30} = \{8\}$. □

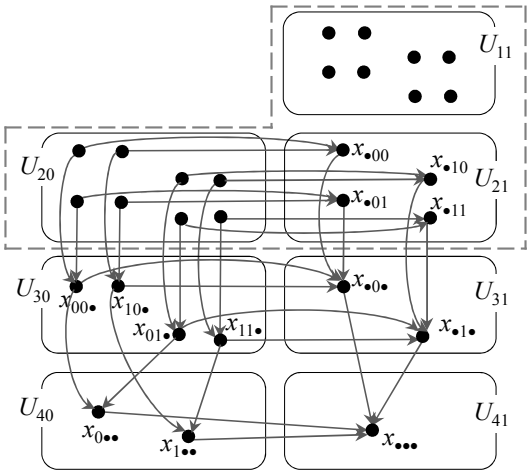

Figure 3.3.10: All paths from U_{20} to a vertex $x_{\bullet\bullet\bullet} \in U_{41}$ when $a \geq 5$, $m \geq 1$ and $(a, m) \neq (5, 1)$

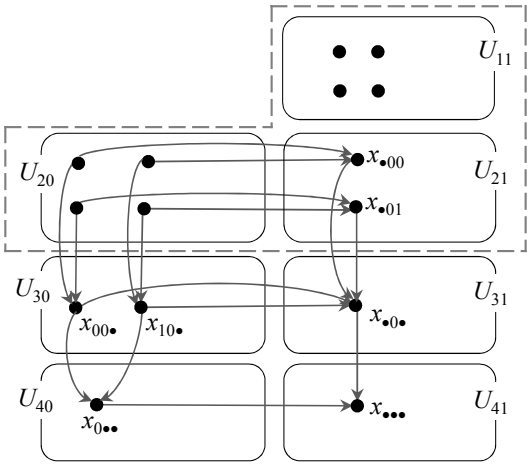

Figure 3.3.11: All paths from U_{20} to a vertex $x_{\bullet\bullet\bullet} \in U_{41}$ when $(a, m) = (5, 1)$

Theorem 3.3.29. *For $a \geq 4$ and $m \geq 1$ with $\gcd(m, 6) = 1$,*

$$M_\varphi^e(2^a 3m, 4) = 2^{a-4} 5\varphi(m) + M_\varphi^e(2^{a-3} 3m, 4).$$

Proof: Let $\mathcal{C}'$ be an optimal code in $\mathrm{CAC}^e(V_{2^{a-3}3m})$, and let $V' = \bigcup_{i=3}^{a} \bigcup_{j=0}^{1} U_{ij}$. Since $V' = 2^3 V_{2^{a-3}3m}$, the code $2^3\mathcal{C}'$, which is obtained by multiplying all the

codewords in $\mathcal{C}'$ by 2^3, is regarded as an optimal code in $\mathrm{CAC}^e(V')$. Thus, it is sufficient to prove the existence of an optimal code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a3m})$ such that $|\mathcal{C} \cap (V_{2^a3m} \setminus V')| = 2^{a-4}5\varphi(m)$ and $\mathcal{C} \cap V' = 2^3\mathcal{C}'$.

For cases (A3) and (D3) in Table 3.3.1 with $j = a-1$, Lemmas 3.3.25 and 3.3.27 assure the existence of an optimal code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^a3m})$ such that $c_{00} = 2^{a-2}\varphi(m)$, $c_{11} = 2^{a-4}\varphi(m)$, $c_{01} = c_{10} = c_{20} = c_{21} = 0$ and $\mathcal{C} \cap V' = 2^3\mathcal{C}'$.

It can be easily demonstrated that (t_{a-1}, t_{a-2}) will never be case (C3) in Table 3.3.1 with $j = a-1$. From Lemma 3.1.24, $(t_{a-1}, t_{a-2}) = (2^{a-3}, 2^{a-4})$ holds when $m = 1$, which is case (B3) if $a = 4$, or (D3) if $a \geq 5$. If $m \geq 5$ and $a \geq 3$, Table 3.3.3 shows that (t_{a-1}, t_{a-2}) is one of the cases (A3), (B3) and (D3) by Table 3.3.3.

For case (B3) in Table 3.3.1 with $j = a-1$, we only need to consider the case $a \geq 5$, since (t_3, t_2) will never be case (B3) (see Table 3.3.3). Then, Lemmas 3.3.25 and 3.3.28 assure the existence of an optimal code in $\mathrm{CAC}^e(V_{2^a3m})$ such that $c_{00} = 2^{a-2}\varphi(m)$, $c_{11} = \frac{|U_{21}|}{t_{a-2}}(t_{a-2}-1)$, $c_{20} = \frac{|U_{21}|}{t_{a-2}}$, $c_{01} = c_{10} = c_{21} = 0$ and $\mathcal{C} \cap V' = 2^3\mathcal{C}'$. □

Corollary 3.3.30. *For $a \geq 4$ and $m \geq 1$ with $\gcd(m, 6) = 1$,*

$$M_\varphi^e(2^a3m, 4) = \begin{cases} \frac{5}{7}(2^{a-1}-1)\varphi(m) + M_\varphi^e(6m, 4) & \text{if } a \equiv 1 \pmod 3, \\ \frac{10}{7}(2^{a-2}-1)\varphi(m) + M_\varphi^e(12m, 4) & \text{if } a \equiv 2 \pmod 3, \\ \frac{20}{7}(2^{a-3}-1)\varphi(m) + M_\varphi^e(24m, 4) & \text{if } a \equiv 0 \pmod 3. \end{cases}$$

Next, we discuss $M_\varphi^e(2^a3m, 4)$ for $a = 0, 2$ and 3. For the case $a = 1$, we do not have enough constraints to determine the size of the optimal subcodes of $\mathcal{C} \cap (U_{0j} \cup U_{1j})$, since $\sigma_2(U_{0j}) = U_{1j}$ is a bijection for $j \in \{0, 1\}$. Hence, we do not discuss the case $M_\varphi^e(6m, 4)$ here.

Theorem 3.3.31. *For $m \geq 5$ with $\gcd(m, 6) = 1$, let $d_i = \mathrm{sord}_{3^im}(2)$. Then*

$$M_\varphi^e(3m, 4) = \begin{cases} \frac{1}{2}\varphi(m) & \text{if } m \geq 5 \text{ and } d_0 = d_1 \text{ is even,} \\ & \text{or } m \geq 5,\ d_0 \text{ is odd and } d_1 = 2d_0, \\ \frac{1}{2}(1 - \frac{1}{d_0})\varphi(m) & \text{otherwise.} \end{cases}$$

Proof: Let $\rho_{01} = |\mathcal{C} \cap D_{01}|$ and $\rho_{00} = |\mathcal{C} \cap \sigma_3^{-1}(D_{01})| = |\mathcal{C} \cap (D_{00} \cup \bar{D}_{00})|$, where $\bar{D}_{00} = \emptyset$ if $d_1 = 2d_0$. Then, the size of a code $\mathcal{C} \in \mathrm{CAC}^e(V_n)$ is given by

$$|\mathcal{C}| = c_{00} + c_{01} = \frac{|U_{00}|}{2d_0}\rho_{00} + \frac{|U_{01}|}{d_0}\rho_{01} = \frac{\varphi(m)}{2d_0}(\rho_{00} + \rho_{01}).$$

This means that the maximum value of $|\mathcal{C}|$ can be obtained by maximizing $\rho_{00} + \rho_{01}$. From Lemmas 3.3.5 and 3.3.6, we have

$$\mathcal{C}_{01} \,\dot\cup\, \sigma_2(\mathcal{C}_{01}) \,\dot\cup\, \sigma_3(\mathcal{C}_{00}) \,\dot\cup\, \sigma_3(\mathcal{C}_{01}) \subset U_{01},$$

which implies that $c_{00} + 3c_{01} \le |U_{01}|$. Thus

$$\rho_{00} + 3\rho_{01} \le d_0. \tag{3.3.24}$$

By applying Lemma 3.3.17 with $S = \mathcal{C} \cap (\sigma_3^{-1}(D_{01}) \cup D_{01})$, the optimal solution for maximizing $\rho_{00} + \rho_{01}$ subject to (3.3.24) is $\rho_{01} = 0$, and $\rho_{00} = d_0$ for cases (A2) and (D2), or $\rho_{00} = d_0 - 1$ for cases (B2) and (C2), where (A2)–(D2) are the cases in Table 3.3.2. Thus there exists an optimal code in $\mathrm{CAC}^e(V_{3m})$ satisfying $c_{01} = 0$ and

$$c_{00} = \begin{cases} |U_{01}| & \text{for (A2) and (D2),} \\ \dfrac{|U_{01}|}{d_0}(d_0 - 1) & \text{for (B2) and (C2).} \end{cases}$$

The assertion is proved. □

Theorem 3.3.32. *Let $m \ge 1$ with $\gcd(m, 6) = 1$. Then*

$$M_\varphi^e(12m, 4) = \begin{cases} 1 & \text{if } m = 1, \\ \frac{3}{2}\varphi(m) & \text{if } m \ge 5. \end{cases}$$

Proof: It is easy to see that $M^e(12) = 1$. For $m \ge 5$, from Lemma 3.3.25, there exists an optimal code in $\mathrm{CAC}^e(V_{2^a 3m})$ satisfying $c_{00} = 2^{a-2}\varphi(m)$ and $c_{01} = c_{10} = 0$. By Lemma 3.3.26 with $j = a - 1 = 1$, we have an optimal subcode satisfying $c_{11} + c_{20} + c_{21} = |U_{21}| = \frac{\varphi(m)}{2}$ if $m \ge 5$. This completes the proof. □

Recall that $t_i = \mathrm{sord}_{2^i m}(3)$ and $d_i = \mathrm{sord}_{3^i m}(2)$. To discuss $M_\varphi^e(24m, 4)$, we need to consider the relation between (t_1, t_2) and (d_0, d_1) as shown in Table 3.3.4.

Table 3.3.4: Four cases for the relation between (t_1, t_2) and (d_0, d_1)

		(t_1, t_2)	
		(A3) or (D3)	(B3) or (C3)
(d_0, d_1)	(A2) or (D2)	(A6)	(B6)
	(B2) or (C2)	(C6)	(D6)

Note that (A2)–(D2) are the cases in Table 3.3.2 and (A3)–(D3) are the cases in Table 3.3.1 with $j = 2$.

Theorem 3.3.33. *For $m \geq 1$ with $\gcd(m, 6) = 1$,*

$$M^e_\varphi(24m, 4) = \begin{cases} 3\varphi(m) & \text{if } m = 1, \text{ or } m \geq 5 \text{ and (A6) is satisfied,} \\ (3 - \frac{1}{2d_0})\varphi(m) & \text{if } m \geq 5 \text{ and (C6) is satisfied,} \end{cases}$$

where (A6) and (C6) are the cases in Table 3.3.4.

Proof: When $m = 1$, that is, $n = 24$, it is easy to verify that $M^e_\varphi(24, 4) = 3$ with $c_{00} = 2$ and $c_{20} = 1$. In the case when $m \geq 5$, and (A6) or (C6) is satisfied, by Lemmas 8.2 and 8.4, there exists an optimal code $\mathcal{C} \in \mathrm{CAC}^e(V_{2^3 3m})$ satisfying $c_{00} = 2\varphi(m)$, $c_{11} = \varphi(m)/2$ and $c_{01} = c_{10} = c_{20} = c_{21} = 0$. Then we have $M^e_\varphi(24m, 4) = \frac{5}{2}\varphi(m) + M^e_\varphi(3m, 4)$. Theorem 3.3.31 then completes the proof. □

For cases (B6) and (D6) in Table 3.3.4, determining $M^e_\varphi(24m, 4)$ for general $m \geq 1$ with $\gcd(m, 6) = 1$ is an open problem because, in many instances, it depends on the relation between σ_2-orbits in U_{30} and σ_3-orbits in U_{21}, which we have not elucidated so far. For a similar reason, $M^e_\varphi(6m, 4)$ is also unsolved in this thesis. However, if m is small, we can find $M^e_\varphi(24m, 4)$ and $M^e_\varphi(6m, 4)$ by directly examining $G(V_{24m})$ and $G(V_{6m})$, respectively, which can provide substance to Corollary 3.3.30. The following theorem shows two companion examples to Theorem 3.3.23 for $m = 5$ and 7:

Theorem 3.3.34. *For $a \geq 2$ and odd $b \geq 3$,*

$$M^e(2^a 3^b 5) = \frac{1}{7}\{5 \cdot 2^{a-3}(3^b 7 - 1) - \xi_5\},$$

and

$$M^e(2^a 3^b 7) = 2^{a-3}(3^b 7 - 1) - \xi_7,$$

hold, where

$$\xi_5 = \begin{cases} 4 & \text{if } a \equiv 1 \pmod 3, \\ 1 & \text{if } a \equiv 2 \pmod 3, \\ 2 & \text{if } a \equiv 0 \pmod 3, \end{cases} \quad \text{and} \quad \xi_7 = \begin{cases} 1 & \text{if } a \equiv 1 \pmod 3, \\ 0 & \text{otherwise.} \end{cases}$$

Proof: It is easy to see that $M^e_\varphi(6, 4) = 0$, $M^e_\varphi(6 \cdot 5, 4) = 3$ and $M^e_\varphi(6 \cdot 7, 4) = 4$. From Theorem 3.3.32, we have $M^e_\varphi(12, 4) = 1$, $M^e_\varphi(12 \cdot 5, 4) = 6$ and

$M^e_\varphi(12{\cdot}7, 4) = 9$. By Theorem 3.3.33, we have $M^e_\varphi(24, 4) = 3$. Since the cases of $m = 5$ and 7 correspond to (D6) and (B6) in Table 3.3.4, respectively, Theorem 3.3.33 cannot be applied to find $M^e_\varphi(24m, 4)$. Thus, by directly examining $G(V_{24\cdot 5})$ and $G(V_{24\cdot 7})$, we find $M^e_\varphi(24{\cdot}5, 4) = 11$ and $M^e_\varphi(24{\cdot}7, 4) = 17$. Then, by applying Corollary 3.3.30, Theorem 3.3.11 and (3.3.2), we can obtain $M^e(2^a3^b5, 4)$ and $M^e(2^a3^b7, 4)$. □

Since the exact value of $M^e_\varphi(12m, 4)$ is computable by Theorem 3.3.32, we can state the following:

Theorem 3.3.35. *For $a \geq 4$ with $a \equiv 2 \pmod 3$, odd $b \geq 3$ and $m \geq 1$ with $\gcd(m, 6) = 1$,*

$$M^e(n = 2^a3^bm, 4) = \frac{1}{14}\big\{2^{a-2}(3^b7 - 1)m + m - 7\big\}.$$

Proof: By applying Theorem 3.3.32, the second case of Corollary 3.3.30 can be completely determined. That is, for any $a \geq 4$ with $a \equiv 2 \pmod 3$,

$$M^e_\varphi(2^a3m, 4) = \begin{cases} \frac{1}{7}(2^{a-1}5 - 3) & \text{if } m = 1, \\ \frac{1}{7}(2^{a-1}5 + 1)\varphi(m) & \text{if } m \geq 5 \end{cases}$$

holds. Then it follows from (3.3.2) that $M^e(2^a3m, 4) = \frac{m}{14}(2^a5 + 1) - \frac{1}{2}$, and the formula for $M^e(n = 2^a3^bm, 4)$ can be proved by applying Theorem 3.3.11. □

3.3.7 Summary for equi-difference conflict-avoiding codes of weight four

By using a graph representation defined in Section 3.3.1, we derived a recurrence formula for $M^e(n = 2^a3^bm, 4)$ with respect to b as in Theorem 3.3.11, which can be rewritten as

$$M^e(2^a3^bm, 4) = \begin{cases} 2^{a-3}(3^b - 1)m + \sum_{d|m} M^e_\varphi(2^ad, 4) & \text{if } b \text{ is even}, \\ 2^{a-3}(3^b - 3)m + \sum_{d|m} M^e_\varphi(2^a3d, 4) & \text{if } b \text{ is odd} \end{cases} \tag{3.3.25}$$

for $a \geq 0$, $b \geq 2$ and $m \geq 1$ with $\gcd(m, 6) = 1$ by using (3.3.2). This means that, in order to find $M^e(n, 4)$, it is sufficient to find $M^e_\varphi(2^am, 4)$ or $M^e_\varphi(2^a3m, 4)$ for general $m \geq 1$ with $\gcd(m, 6) = 1$. In Sections 3.3.5 and 3.3.6, we gave recurrence formulae also for $M^e_\varphi(2^am, 4)$ and $M^e_\varphi(2^a3m, 4)$

with respect to a and investigated conditions for which $M^e_\varphi(2^a m, 4)$ and $M^e_\varphi(2^a 3m, 4)$ are explicitly determined. The results are summarized in Table 3.3.5. As shown in Table 3.3.5, to complete the spectrum of $M^e(n, 4)$ for any $n \in \mathbb{N}$, we still have to find $M^e_\varphi(m, 4)$, $M^e_\varphi(2m, 4)$, $M^e_\varphi(6m, 4)$ and a part of $M^e_\varphi(24m, 4)$ for general $m \geq 5$ with $\gcd(m, 6) = 1$.

Table 3.3.5: Exact values or references of $M^e_\varphi(2^a 3^b m, 4)$

m	b	a				
		0	1	2	3	≥ 4
1	0	0		Cor. 3.3.20 ([49, Theorem 1])		
	1	0	1	[49, Theorem 2]		
≥ 5	0	unknown		Cor. 3.3.21[1]		
	1	Thm. 3.3.31	unknown	Thm. 3.3.32	Thm. 3.3.33[2]	Cor. 3.3.30[3]

1) For $M^e_\varphi(2^a m, 4)$ to be computable, $M^e_\varphi(m, 4)$ and $M^e_\varphi(2m, 4)$ should be known.

2) For cases (A6) and (C6) in Table 3.3.4, $M^e_\varphi(2^a 3m, 4)$ is computable, but not for cases (B6) and (D6).

3) If $a \equiv 2 \pmod 3$, or $a \equiv 0 \pmod 3$ and the relation between (t_1, t_2) and (d_0, d_1) is case (A6) or (C6) in Table 3.3.4, then $M^e_\varphi(2^a 3m, 4)$ is computable. Otherwise $M^e_\varphi(6m, 4)$ or $M^e_\varphi(24m, 4)$ should be known.

As a series of explicitly determined $M^e(n, 4)$, we obtained

$$M^e(n = 2^a 3^b m, 4) = \frac{1}{14}\{2^{a-2}(3^b 7 - 1)m + m - 7\}$$

for $a \geq 4$ with $a \equiv 2 \pmod 3$, odd $b \geq 3$ and $m \geq 1$ with $\gcd(m, 6) = 1$ (see Theorem 3.3.35), since the exact value of $M^e_\varphi(12m, 4)$ has been given by Theorem 3.3.32. In order to get any other series of explicitly computable $M^e(2^a 3^b m, 4)$, we need to solve the unknown cases in Table 3.3.5 first and then accumulate the results that will be obtained. However, if m is small (thus all divisors d of m are small), the values of $M^e_\varphi(2^a 3^b m, 4)$ can be determined by directly examining $G(V_{2^i 3^j m})$ for $i \leq 3$ and $j \leq 1$. Theorems 3.3.23 and 3.3.34 are just two examples of such m, and, in the same way, we can get more series for other small m.

Chapter 4

Conclusion

In this thesis, we focused on t-SEEDs and conflict-avoiding codes as combinatorial designs and codes related to information-communication, discussing their optimalities, existence and constructions.

In Chapter 2, it was clarified that an extremal t-$(v, k; m)$ SEED is a large set of Steiner t-designs. There is no doubt that the upper bound (2.1.1) cannot be achieved when a large set of Steiner t-designs does not exist. Finding a sharper bound for a t-SEED in such a case is an open problem:

Problem 1. Improve the upper bound of (2.1.1) for the number m of designs of a t-SEED when there is no large set of Steiner t-designs.

By utilizing some fundamental combinatorial configurations, several recursive constructions were presented in Section 2.2. Unfortunately, those constructions did not attain the upper bound of (2.1.1). It is a challenging problem to construct t-SEEDs with the maximal number of mutually disjoint designs.

Problem 2. Find a t-SEED whose number of designs attains the improved upper bound.

In Section 2.3, a new application of a t-SEED to a secret sharing scheme was given. The balanced property of a t-SEED has more flexibility than that of many other combinatorial designs; therefore, a t-SEED is expected to have more applications.

In Chapter 3, we treated optimal equi-difference CACs of weights three and four. In Section 3.1, we paid particular attention to examining properties

of the multiplicative order and suborder of a unit in $\mathbb{Z}_n$, and verified the values of $\mathrm{ord}_n(\theta)$ and $\mathrm{sord}_n(\theta)$ for the specific units $\theta = 2, 3$. Based on the results obtained in Section 3.1, we gave, in Section 3.2, some explicit series of optimal equi-difference CACs for which $M^e(n, 3)$ can be exactly determined, except for some of the cases when n contains a prime factor $p \equiv 1 \pmod 8$. We leave the following as an open problem:

Problem 3. For any odd n containing a prime factor $p \equiv 1 \pmod 8$, find $M^e(n, 3)$.

It should be mentioned that, for the case when the "equi-difference" property is not imposed on a code, $M(n, 3)$ for odd n has not been completely determined yet.

In Section 3.3, by defining a directed graph, we examined possible codewords in equi-difference CACs of weight four. Using such a directed graph, we derived several recurrence formulae for $M^e(n = 2^a 3^b m, 4)$, together with constructions, where $a, b \geq 0$ and $m \geq 1$ with $\gcd(m, 6) = 1$. This implies that $M^e(n, 4)$ can be determined in many cases from our results. In order to complete the spectrum of $M^e(n, 4)$ for any $n \in \mathbb{N}$, we still need to solve the following:

Problem 4. Let $m \geq 5$ with $\gcd(m, 6) = 1$. Find the following values: (i) $M^e_\varphi(m, 4)$, (ii) $M^e_\varphi(2m, 4)$, (iii) $M^e_\varphi(6m, 4)$, and (iv) $M^e_\varphi(24m, 4)$ for cases (B6) and (D6) in Table 3.3.4.

Also, for the weight four case, $M(n, 4)$ is not known for general n. When it comes to general weight $w \geq 5$, finding both $M(n, w)$ and $M^e(n, w)$ are open problems.

List of papers related to this thesis

[1] Y. Lin and M. Jimbo, Extremal properties of t-SEEDs and recursive constructions, *Des. Codes Cryptogr.,* **73**, 805-823 (2014).

[2] Y. Lin, M. Mishima, J. Satoh and M. Jimbo, Optimal equi-difference conflict-avoiding codes of odd length and weight three, *Finite Fields Appl.,* **26**, 49–68 (2014).

[3] Y. Lin, M. Mishima and M. Jimbo, Optimal equi-difference conflict-avoiding codes of weight four, *Des. Codes Cryptogr.,* (2014) DOI 10.1007/s10623-014-0030-x.

Bibliography

[1] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl and M. Mussinger, Stabilizing distinguishable qubits against spontaneous decay by detected-jump correcting quantum codes, *Phys. Rev. Lett.* **86**, 4402–4405 (2001).

[2] G. Alber, T. Beth, C. Charnes, A. Delgado, M. Grassl and M. Mussinger, Detected-jump-error-correcting quantum codes, quantum error designs and quantum computation, *Phys. Rev. A* **68**, 012316 (2003).

[3] M. Araya, More mutually disjoint Steiner systems $S(5, 8, 24)$, *J. Combin. Theory Ser. A.* **102**, 201–203 (2003).

[4] Z. Baranyai, On the factorizations of the complete uniform hypergraph, *Finite and infinite sets*, Colloq. Math. Soc. Janos Bolyai 10 North-Holland, Amsterdam 91–108 (1975).

[5] L. A. Bassalygo and M. S. Pinsker, Limited multiple-access of a non-synchronous channel (in Russian), *Probl. Inf. Transm.* **19**(4), 92–96 (1983).

[6] T. Beth, C. Charnes, M. Grassl, G. Alber, A. Delgado and M. Mussinger, A new class of designs which protect against quantum jumps, *Des. Codes Cryptogr.* **29**, 51–70 (2003).

[7] A. Betten, R. Lauea and A. Wassermann, New t-designs and large sets of t-designs. *Discrete Math.* **197/198**, 111–121 (1999).

[8] G. R. Blakley, Safeguarding cryptographic keys, *AFIPS Conference Proc.* **48**, 313–317 (1979).

[9] A. R. Calderbank, E. M. Rains, P. W. Shor and N. J. A. Sloane, Quantum error correction via codes over $GF(4)$, *IEEE Trans. Inform. Theory* **44**, 1369–1387 (1998).

[10] A. R. Calderbank and P. W. Shor, Good quantum error-correcting codes exist, *Phys. Rev. A* **54**, 1098–1105 (1996).

[11] A. Cayley, On the triadic arrangements of seven and fifteen things, *London, Edinburgh and Dublin Philos. Mag. J. Sci.* **37**, 50–53 (1850).

[12] Y. M. Chee and S. S. Magliveras, A few more large sets of t-designs, *J. Combin. Des.* **6**, 293–308 (1998).

[13] D. Chen, C. C. Lindner and D. R. Stinson, Further results on large sets of disjoint group-divisible designs, *Discrete Math.* **110**, 35–42 (1992).

[14] D. Chen and D. R. Stinson, Recent results on combinatorial constructions for threshold schemes, *Australas. J. Combin.* **1**, 29–48 (1990).

[15] L. G. Chouinard, Partitions of the 4-subsets of a 13-set into disjoint projective planes, *Discrete Math.* **45**, 297–300 (1983).

[16] Y. P. Deng, L. F. Guo, and M. L. Liu, Constructions for Anonymous secret sharing schemes using combinatorial designs, *Acta Math. Appl. Sin. Engl. Ser.* **23** (1), 67–78 (2007).

[17] L. E. Dickson, *History of the Theory of Numbers, Volume I: Divisibility and Primality*, Carnegie Institute of Washington, Washington (1919), `http://archive.org/details/historyoftheoryo01dick`.

[18] I. B. Djordjevic, Quantum LDPC codes from balanced incomplete block designs, *IEEE Commun. Lett.* **12**, 389–391 (2008).

[19] F. G. Dorais, A Wieferich Prime Search up to 6.7×10^{15}, Article 11.9.2, J. Integer Seq. **14** (2011), `https://cs.uwaterloo.ca/journals/JIS/VOL14/Klyve/klyve3.pdf`.

[20] A. Ekert and C. Macchiavello, Quantum error correction for communication, *Phys. Rev. Lett.* **77**, 2585–2588 (1996).

[21] M. Emami and O. Naserian, Some new large sets of t-designs, *Discrete Math.* **310**, 1629–1632 (2010).

[22] T. Etzion and A. Hartman, Towards a large set of Steiner quadruple systems, *SIAM J. Discrete Math.* **4**, 182–195 (1991).

[23] J. Fang and Y. Chang, Mutually disjoint t-designs and t-SEEDs from extremal doubly-even self-dual codes, *Des. Codes Cryptogr.* **73**(3), 769–780 (2014).

[24] J. Fang and Y. Chang, Mutually disjoint 5-designs and 5-spontaneous emission error designs from extremal ternary self-dual codes, *J. Combin. Des.* **23**(2), 78–89 (2015).

[25] J. Fang, J. Zhou and Y. Chang, Nonexistence of some quantum jump codes with specified parameters, *Des. Codes Cryptogr.* **73**(1), 223–235 (2014).

[26] R. A. Fisher, *Statistical Methods for Research Wrkers*, Oliver and Boyd, Edinburgh, (1925).

[27] R. A. Fisher, *The Design of Experiments*, Oliver and Boyd, Edinburgh, (1947).

[28] H.-L. Fu, Y.-H. Lin and M. Mishima, Optimal conflict-avoiding codes of even length and weight 3, *IEEE Trans. Inform. Theory* **56**(11), 5747–5756 (2010).

[29] H.-L. Fu, Y.-H. Lo and S. W. Shum, Optimal conflict-avoiding codes of odd length and weight three, *Des. Codes Cryptogr.* **72**(2), 289–309 (2014).

[30] Y. Fujiwara, D. Clark, P. Vandendriessche, M. De Boeck, and V. D.. Tonchev, Entanglement-assisted quantum low-density parity-check codes, *Phys. Rev. A* **82**, 042338 (2010).

[31] Y. Gallot, Cyclotomic polynomials and prime numbers, `http://yves.gallot.pagesperso-orange.fr/papers/cyclotomic.pdf`.

[32] L. Györfi and I. Vajda, Constructions of protocol sequences for multiple access collision channel without feedback, *IEEE Trans. Inform. Theory* **39**(5), 1762–1765 (1993).

[33] R. W. Hamming, Error detecting and error correcting codes, *Bell System Technical Journal* **29**,147–160 (1950).

[34] A. Hartman, Halving the complete design, *Ann. Discrete Math.* **34**, 207–224 (1987).

[35] M. Ito, A. Saito and T. Nishizeki, Multiple assignment scheme for sharing secret, *J. Cryptology.* **6**, 15–20 (1993).

[36] M. Jimbo, M. Mishima, S. Janiszewski, A. Y. Teymorian and V. D. Tonchev, On conflict-avoiding codes of length $n = 4m$ for three active users, *IEEE Trans. Inform. Theory* **53**(8), 2732–2742 (2007).

[37] M. Jimbo and K. Shiromoto, A construction of mutually disjoint Steiner systems from isomorphic Golay codes, *J. Combin. Theory Ser. A* **116**, 1245–1251 (2009).

[38] M. Jimbo and K. Shiromoto, Quantum jump codes and related combinatorial designs, D. Crnkovic'and V. Tonchev, *Information Security, Coding Theory and Related Combinatorics* **29**, 285–311 IOS Press (2011).

[39] G. G. Khosrovshahi and S. Ajoodani-Namini, Combining t-designs, *J. Combin. Theory Ser. A* **58**, 26–34 (1991).

[40] G. B. Khosrovshahi, R. Laue and B. Tayfeh-Rezaie, On large sets of t-designs of size four, *Bayreuth. Math. Schr.* **74**, 136–144 (2005).

[41] G. B. Khosrovshahi and B. Tayfeh-Rezaie, Some results on the existence of large sets of t-designs, *J. Combin. Des.* **11** 144-151 (2003).

[42] G. B. Khosrovshahi and B. Tayfeh-Rezaie, Large sets of t-designs through partitionable sets: A survey, *Discrete Math.* **306**, 2993–3004 (2006).

[43] E. S. Kramer, S. S. Magliveras and E. A. O'Brien, Some new large sets of t-designs, *Australas. J. Combin.* **7**, 189–193 (1993).

[44] R. Laue, S. S. Magliveras and A. Wassermann, New large sets of t-designs, *J. Combin. Des.* **9** 40–59 (2001).

[45] V. I. Levenshtein, One method of constructing quasi codes providing synchronization in the presence of errors, *Probl. Inf. Transm.* **7**(3), 215–222 (1971).

[46] V. I. Levenshtein, Conflict-avoiding codes and cyclic triple systems, *Probl. Inf. Transm.* **43**(3), 199–212 (2007).

[47] V. I. Levenshtein and V. D. Tonchev, Optimal conflict-avoiding codes for three active users, Proc. IEEE Int. Symp. Inform. Theory, Adelaide, Australia, Sep. 2005, 535–537 (2005).

[48] V. I. Levenshtein and A. J. Han Vinck, Perfect (d, k)-codes capable of correcting single peak-shifts, *IEEE Trans. Inform. Theory* **39**(2), 656–662 (1993).

[49] Y.-H. Lo, H.-L. Fu and Y.-H. Lin, Weighted maximum matchings and optimal equ-difference conflict-avoiding codes, *Des. Codes Cryptogr.*, (2014) DOI 10.1007/s10623-014-9961-5.

[50] J. X. Lu, On large sets of disjoint Steiner triple systems I, II and III, *J. Combin. Theory Ser. A* **37**, 140–182 (1983).

[51] J. X. Lu, On large sets of disjoint Steiner triple systems IV, V and VI, *J. Combin. Theory Ser. A* **37**, 136–192 (1984).

[52] W. Ma, C. Zhao and D. Shen, New optimal constructions of conflict-avoiding codes of odd length and weight 3, *Des. Codes Cryptogr.*, **73**(3), 791–804 (2014).

[53] S. S. Magliveras and T. E. Plambeck, New infinite families of simple 5-designs, *J. Combin. Theory Ser. A* **44**, 1–5 (1987).

[54] J. L. Massey and P. Mathys, The collision channel without feedback, *IEEE Trans. Inform. Theory* **31**(2), 192–204 (1985).

[55] R. A. Mathon, Searching for spreads and packings, *Geometry, Combinatorial Designs and Related Structures*, London Math. Soc. Lecture Note Ser. 245, Spetses 1996, Cambridge Univ. Press, 161–176 (1997).

[56] P. Mathys, A class of codes for a T active users out of N multiple-access communication system, *IEEE Trans. Inform. Theory* **36**(6), 1206–1219 (1990).

[57] Y. Miao, A combinatorial characterization of regular anonymous perfect threshold schemes, *Inform. Process. Lett.* **85**, 131–135 (2003).

[58] M. Mishima, H.-L. Fu and S. Uruno, Optimal conflict-avoiding codes of length $n \equiv 0 \pmod{16}$ and weight 3, *Des. Codes Cryptogr.* **52**(3), 275–291 (2009).

[59] K. Momihara, Necessary and sufficient conditions for tight equi-difference conflict-avoiding codes of weight three, *Des. Codes Cryptogr.* **45**(3), 379–390 (2007).

[60] K. Momihara, M. Müller, J. Satoh and M. Jimbo, Constant weight conflict-avoiding codes, *SIAM J. Discrete Math.* **21**(4), 959–979 (2007).

[61] A. Munemasa, On perfect t-shift codes in Abelian groups, *Des. Codes Cryptogr.* **5**(3), 253–259 (1995).

[62] A. Munemasa, Flag-transitive 2-designs arising from line-spreads in $PG(2n-1,2)$, *Geom. Dedicata* **77**, 209–213 (1999).

[63] Q. A. Nguyen, L. Györfi, and J. L. Massey, Constructions of binary constant-weight cyclic codes and cyclically permutable codes, *IEEE Trans. Inform. Theory* **38**(3), 940–949 (1992).

[64] D. Raghavarao, *Constructions and Combinatorial Problems in Design of Experiments*, Wiley, New York (1971).

[65] C. R. Rao, Factorial experiments derivable from combinatorial arrangements of arrays, *J. R. Stat. Soc. Suppl.* **9**, 128–139 (1947).

[66] P. J. Schellenberg and D. R. Stinson, Threshold schemes from combinatorial designs, *J. Combin. Math. Combin. Comput.* **5**, 143-160 (1989).

[67] S. Schreiber, Covering all triples on n marks by disjoint Steiner systems, *J. Combin. Theory Ser. A* **15**, 347–350 (1973).

[68] S. Schreiber, Some balanced complete block designs, *Israel J. Math.* **18**, 31–37 (1974).

[69] A. Shamir, How to share a secret, *Commun. ACM* **22**, 612–613 (1979).

[70] C. E. Shannon, A mathematical theory of communication, *Bell Syst. Tech. J.* **27**, 379–423, 623–656, July-October (1948).

[71] P. W. Shor, Scheme for reducing decoherence in quantum computer memory, *Phys. Rev. A* **52**, 2493–2496 (1995).

[72] K. W. Shum, W. S. Wong and C. S. Chen, A general upper bound on the size of constant-weight conflict-avoiding codes, *IEEE Trans. Inform. Theory* **56**(7), 3265–3276 (2010).

[73] N. J. A. Sloane, Seq. no. A001220, The On-line Encyclopedia of Integer Sequences, The OEIS Foundation Inc., `http://oeis.org/`.

[74] N. J. A. Sloane, Seq. no. A135304, The On-line Encyclopedia of Integer Sequences, The OEIS Foundation Inc., `http://oeis.org/`.

[75] A. M. Steane, Multiple particle interference and quantum error correction, *Proc. R. Soc. Lond. A* **452**, 2551–2577 (1996a).

[76] A. M. Steane, Error correcting codes in quantum theory, *Phys. Rev. Lett.* **77**, 793–797 (1996b).

[77] D. R. Stinson and S. A. Vanstone, A combinatorial approach to threshold schemes, *SIAM J. Discrete Math.* **1**, 230–237 (1988).

[78] B. Tayfeh-Rezaie, On the existence of large sets of t-designs of prime sizes, *Des. Codes Cryptogr.* **37** 143–149 (2005).

[79] L. Teirlinck, A completion of Lu's determination of the spectrum of large sets of disjoint Steiner Triple systems, *J. Combin. Theory Ser. A* **57**, 302–305 (1991).

[80] L. Teirlinck, Large sets of disjoint designs and related structures, *Contemporary Design Theory: A Collection of Surveys*, J. H. Dinitz and D. R. Stinson eds., Wiley-Intersci. Ser. Discrete Math. Optim. 561–592 (1992).

[81] L. Teirlinck, On the maximum number of disjoint triple systems, *J. Geom.* **12**, 93–96 (1975).

[82] L. Teirlinck, On large sets of disjoint quadruple systems, *Ars Combin.* **17**, 173–176 (1984).

[83] L. Teirlinck, Locally trivial t-designs and t-designs without repeated blocks, *Discrete Math.* **77**, 345–356 (1989).

[84] V. D. Tonchev, Quantum codes from caps, *Discrete Math.* **398**, 6368–6372 (2008).

[85] T. van Trung, On the construction of t-designs and the existence of some new infinite families of simple 5-designs, *Arch. Math.* **47**, 187–192 (1986).

[86] B. S. Tsybakov and A. R. Rubinov, Some constructions of conflict-avoiding codes, *Probl. Inf. Transm.* **38**(4), 268–279 (2002).

[87] S.-L. Wu and H.-L. Fu, Optimal tight equi-difference conflict-avoiding codes of length $n = 2^k \pm 1$ and weight three, *J. Combin. Des.* **21**(6), 223–231 (2013).

[88] F. Yates, Incomplete randomized blocks, *Ann. Eugen.* **7**, 121–40 (1936).

[89] G. Zémor, On Cayley graphs, surface codes, and the limits of homological coding for quantum error correction, In Proc. of the 2nd International Workshop on Coding and Cryptology, 259–273 (2009).