Combinatorial Designs with Certain Inner Structures and Number Theoretic Approaches to Their Existence

A dissertation submitted in partial fulfillment of the requirements for the degree of Doctor of Information Science

Xiaonan Lu

Department of Computer Science
and Mathematical Informatics
Graduate School of Information Science
Nagoya University

January, 2017

Acknowledgements

It is the sixth year since I came to Japan. I will never forget the day in March 2011 when I first went to meet Professor Masakazu Jimbo for graduate school applications. At that time, I knew very little about combinatorics and could not speak Japanese. He gave me much helpful advice for the admission exam and lent me the introductory textbook “Design Theory” written by Zhe-Xian Wan. That was the starting point for me to establish the connections to Nagoya University, and to combinatorial design theory. I am most grateful to Professor Masakazu Jimbo for leading me into the world of combinatorics and guiding the first step of my academic career. Under his supervision during my master’s course and the first year of my doctoral course, I learned a lot about doing research as a mathematician and as an applied mathematician.

I would like to express my sincere thanks to Professor Junya Satoh who advised me during the last two years of my doctoral course for his assistance and great support. I am very grateful to him for inspiring me to get into more in-depth studies of number theory. Without their patience, excellent guidance, and encouragement, this dissertation could not be completed.

I am particularly grateful to Professor Masanori Sawa at Kobe University, who was my co-advisor for master’s course. He encouraged me greatly for my first poster presentation and my first research manuscript, and introduced me to many workshops and conferences for communicating with a wide variety of researchers.

I gratefully acknowledge Professor Yo Matsubara and Professor Masahiro Yasumoto, who are the members of the dissertation committee, for their time and valuable feedback on my dissertations. I would like to give special thanks to Dr. Janet Nora Henderson, who carefully reviewed the English writing for this dissertation and gave me accurate advice.

I would like to express my gratitude to many people for helping me during my graduate studies. I would like to thank Emeritus Professor Ryoh Fuji-Hara and Professor Ying Miao at University of Tsukuba, who took care of me during my first international conference in Germany and helped me a lot for these years. I am also thankful to Professor Sanpei Kageyama, Professor Shinji Kuriki, Professor Akihiro Munemasa, Professor Masaaki Harada, Professor Keisuke Shiromoto, Professor Kiyoshi Yoshimoto, Professor Tomoko Adachi, Professor Miwako Mishima, Professor Nobuko Miyamoto, Professor Kazuki Matsubara, Professor Yuichiro Fujiwara, Professor Masatake Hirao, and Professor Koji Momihara for their help, advice, and encouragement.

I would like to express my sincere gratitude to Emeritus Professor Richard Wilson at California Institute of Technology, Professor Charles Colbourn at Arizona State University, Professor Hung-Lin Fu at National Chiao Tung University, Professor Chin-Mei Kau at Tamkang University, Professor Marco Buratti at Perugia University, Professor David Pike at Memorial University of Newfoundland, Professor Saad El-Zanati at Illinois State University, Professor Lijun Ji at Soochow University, and Professor Tao Feng at Beijing Jiaotong University for valuable discussions and suggestions on combinatorial designs and related research.

I would like to express my warm thanks to Professor Tao Feng at Zhejiang University, Professor Chih-Hung Yen at National Chiayi University, Professor Fei-Huang Chang and Professor Jun-Yi Guo at National Taiwan Normal University for providing me opportunities to present my work on their workshops.

I also owe my gratitude to our laboratory members, Dr. Yiling Lin, Kohei Yamada, and Shohei Satake, for their support and help.

Finally, I would like to thank my beloved parents, Fu-Zeng Lu and Yan-Li Huang, for their selflessness in these thirty years. Special thanks go to my wife Jin-Ling and my lovely sons, Jia-Chen (Ka-Shin) and Jia-Yi (Ka-Itsu), who accompanied me and made my life colorful. I could not have completed this work without their hearty encouragement.

This study was partially funded by JSPS Research Fellowships for Young Scientists during my doctoral course at Graduate School of Information Science in Nagoya University.

Xiaonan Lu
Nagoya University

Contents

1 Introduction **1**

1.1 Combinatorial t-designs . . . 3

1.2 Automorphism groups of t-designs and applications to optical communications . . . 5

1.3 Quadruple systems with a prescribed automorphism group . . . 8

1.4 Difference families and cyclotomic cosets . . . 11

1.5 Grid-block designs and grid-block difference families . . . 14

1.6 Outline of this dissertation . . . 18

2 Affine-invariant quadruple systems **19**

2.1 Graphs associated with $\mathrm{PSL}(2, q)$ . . . 20

2.1.1 LG graphs . . . 20

2.1.2 CG graphs . . . 25

2.1.3 Further remarks on CG graphs . . . 30

2.2 Affine-invariant strictly cyclic Steiner quadruple systems over $\mathbb{Z}_{2p}$ 31

2.2.1 Block presentations . . . 31

2.2.2 Direct construction A . . . 32

2.2.3 Direct construction B . . . 36

2.3 Affine-invariant strictly cyclic Steiner quadruple systems over $\mathbb{Z}_{2p^m}$ 43

2.3.1 Preliminaries . . . 43

2.3.2 Recursive construction A . . . 49

2.3.3 Recursive construction B . . . 55

2.4 A necessary condition for the existence of affine-invariant strictly cyclic Steiner quadruple systems . . . 59

2.5 Affine-invariant two-fold quadruple systems over $\mathbb{Z}_p$ . . . 60

2.6 Affine-invariant two-fold quadruple systems over $\mathbb{Z}_{p^m}$ . . . 61

2.7 Applications . . . 64

2.7.1 Searching blocks . . . 64

2.7.2 Generating blocks . . . 65

3 Grid-block difference families **67**

3.1 An intermediate consequence derived from Weil's Theorem on multiplicative character sums . . . 67

3.2 Direct constructions and asymptotic existence of grid-block difference families 73
3.2.1 Grid-block difference families with a multiplier of order 3 . . . 73
3.2.2 Row-radical grid-block difference families 75
3.3 Row-radical $2 \times k$ grid-block difference families with $k \geq 5$ 80
3.4 Kronecker density related to row-radical $2 \times k$ grid-block difference families 85
3.4.1 The Kronecker density of "good" primes 85
3.4.2 The Kronecker density of "arithmetic" primes 87
3.5 Recursive constructions 89

4 Resolvable grid-block coverings **91**
4.1 Construction of resolvable grid-block designs via grid-block difference families 91
4.2 Optimal resolvable grid-block coverings 94
4.3 Optimal resolvable 2×3 grid-block coverings 97

5 Concluding remarks and further problems **100**

List of papers related to this dissertation **102**

Bibliography **103**

Chapter 1

Introduction

Combinatorial design theory is a branch of combinatorics studying the systems of finite or discrete objects whose arrangements satisfy specified criteria, such as the properties of balance and symmetry. The study of design theory mainly involves the problems of finding a finite set system with restrictions on the membership and intersections, such as block designs and combinatorial codes. On the other hand, it could also involve the spatial arrangements of entries in arrays, such as magic squares and Latin squares.

Combinatorial inventions on magic squares can be traced back to high antiquity in early China. The Luoshu (Luo River Writing) square, which is legendarily believed to have been created between the 3rd and the 2nd millennium BC, is the earliest record of a 3×3 magic square with the numbers 1 to 9. In modern mathematics, the study of design theory has its roots in the work of L. P. Euler who posed the "36 officer problem" in 1782. This problem is equivalent to finding "mutually orthogonal Latin squares (MOLSs)" of order 6. Euler also conjectured that MOLSs of order n do not exist for any $n \equiv 2 \pmod 4$, which was known as Euler's conjecture until it was shown to be false by Bose, Shrikhande, and Parker [11] in 1960. Later in the 19th century, combinatorial designs were studied as geometric configurations by T. P. Kirkman, J. Steiner, and A. Cayley.

In the 1930s, the development of statistical experimental designs greatly promoted research on combinatorial designs. A milestone of design theory was established by Fisher and Yates, who made use of "balanced incomplete block designs" (BIBDs) and "lattice squares" for agricultural experiments [45, 127, 128]. Around the same time, Bose [10] published a long paper on the constructions of BIBDs, in which a most significant construction technique for designs, called "the method of differences", was proposed. Along this direction, the existence and construction of "difference families" has become a rapidly expanding subject with fundamental importance. In terms of contemporary design theory, a BIBD is a 2-design, and a difference family generates a 2-design with an automorphism group acting sharply transitively on its points. The main problems for design theory in recent stages can be summarized as "existence", "construction", and "characterization".

Constructions of designs fall into two categories, direct constructions and recursive constructions. For 2-designs, difference families are commonly used for direct constructions, and related studies have been investigated by intensive use of finite fields, finite groups, and algebraic number theory. However, recursive constructions are usually purely combinatorial. Infinite families of new designs can be obtained from known designs via recursive constructions, like an interlocking puzzle game. The most outstanding recursive construction of 2-designs is due to Wilson [121], who proposed the "pairwise balanced design (PBD) construction" and then revolutionarily established the existence of 2-designs. Thereafter, using similar ideas, various recursive constructions have been studied, and excellent progress has been made on the existence of designs.

In contrast, only a few constructions for t-designs with $t \geq 3$ are known. In the mid 20th century, before the completion of the classification of finite simple groups, group theorists found a close relationship between high transitivity of finite groups and designs. They tried to develop research on finite groups via the study of t-designs with large t [124]. However, non-trivial t-designs have been proved to exist for any positive integer t by Teirlinck [113], which leads to a gap with highly transitive finite groups. Recently, Keevash [63] settled the existence of t-designs for all but finitely many admissible parameters by a new probabilistic method referred to as "randomized algebraic construction". Nevertheless, to find an explicit construction for a t-design with given parameters is still difficult in general. In particular, for the cases when $t \geq 3$, the existence of a t-design which is invariant under a prescribed permutation group without high transitivity is still often unknown.

Characterizations of designs study the inner structures of a design, which roughly fall into two aspects, algebraic characterizations and geometric characterizations. For the algebraic aspects, the "automorphism groups" of a design is the main theme. In other words, it is desired to consider designs which are invariant under a permutation group. In particular, cyclic designs are desired for applications to communication systems. For the geometric aspects, a design can be viewed as a "geometry" consisting of "points" and "lines", and the intersections between "lines" are the most important. In particular, if a design can be partitioned into subsystems, each of which forms a "parallel class" of lines, then the design is said to be resolvable. For applications to experiments and group testings, resolvability plays an important role.

In this dissertation, we will concentrate on two kinds of designs, both of which have specific inner structures. Firstly, we consider 3-designs which are invariant under the generalized affine groups, which are a special type of cyclic 3-designs. Secondly, we will study the difference families with respect to "grid-block designs", which are known to play an essential role for DNA library screening and other group testing models for experiments. For both types, approaches to the direct constructions and existence will be given by employing group theoretic and number theoretic tools. Recursive constructions and computational results will also be used to establish their existence.

This chapter is devoted to providing a brief introduction and preliminaries in design theory. Some basic concepts and properties on t-designs will be presented in Sections 1.1 and 1.2. Moreover, we will focus mainly on 3-designs with prescribed automorphism groups, difference families, and grid-block designs in Sections 1.3, 1.4, and 1.5, respectively.

Before proceeding further, we introduce some notation that will be used throughout this dissertation.

Let V be a finite set and let X be a subset of V with $|X| = k$, where $|X|$ is the cardinality of X. Then we also say X is a k-subset of V and denote all the k-subsets of V by $\binom{V}{k}$. Moreover, let 2^V denote the set consisting of all the subsets of V. We also use $\#X$ to denote the cardinality of X, especially when X has a complicated set-builder notation with a vertical bar in it.

Moreover, suppose Ω is a permutation group acting on V. Then Ω acts naturally on $\binom{V}{k}$ for any positive integer k. For any $B \in \binom{V}{k}$, let $\mathcal{O}_\Omega(B)$ denote the orbit of B under the action of Ω, that is $\mathcal{O}_\Omega(B) = \{B^\omega \mid \omega \in \Omega\}$. Moreover, for any $\mathcal{B} \subseteq 2^V$, let $\mathcal{O}_\Omega(\mathcal{B}) = \bigcup_{B\in\mathcal{B}} \mathcal{O}_\Omega(B)$. If $\mathcal{O}_\Omega(\mathcal{B}) = \mathcal{B}$, then $\mathcal{B}$ is said to be *invariant* under the action of Ω, or Ω leaves $\mathcal{B}$ invariant.

Let G be an additive group and let X, Y be subsets of G. We denote $X + Y = \{x + y \mid x \in X, y \in Y\}$ and $X + a = \{x + a \mid x \in X\}$ for any $a \in G$.

For positive integers a, b with $a < b$, let $[a, b]$ denote the set $\{a, a+1, \ldots, b\}$. In particular, let $[n]$ denote the set $\{1, 2, \ldots, n\}$ for a positive integer n. For a real number x, let $\lfloor x \rfloor$ denote the the largest integer less than or equal to x.

Let $\mathbb{Z}_n$ denote the ring of integers modulo n, that is $\mathbb{Z}/n\mathbb{Z}$. Let $\mathbb{Z}_n^\times$ and $\mathbb{Z}_n^*$ denote the multiplicative group and the set of all nonzero elements, respectively, of $\mathbb{Z}_n$. We also use $\mathbb{Z}_n$ for the cyclic group of order n. Let $\mathbb{F}_q$ denote the finite field of order q and let $\mathbb{F}_q^*$ denote the multiplicative group of $\mathbb{F}_q$, that is, the set of all nonzero elements of $\mathbb{F}_q$. More notation for further discussion over $\mathbb{F}_q$ will be introduced in Section 1.4.

1.1 Combinatorial t-designs

In this section, we give a brief overview of some basic concepts and important results of combinatorial t-designs.

Definition 1.1.1 (t-design)**.** Let V be a finite set of v points, and let $\mathcal{B}$ be a collection of k-subsets (blocks) of V. The pair $(V, \mathcal{B})$ is called a t-(v, k, λ) *design* if every t-subset appears in exactly λ blocks of $\mathcal{B}$.

The parameters k and λ are called *block size* and *index*, respectively. $(V, \mathcal{B})$ is said to be *simple* if there are no repeated blocks in $\mathcal{B}$. A 2-design is well known as a *balanced incomplete block design* (BIBD), which is commonly used for experimental designs. In the case of $\lambda = 1$, t-designs are also called *Steiner systems*. In particular, 2-$(v, 3, 1)$ designs and 3-$(v, 4, 1)$ designs are known as *Steiner triple systems* and *Steiner quadruple systems*, and denoted by STS(v) and SQS(v), respectively.

The earliest study involving t-designs can be traced to Plücker [95], in 1835, who mentioned a 2-$(9, 3, 1)$ design (STS(9)) in his work on algebraic curves.

Later, in 1839, Plücker [96] described a 3-$(28,4,1)$ design (SQS(28)) and then he asked what kind of parameters t and v are realizable for a t-$(v,t+1,1)$ design. In 1844, Woolhouse [125] presented a more general problem: does there exist $(V,\mathcal{B})$ such that any t-subset of V is contained in at most one block? Such a design is now known as a t-packing design (see Definition 1.2.9).

By counting the number of blocks containing a fixed i-subset I for $0 \le i \le t$, we have

$$\#\{B \in \mathcal{B} \mid I \subset B\} = \lambda \frac{\binom{v-i}{t-i}}{\binom{k-i}{t-i}},$$

which implies the following divisibility conditions:

Proposition 1.1.2 (divisibility conditions)**.** If there exists a t-(v,k,λ) design, then

$$\lambda\binom{v-i}{t-i} \equiv 0 \pmod{\binom{k-i}{t-i}} \quad \text{for any } 0 \le i \le t. \tag{1.1}$$

Proposition 1.1.3 (divisibility conditions for 2-designs)**.** If there exists a 2-(v,k,λ) design, then

$$\lambda v(v-1) \equiv 0 \pmod{k(k-1)} \quad \text{and} \quad \lambda(v-1) \equiv 0 \pmod{k-1}. \tag{1.2}$$

For Steiner triple systems, Kirkman [64] proved that the divisibility conditions (1.2) are also sufficient. Six years later, without knowing Kirkman's work, Steiner [109] noticed the divisibility condition, that is $v \equiv 1,3 \pmod 6$, and presented the problem of the existence of Steiner triple systems. Actually, for 2-designs with larger k, the results are also plentiful. The existence problem of 2-$(v,4,1)$ designs and 2-$(v,5,1)$ designs were solved by Hanani [53, 54] in 1961 and 1972, respectively. For $6 \le k \le 9$, the existence of 2-designs are nearly completely settled except for some small parameters (see [34] §3.1 for details). It is notable that, in order to show the existence of 2-designs, Wilson [121, 122, 123] developed an outstanding construction, called PBD-construction, and finally proved the following theorem:

Theorem 1.1.4 (Wilson [123])**.** *For given k and λ and for a sufficiently large $v \ge v_0(k,\lambda)$, the divisibility conditions* (1.2) *are sufficient for the existence of a* 2-(v,k,λ) *design.*

It is nature to consider a 2-(v,k,λ) design as a decomposition of $K_v^{(\lambda)}$ into k-cliques, where $K_v^{(\lambda)}$ denotes the complete multi-graph with v vertices such that there are λ edges between every pair of vertices. In particular, when $\lambda = 1$, $K_v^{(1)}$ is the complete graph of order v in the usual sense. We can also replace "k-clique" to any other subgraph of K_v for "graph decompositions" in general. For "graph decompositions", there are plenty of literature, and the formal definitions will be given in Section 1.5. For more details, the interested readers may refer to [34] §VI.24.

In contrast, the constructions for t-designs with $t \ge 3$ are quite rare. First, we give a brief historical review on the study of Steiner quadruple systems, which are the minimal nontrivial classes for $t \geq 3$. In 1847, Kirkman [64] proved that for any positive integer n, there exists an SQS(2^n). Nearly 70 years later, Fitting [46] constructed an SQS(26) and an SQS(34) by proposing a graph theoretic construction. Eventually, the existence of Steiner quadruple systems was settled by Hanani [52] in 1960 via a series of complicated recursive constructions. Thereafter, Lenz [70] and Hartman [55] simplified Hanani's proof. Recently, Zhang and Ge [132] proposed a new proof which is more elegant and more concise.

Theorem 1.1.5 (Hanani [52]). *There is an SQS(v) if, and only if, $v \equiv 2, 4 \pmod 6$.*

The first existence result of t-designs dealing with general t is due to Teirlinck [113] who showed the following theorem:

Theorem 1.1.6 (Teirlinck [113]). *There exists a non-trivial t-design for any positive integer t.*

It should be mentioned that Keevash [63] posted work in 2014 which claims that the divisibility conditions (1.1) for a t-(v, k, λ) design are sufficient for all but finitely many admissible parameters. Keevash's proof relies deeply on probabilistic combinatorics, and his new method is referred to as "randomized algebraic construction". Nevertheless, the constructions for a t-(v, k, λ) design are still of interest, from both theoretical and application reasons.

Finally, we introduce the concept of *resolvability* for t-designs. A t-design $(V, \mathcal{B})$ is said to be *resolvable* if $\mathcal{B}$ can be partitioned into *parallel classes* (also known as *resolution classes*), where each parallel class is a partition of V.

1.2 Automorphism groups of t-designs and applications to optical communications

In this section, we focus on t-designs with specific algebraic inner structures, that is, t-designs admitting specific automorphism groups. Also, some applications of cyclic designs to optical communications will be interpreted.

Definition 1.2.1 (automorphism groups of t-designs). Let G be a permutation group acting on V and let $(V, \mathcal{B})$ be a t-(v, k, λ) design. If G leaves $\mathcal{B}$ invariant, then G is called an *automorphism group* of $(V, \mathcal{B})$. In this case, $\mathcal{B}$ can be partitioned into orbits under the action of G. We can choose any block in an orbit as a *base block* to represent the whole orbit. For any $B \in \mathcal{B}$, if $|\mathcal{O}_G(B)| = |G|$, then $\mathcal{O}_G(B)$ is said to be *full*, otherwise *short*.

Furthermore, if $|V| = v$ and G is the cyclic group of order v, then the orbits are called *cyclic orbits* and $(V, \mathcal{B})$ is said to be *cyclic*. If $\mathcal{B}$ gives no short orbit under the action of G, then $(V, \mathcal{B})$ is said to be *strictly cyclic*. In these cases, the point set V can be identified with $\mathbb{Z}_v$. Strictly cyclic 2-designs are equivalent to cyclic difference families, which will be discussed in detail in Section 1.4.

Example 1.2.2. Let $V = \mathbb{Z}_{10}$ and let $\mathcal{B}$ be the collection of the following blocks:

$$\begin{array}{lll}
\{0,1,5,9\}, & \{0,2,5,8\}, & \{0,1,3,4\}, \\
\{1,2,6,0\}, & \{1,3,6,9\}, & \{1,2,4,5\}, \\
\{2,3,7,1\}, & \{2,4,7,0\}, & \{2,3,5,6\}, \\
\{3,4,8,2\}, & \{3,5,8,1\}, & \{3,4,6,7\}, \\
\{4,5,9,3\}, & \{4,6,9,2\}, & \{4,5,7,8\}, \\
\{5,6,0,4\}, & \{5,7,0,3\}, & \{5,6,8,9\}, \\
\{6,7,1,5\}, & \{6,8,1,4\}, & \{6,7,9,0\}, \\
\{7,8,2,6\}, & \{7,9,2,5\}, & \{7,8,0,1\}, \\
\{8,9,3,7\}, & \{8,0,3,6\}, & \{8,9,1,2\}, \\
\{9,0,4,8\}, & \{9,1,4,7\}, & \{9,0,2,3\}.
\end{array}$$

Then $(V, \mathcal{B})$ is a 3-$(10, 4, 1)$ design (SQS(10)), which is strictly cyclic. Each cyclic orbit consists of the ten blocks listed in each column.

Then, we introduce the concept of the affine-invariant property for a cyclic t-design.

Definition 1.2.3 (multiplier)**.** Let $(\mathbb{Z}_v, \mathcal{B})$ be a cyclic t-design and let α be a unit in $\mathbb{Z}_v$, that is $\alpha \in \mathbb{Z}_v^\times$. For any $B \in \mathcal{B}$, if $\alpha B \in \mathcal{B}$, then α is called a *multiplier* of $(\mathbb{Z}_v, \mathcal{B})$.

Definition 1.2.4 (affine-invariant t-design)**.** A cyclic t-design $(\mathbb{Z}_v, \mathcal{B})$ is said to be *affine-invariant*, if every $\alpha \in \mathbb{Z}_v^\times$ is a multiplier.

In other words, an affine-invariant t-design $(\mathbb{Z}_v, \mathcal{B})$ admits the group A as its automorphism group, where A is the general affine group of degree one over $\mathbb{Z}_v$ defined by

$$A = \{(i, \alpha) \mid i \in \mathbb{Z}_v, \alpha \in \mathbb{Z}_v^\times\} \cong \mathbb{Z}_v \rtimes \mathbb{Z}_v^\times.$$

For a subset $S \subseteq \mathbb{Z}_v$, the *affine orbit* of S is the orbit of S under the action of the general affine group A , denoted by $\mathcal{O}_A(S)$.

Example 1.2.5. The unique (up to isomorphism) SQS(10) in Example 1.2.2 is affine-invariant. Take

$$B_1 = \{0,1,5,9\}, \quad B_2 = \{0,2,5,8\}, \text{ and } B_3 = \{0,1,3,4\}$$

as base blocks of the cyclic orbits. We have $B_1 \times 3 + 5 = \{0,3,5,7\} + 5 = \{5,8,0,2\} = B_2$ over $\mathbb{Z}_{10}$. Hence, the cyclic orbits of B_1 and B_2 are contained in the same affine orbit. In fact, there are only two affine orbits, namely, $\mathcal{O}_A(B_1)$ $(= \mathcal{O}_A(B_2))$ and $\mathcal{O}_A(B_3)$.

Now we begin to consider a family of combinatorial codes. An optical orthogonal code (briefly, OOC) is a binary code with good auto- and cross-correlation properties. The study of OOCs is motivated by applications to code-division multiple-access (CDMA) communication by fiber-optic channels. Low auto- and cross-correlations can efficiently reduce conflicts with undesired signals in communication (see [32]). We first give the definition of optical orthogonal codes from the point of view of binary codes.

Definition 1.2.6 (optical orthogonal code)**.** A binary code $\mathcal{C} \subseteq \{0,1\}^n$ is called an *optical orthogonal code* with parameter $(n, k, \lambda_a, \lambda_c)$ (briefly, an $(n, k, \lambda_a, \lambda_c)$-OOC), if the following properties hold:

(i) For any codeword $\boldsymbol{x} = (x_0, x_1, \cdots, x_{n-1}) \in \mathcal{C}$, the Hamming weight $\mathrm{w}(\boldsymbol{x}) = k$;

(ii) For any codeword $\boldsymbol{x} = (x_0, x_1, \cdots, x_{n-1}) \in \mathcal{C}$ and any relative delay offset $\tau \not\equiv 0 \pmod{n}$, the Hamming auto-correlation of $\boldsymbol{x}$ satisfies

$$H_{\boldsymbol{x}}(\tau) = \sum_{t=0}^{n-1} x_t x_{t+\tau} \leq \lambda_a;$$

(iii) For any pair of distinct codewords $\boldsymbol{x} = (x_0, x_1, \cdots, x_{n-1}) \in \mathcal{C}$, $\boldsymbol{y} = (y_0, y_1, \cdots, y_{n-1}) \in \mathcal{C}$ and any relative delay offset τ, the Hamming cross-correlation of $\boldsymbol{x}$ and $\boldsymbol{y}$ satisfies

$$H_{\boldsymbol{x},\boldsymbol{y}}(\tau) = \sum_{t=0}^{n-1} x_t y_{t+\tau} \leq \lambda_c,$$

where the subscripts of x_i and y_j are reduced modulo n. In particular, if $\lambda_a = \lambda_c = \lambda$, we simply write an (n, k, λ)-OOC. The number of codewords in $\mathcal{C}$ is called the *size* of $\mathcal{C}$.

Alternatively, the definition can be rephrased by considering the support of each codeword $\boldsymbol{x}$, that is the set of indices of all nonzero coordinates of $\boldsymbol{x}$. Then we can identify $\mathcal{C}$ with a collection of k-subsets of $\mathbb{Z}_n$.

Definition 1.2.7 (an optical orthogonal code as a set system)**.** Let $\mathcal{C}$ be a collection of subsets of $\mathbb{Z}_n$, $\mathcal{C}$ is called an $(n, k, \lambda_a, \lambda_c)$ optical orthogonal code if

(i)$'$ For any $X \in \mathcal{C}$, $|X| = k$;

(ii)$'$ For any $X \in \mathcal{C}$ and any nonzero $\tau \in \mathbb{Z}_n$, $|X \cap (X + \tau)| \leq \lambda_a$;

(iii)$'$ For any distinct $X, Y \in \mathcal{C}$ and any $\tau \in \mathbb{Z}_n$, $|X \cap (Y + \tau)| \leq \lambda_c$.

For given parameters (n, k, λ), we denote the largest possible size of an (n, k, λ)-OOC by $\Phi(n, k, \lambda)$. An (n, k, λ)-OOC $\mathcal{C}$ is said to be *optimal* if $|\mathcal{C}| = \Phi(n, k, \lambda)$. In general, it is hard to determine the exact value of $\Phi(n, k, \lambda)$ for certain (n, k, λ). However, an OOC can be seen as a constant weight error-correcting code. Thus $\Phi(n, k, \lambda)$ can be bounded above by the Johnson bound $J(v, k, \lambda)$ [62].

Proposition 1.2.8 (Johnson bound [62]).

$$\Phi(n,k,\lambda) \le \left\lfloor \frac{1}{k} \left\lfloor \frac{n-1}{k-1} \left\lfloor \frac{n-2}{k-2} \left\lfloor \cdots \left\lfloor \frac{n-\lambda}{k-\lambda} \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor \right\rfloor =: J(v,k,\lambda)$$

Optimal OOCs are closely related to t-designs and t-packings.

Definition 1.2.9. A t-(v,k,λ) *packing design*, or simply a t-(v,k,λ) *packing*, is a pair $(V,\mathcal{B})$, where V is a set of v points, and $\mathcal{B}$ is a collection of k-subsets (blocks) of V, such that any t-subset of V appears in at most λ blocks.

Clearly, a t-packing generalizes the notion of a t-design. Similarly, a t-(v,k,λ) packing is cyclic if it admits $\mathbb{Z}_v$ as its automorphism group, and it is *strictly cyclic* if all the cyclic orbits are full. A strictly cyclic t-(v,k,λ) packing is said to be *optimal* if the number of base blocks, say b, attains the following equality (see [102]):

$$b \le \left\lfloor \frac{1}{k} \left\lfloor \frac{v-1}{k-1} \left\lfloor \frac{v-2}{k-2} \left\lfloor \cdots \left\lfloor \frac{v-t+1}{k-t+1}\lambda \right\rfloor \cdots \right\rfloor \right\rfloor \right\rfloor \right\rfloor. \tag{1.3}$$

There is an equivalence between an optimal OOC and an optimal t-packing.

Theorem 1.2.10 (Fuji-Hara and Miao [48], Chu [31]). *Any optimal* (v,k,λ)-*OOC is equivalent to an optimal strictly cyclic* $(\lambda+1)$-$(v,k,1)$ *packing, provided that* $1 \le \lambda < k-1$.

In particular, a strictly cyclic SQS(v) is equivalent to an optimal $(v,4,2)$-OOC. In Section 1.3, we will introduce some important results on strictly cyclic SQSs.

1.3 Quadruple systems with a prescribed automorphism group

In this section, we draw our attention to quadruple systems, that is 3-$(v,4,\lambda)$ designs. As stated before, we write an SQS(v) for a 3-$(v,4,1)$ design. Moreover, we write a TQS(v) for a two-fold quadruple system, that is a 3-$(v,4,2)$ design. Firstly, we will briefly introduce the results on cyclic SQSs. Let σ denote the permutation on $\mathbb{Z}_v$ defined by $a^\sigma = -a$, and let $\widehat{\mathbb{Z}_v} = \mathbb{Z}_v \rtimes \langle\sigma\rangle$. A block B is said to be *symmetric* if $\mathcal{O}_{\mathbb{Z}_v}(B) = \mathcal{O}_{\widehat{\mathbb{Z}_v}}(B)$. A cyclic SQS $(V,\mathcal{B})$ is said to be *symmetric* if every block in $\mathcal{B}$ is symmetric and $\mathcal{B}$ is invariant under the action of $\widehat{\mathbb{Z}_v}$.

Now we denote a cyclic SQS by a *CSQS*, a strictly cyclic SQS by an *sSQS*, and a symmetric cyclic SQS by an *S-cyclic SQS*. A divisibility condition for the existence of an sSQS(v) can be easily shown.

Proposition 1.3.1 (Köhler [65]). If an sSQS(v) exists, then $v \equiv 2, 10 \pmod{24}$.

We have mentioned that Fitting [46] constructed an SQS(26) and an SQS(34) in 1915. In fact, those SQSs are S-cyclic. The most famous construction of S-cyclic sSQSs is due to Köhler [65], who introduced the notion of "first Köhler graphs".

Theorem 1.3.2 (Köhler [65]). *Let $v \equiv 2, 10 \pmod{24}$. If the first Köhler graph has a 1-factor, then there exists an sSQS(v).*

In order to facilitate the process of finding a 1-factor, Köhler [65] investigated the multiplier automorphisms on those graphs, and introduced the "Köhler orbit graphs" (see also [12, 66, 71]). Along this direction, Siemon [103] investigated "Köhler orbit graphs" for a few more parameters.

Lemma 1.3.3 (Köhler [65], Siemon [103]). *There exists an sSQS(v) if*

(i) $v \in \{2, 10, 26, 34, 50, 58, 74, 82, 106, 178, 202, 226, 274, 298, 346, 394, 466, 586, 634\}$,

(ii) $v \in \{122, 170, 194, 314, 338, 386, 458, 578\}$.

By observing the "embedding" structure of "Köhler orbit graphs", Siemon [103, 104] proposed infinite families of sSQSs.

Theorem 1.3.4 (Siemon [103, 104]). *Let m be a positive integer. For $p \equiv 5 \pmod{12}$, if the "Köhler orbit graph" with respect to an sSQS($2p$) has a 1-factor, then an sSQS($2p^m$) exists.*

Thereafter, Siemon [105] found that the existence of 1-factors of "Köhler orbit graphs" can be reduced to a number theoretic conjecture called "complete interval conjecture" (see also [2] Problem 146), and verified the conjecture for more parameters.

Theorem 1.3.5 (Siemon [105]). *There exists an S-cyclic sSQS($2p$) for all prime $p \equiv 53, 77 \pmod{120}$ and $p < 500000$.*

Piotrowski presented a number of important results on S-cyclic sSQSs in his dissertation [93] (see also [104]).

Theorem 1.3.6 (Piotrowski [93]). *There exists an S-cyclic sSQS($2p$) for a prime p if*

(i) $p \equiv 1 \pmod 4$ *and* $p \leq 229$, *or*

(ii) $p \equiv 1 \pmod 4$ *and* $p \not\equiv 1, 49 \pmod{60}$ *and* $p < 15000$.

Theorem 1.3.7 (Piotrowski [93] Satz 14.1). *There exists an S-cyclic SQS(v) if and only if $v \equiv 0 \pmod 2$, $v \not\equiv 0 \pmod 3$, $v \not\equiv 0 \pmod 8$, $v \geq 4$, and there exists an S-cyclic SQS($2p$) for any prime divisor p of v .*

Bitan and Etzion [8] extended Köhler's graph construction [65] and refined Siemon's "complete interval conjecture" [105] for S-cyclic SQS($4p$). They verified the number theoretic conjecture by computer programs and showed the following:

Theorem 1.3.8 (Bitan and Etzion [8])**.** *There is an S-cyclic SQS*$(4p)$ *for any prime* $p \equiv 5 \pmod{12}$ *with* $p < 1500000$*.*

For more information about CSQSs and SQSs with other specified automorphism groups, the reader may refer to Lindner and Rosa [78], Grannel and Griggs [51], Hartman and Phelps [55], and Siemon [107]. Notably, Munemasa and Sawa [83] generalized "Köhler orbit graphs" and Piotrowski's theorem on CSQSs to an abelian group A whose Sylow 2-subgroup is cyclic, and established the theory for symmetric A-invariant SQSs.

Recursive constructions of 3-designs with a point-regular automorphism group are more complicated than that of 2-designs (difference families). For recent progress on recursive constructions, the reader may refer to Feng, Chang, and Ji [44], Feng and Chang [43], and Li and Ji [72].

Next, we consider an affine-invariant sSQS(v) which is simply written as an AsSQS(v). In general, the number of affine orbits is much less than that of cyclic orbits. For instance, the number of affine orbits of the AsSQS(v) obtained by our Construction 2.2.20 is approximately $\frac{1}{6}v$. In contrast, the number of cyclic orbits is approximately $\frac{1}{24}v^2$ (see Tables 2.4 and 2.5 in Section 2.2.3). From the viewpoint of OOCs, the storage requirements of codewords are reduced by up to $\frac{1}{4}v$ times. Therefore, we are willing to consider an AsSQS rather than just an sSQS.

Constructions for AsSQSs are less known. Piotrowski [93] proved the following Theorem 1.3.9 (see also [104]). All the previously mentioned results use the aid of some graphs.

Theorem 1.3.9 (Piotrowski [93])**.** *There exists an AsSQS*$(2p)$ *for prime* $p \equiv 1 \pmod{4}$ *if* $p \not\equiv 1, 49 \pmod{60}$ *and* $p < 15000$*, or* $p \leq 229$*.*

On the other hand, without the help of graphs, Yoshikawa [129] independently presented an algorithm for constructing an AsSQS$(2p)$ and obtained the following theorem:

Theorem 1.3.10 (Yoshikawa [129])**.** *There exists an AsSQS*$(2p)$ *for prime* $p \equiv 1, 5 \pmod{12}$ *with* $17 \leq p < 200$*.*

Although the parameters are covered by Piotrowski's Theorem 1.3.9, the resulting AsSQSs can be shown to be non-isomorphic. We will characterize Yoshikawa's idea and propose a criterion for the existence of this kind of AsSQSs in Section 2.2.3.

Furthermore, affine-invariant 3-$(v, 4, \lambda)$ designs for $\lambda \geq 2$ have also been studied by Köhler [67], who proposed necessary and sufficient conditions for the existence of an affine-invariant 3-$(p, 4, \lambda)$ design when p is prime and $\lambda \geq 2$ (see also [13]). However, Köhler's construction for a TQS(p) also relies on "Köhler orbit graphs", and hence did not able to give an infinite family. In Sections 2.5 and 2.6, we will consider an affine-invariant TQS(p) and develop a recursive construction to provide an infinite family of affine-invariant TQSs, that is an affine-invariant TQS(p^m) for prime p and any positive integer m.

Lastly, for 3-fold quadruple systems with specific automorphism groups, Munemasa and Sawa [82] provided a perfect answer to their existence, which can be seen as a generalization of Köhler's results [67]. They proved that there exists a simple 3-fold quadruple system with $A \rtimes \mathrm{Aut}(A)$ as its automorphism group for any abelian group A of order $v \equiv 2 \pmod 4$. Moreover, for resolvable quadruple systems, Sawa [100] considered the resolution classes under cyclic permutations, and proved that the necessary divisibility conditions for the existence of a λ-fold quadruple system with a cyclic resolution are sufficient for any $\lambda \equiv 0 \pmod 3$.

1.4 Difference families and cyclotomic cosets

Let G be a finite group of order v, written additively, and let k be a positive integer. Let A be a subset of G. Then the multiset

$$\Delta A = \{x - y \mid x, y \in A, x \neq y\}$$

is defined to be the *list of differences* of A.

Definition 1.4.1 (difference family)**.** Let $\mathcal{A}$ be a collection of subsets of G. If every nonzero element of G occurs exactly λ times in the list $\Delta\mathcal{A} = \bigcup_{A \in \mathcal{A}} \Delta A$ then $\mathcal{A}$ is called a (v, k, λ) *difference family* (DF) over G, where v is the *order* of the DF. The members of $\mathcal{A}$ are called *base blocks*.

The number of base blocks should be $\frac{\lambda(v-1)}{k(k-1)}$, which implies the necessary divisibility condition

$$\lambda(v-1) \equiv 0 \pmod{k(k-1)} \tag{1.4}$$

for the existence of a (v, k, λ)-DF.

Example 1.4.2. Let

$$B_1 = \{0, 1, 3, 13, 34\}, B_2 = \{0, 4, 9, 23, 45\}, \text{ and } B_3 = \{0, 6, 17, 24, 32\}.$$

Then $\{B_1, B_2, B_3\}$ forms a $(61, 5, 1)$-DF over $\mathbb{Z}_{61}$.

Moreover, if all the base blocks of a (v, k, λ)-DF, say $\mathcal{A}$, are mutually disjoint, then $\mathcal{A}$ is said to be a (v, k, λ) *disjoint difference family* (DDF). DDFs have an important application, that is the construction of resolvable 2-designs via DDFs due to Ray-Chaudhuri and Wilson [98] (see also [50] Theorem 3.2.5).

A (v, k, λ)-DF over a cyclic group $\mathbb{Z}_v$ is simply denoted by a (v, k, λ) *cyclic difference family* (CDF). By translating the base blocks of a (v, k, λ)-CDF, one can immediately obtain a strictly cyclic 2-(v, k, λ) design. Moreover, if G is an elementary abelian group, that is an abelian group in which every nonzero element has the same order, then a (v, k, λ)-DF over G is said to be *elementary abelian*. This is equivalent to considering an elementary abelian DF of order q as in the additive group of the finite field $\mathbb{F}_q$ for a prime power q. The existence and constructions of DFs over $\mathbb{Z}_v$ and $\mathbb{F}_q$ have been extensively studied as essential problems in design theory.

The existence of elementary abelian $(q, 3, 1)$-DFs was settled by Netto [87]. For $4 \leq k \leq 6$, constructions and existence were investigated by Bose [10], Buratti [14, 15, 16, 17], and Wilson [120] over nearly six decades, and were finally settled by Chen and Zhu [28, 29]. We summarize the results as follows:

Theorem 1.4.3. *For $3 \leq k \leq 6$, there exists a $(q, k, 1)$-DF over $\mathbb{F}_q$ for any prime power $q \equiv 1 \pmod{k(k-1)}$ except for $(q, k) = (61, 6)$.*

When $k \geq 7$, existence has not been completely determined. However, the asymptotic existence has been established by Wilson [120].

Theorem 1.4.4 (Wilson [120])**.** *Let q be a prime power with $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$. Then there exists a (q, k, λ)-DF over $\mathbb{F}_q$ if one of the following holds:*

(i) λ *is a multiple of* $\frac{k}{2}$ *or* $\frac{k-1}{2}$*,*

(ii) $\lambda \geq k(k-1)$*,*

(iii) $q > \binom{k}{2}^{k(k-1)}$*.*

The bound in Theorem 1.4.4 (iii) for the asymptotic existence of elementary abelian DFs was greatly improved by Buratti and Pasotti [21] as

$$q > \binom{k}{2}^{2k}. \tag{1.5}$$

This is a consequence of Buratti and Pasotti's [21] main theorem (see Theorem 1.4.8) which can be more widely applied. We will discuss the ideas of the proofs in detail in Section 3.1.

The existence of $(v, k, 1)$-CDFs was solved for $k = 3$ by Peltesohn [89] a long time ago. However, the cases when $k \geq 4$ remains unsolved so far. A recursive construction was introduced by Colbourn and Colbourn [35] and then generalized by Jimbo and Kuriki [61] utilizing the notation of cyclic difference matrices.

Definition 1.4.5 (cyclic difference matrix)**.** A (v, k, λ) *cyclic difference matrix* (CDM) is defined to be a $k \times \lambda v$ matrix $M = (m_{ij})$ with entries in $\mathbb{Z}_v$, where for any pair of indices (i_1, i_2), the list of differences $\{m_{i_1 j} - m_{i_2 j} \mid 1 \leq j \leq \lambda v\}$ covers every element of $\mathbb{Z}_v$ exactly λ times.

In particular, when $\lambda_1 = \lambda_2 = 1$, if u is an integer which is relatively prime to $(k-1)!$, then a $(u, k, 1)$-CDM exists (see [35]).

Theorem 1.4.6 (Jimbo and Kuriki [61])**.** *If there exists a (v, k, λ_1)-CDF, a $(u, k, \lambda_1\lambda_2)$-CDF, and a (u, k, λ_2)-CDM, then there exists a $(uv, k, \lambda_1\lambda_2)$-CDF.*

In order to further improve the existence of DFs and "DF-like" combinatorial structures, including graph decompositions and combinatorial codes (see Lamken and Wilson [68] for a universal framework), plenty of work has been done in the past decades. In particular, for improving the asymptotic existence of DFs, Weil's Theorem on multiplicative character sums plays an essential role. Before stating the theorem, we need some notation which is used throughout this dissertation.

Let e be a positive integer and q be a prime power with $q \equiv 1 \pmod{e}$. Let $\mathbb{F}_q$ and $\mathbb{F}_q^*$ denote the finite field of order q and its multiplicative group, respectively. Suppose g is a primitive element in $\mathbb{F}_q$. Let $C^{(e)}$ denote the multiplicative subgroup of $\mathbb{F}_q^*$ generated by g^e. Then, $\mathcal{C}^{(e)} := \{C_0^{(e)}, C_1^{(e)}, \ldots, C_{e-1}^{(e)}\}$ forms a coset decomposition of $\mathbb{F}_q^*$, where $C_i^{(e)} := g^i C^{(e)}$ is known as a *cyclotomic coset* of index e for each $0 \leq i \leq e-1$. Moreover, let θ_e be a primitive eth root of unity of the complex field $\mathbb{C}$ and χ be the multiplicative character of $\mathbb{F}_q$ of order e defined by

$$\chi(x) = \theta_e^i \text{ for } x \in C_i^{(e)} \text{ with } 0 \leq i \leq e-1 \quad \text{and} \quad \chi(0) = 0.$$

Theorem 1.4.7 (Weil's Theorem, see also [75] Theorem 5.41)**.** *Let $f \in \mathbb{F}_q[x]$ be a polynomial that is not of the form cg^e for some $c \in \mathbb{F}_q$ and $g \in \mathbb{F}_q[x]$. Then,*

$$\left| \sum_{x \in \mathbb{F}_q} \chi(f(x)) \right| \leq (d-1)\sqrt{q},$$

where d is the number of distinct roots of f in its splitting field over $\mathbb{F}_q$.

Notably, Buratti and Pasotti [21] derived an intermediate theorem from Weil's Theorem 1.4.7, which is a quite friendly and powerful tool for combinatorial studies (also given by Chang and Ji [25] independently).

Theorem 1.4.8 (Buratti and Pasotti [21] Theorem 2.2)**.** *Let $q \equiv 1 \pmod{e}$ be a prime power. Let $\{b_1, b_2, \ldots, b_t\}$ be an arbitrary t-subset in $\mathbb{F}_q$ and let $(j_1, j_2, \ldots, j_t)$ be an arbitrary t-tuple of $\mathbb{Z}_e$. Set $X = \{x \in \mathbb{F}_q \mid x - b_i \in C_{j_i}^{(e)}$ for each $1 \leq i \leq t\}$. Then, $|X| > n$ whenever $q > Q(e,t,n)$, where*

$$Q(e,t,n) = \left(\frac{U + \sqrt{U^2 + 4e^{t-1}(t+en)}}{2} \right)^2 \quad \text{and} \quad U = \sum_{h=1}^{t} \binom{t}{h} (e-1)^h (h-1). \tag{1.6}$$

In particular, X is not empty if $q > Q(e,t) := Q(e,t,0)$.

There is a special class of difference family which can be directly constructed from cyclotomic cosets. An elementary abelian $(q,k,1)$-DF is called *radical* if its base blocks are cosets of $C^{(\frac{q-1}{k})}$ for odd k, or the union of a coset of $C^{(\frac{q-1}{k-1})}$ and $\{0\}$ for even k. The terminology seems to have been introduced first by Buratti [16], but these constructions have been extensively studied by Wilson [120] in earlier times.

Theorem 1.4.9 (Wilson [120]). *Let $q \equiv 1 \pmod{k(k-1)}$ be a prime power. Let ζ_k and ζ_{k-1} be a primitive kth and $(k-1)$th root of unity in $\mathbb{F}_q$, respectively, and let*

$$H = \begin{cases} \{\zeta_k^i - 1 \mid 1 \le i \le \frac{k-1}{2}\}, & \text{if } k \text{ is odd,} \\ \{\zeta_{k-1}^i - 1 \mid 1 \le i \le \frac{k}{2} - 1\} \cup \{1\}, & \text{if } k \text{ is even.} \end{cases}$$

If H forms a complete system of representatives of $\mathcal{C}^{(\frac{k-1}{2})}$ for odd k or $\mathcal{C}^{(\frac{k}{2})}$ for even k, then there exists a radical $(q,k,1)$-DF over $\mathbb{F}_q$.

A necessary and sufficient condition for the existence of radical $(q,k,1)$-DFs for $k = 4,5$ was established by Buratti [15], who generalized the results of Bose [10] to "perfect packing" problems (see also [17, 18]). We will give a generalization of Wilson and Buratti's results on radical DFs in Section 3.2.2.

1.5 Grid-block designs and grid-block difference families

Let V be a finite set of cardinality v, and $\mathcal{B}$ be a collection of $r \times k$ arrays with rk distinct entries in V. We call the elements of V and $\mathcal{B}$, respectively, *points* and *grid-blocks*. Two points are *collinear* in a grid-block B if they lie in the same row or in the same column of B.

Definition 1.5.1 (grid-block design). A pair $(V, \mathcal{B})$ is an $r \times k$ *grid-block design* (resp. *packing*, *covering*) on v points, or a $(v, r \times k, 1)$ grid-block design (resp. *packing*, *covering*), if any pair of distinct points of V is collinear in exactly (resp. *at most*, *at least*) one grid-block of $\mathcal{B}$.

In particular, when $v = rk$ and $r = k$ hold, $(V, \mathcal{B})$ is called a *lattice square design*. The study of lattice square designs was motivated by agricultural experiments by Yates [128] in the 1940s. Later, in 1971, Raghavarao proposed a construction of $r \times k$ grid-block designs on p^2 points when p is an odd prime, in the monograph of experimental designs [97]. Hereafter, from the aspect of combinatorics, Hwang [57] proved that an $r \times k$ grid-block design on rk points exists if and only if $r = k$ (i.e., a lattice square design) is odd, and $r - 1$ mutually orthogonal Latin squares (MOLSs) of order r exist. Moreover, Hwang [57] also proposed grid-block designs as an application to DNA library screening. Since then, Fu *et al.* [47] formally introduced the notion of *grid-block designs* with more general parameters, and discussed their further applications to life sciences as group testing models (see also [40]).

Although great progress has been made in the sequencing techniques for DNA library screening, the experimental designs and data analysis on microarrays still present a higher level of statistical challenges (cf. [81] Chapter 13). Moreover, in recent years, numerous applications of group testing designs have been investigated in the areas of coding theory and computer science. For example, the connections of group testing with superimposed codes (see [41]) and compressed sensing (see [4]) have attracted much attention.

Grid-block designs (resp. packings, coverings) can be naturally presented as graph decompositions. Let H denote a (finite, simple, and undirected) graph. A collection $\mathcal{A}$ of subgraphs of H is said to be a *decomposition* of H if each edge of H appears in exactly one subgraph in $\mathcal{A}$. Moreover, if every graph in $\mathcal{A}$ is isomorphic to a graph G, then $\mathcal{A}$ is said to be a *G-decomposition* of H. In particular, if $H = K_v$, namely, the complete graph on v vertices, the G-decomposition is also known as a *G-design* of order v. Accordingly, under the assumption that every graph in $\mathcal{A}$ is isomorphic to G, if each edge of K_v appears in at least (resp. at most) one of the graphs in $\mathcal{A}$, then $(V, \mathcal{A})$ is said to be a *G-covering* (resp. *G-packing*), where V denotes the vertex set of K_v.

Let $L_{r,k}$ denote the Cartesian product graph of the complete graphs K_r and K_k. An $r \times k$ grid-block design (resp. packing, covering) is nothing but an $L_{r,k}$-design (resp. packing, covering).

Clearly, one 2×2 grid-block design is well known as a 4-cycle system (C_4-design), which has been extensively studied (see [77] for details). Hence, we always suppose $\min\{r, k\} \geq 2$ and $\max\{r, k\} \geq 3$ when we discuss $r \times k$ grid-block designs. It is easy to obtain the necessary conditions for the existence of a $(v, r \times k, 1)$ grid-block design.

Proposition 1.5.2. If there exists a $(v, r \times k, 1)$ grid-block design, then

$$v - 1 \equiv 0 \pmod{r + k - 2} \quad \text{and} \quad v(v-1) \equiv 0 \pmod{rk(r + k - 2)}. \tag{1.7}$$

Carter [23] studied 2×3 grid-block designs as graph decompositions into $L_{2,3}$, which is considered as the only non-bipartite connected cubic graph with six vertices. As a consequence, it was proved that the necessary condition (1.7) for a $(v, 2 \times 3, 1)$ grid-block design is sufficient. Moreover, for the cases of $2 \times k$, the existence problems have been completely settled for $k \in \{4, 5, 6\}$ by Mutoh *et al.* [86] ($k = 4$), Li *et al.* [74] ($k = 5$), and Wang and Colbourn [115] ($k = 6$). We summarize their results as follows:

Theorem 1.5.3. *A $(v, 2 \times k, 1)$ grid-block design exists if and only if*

(i) $v \equiv 1 \pmod 9$ *for* $k = 3$,

(ii) $v \equiv 1 \pmod{32}$ *for* $k = 4$,

(iii) $v \equiv 1 \pmod{25}$ *for* $k = 5$,

(iv) $v \equiv 1 \pmod{72}$ *for* $k = 6$.

Zhang *et al.* [131] studied 3×4 and 4×4 grid-block designs, and proved the necessary conditions (1.7) are (almost) sufficient.

Theorem 1.5.4 (Zhang *et al.* [131])**.** *There exists a $(v, 4 \times k, 1)$ grid-block design if and only if*

(i) $v \equiv 1, 16, 21, 36 \pmod{60}$ *except* $v = 16$ *and possibly except* $v \in \{60n+36 \mid n = 1, 2, 4, 5, 10, 20, 22, 26\} \cup \{60n + 16 \mid n = 2, 3, 4, 7, 10, 18, 23\}$ *for* $k = 3$.

(ii) $v \equiv 1 \pmod{96}$ *for* $k = 4$.

For a grid-block design (resp. packing, covering), if the set of grid-blocks can be partitioned into *resolution classes*, in each of which every point occurs exactly once. We will consider the constructions of resolvable grid-blocks designs (resp. packings, coverings) in Chapter 4.

Similarly to t-designs, we are also concerned with grid-block designs admitting prescribed permutation groups as their automorphism groups. Let V be the point set. We write

$$\mathsf{B} = \begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1k} \\ b_{21} & b_{22} & \cdots & b_{2k} \\ \vdots & \vdots & & \vdots \\ b_{r1} & b_{r2} & \cdots & b_{rk} \end{bmatrix} \quad \text{with } b_{ij} \in V$$

to represent an $r \times k$ grid-block. When exchanging any two rows or two columns of B, the resulting grid-block is *equivalent* to B. Explicitly, if we regard B as a matrix, then the grid-block $\mathsf{B}' = P\mathsf{B}Q$ is said to be *equivalent* to B for any permutation matrices P and Q. For a permutation σ on V, we define $\mathsf{B}^\sigma = [b_{ij}^\sigma]_{r\times k}$. Let $(V, \mathcal{B})$ be an $r \times k$ grid-block design. If there is a grid-block equivalent to B^σ in $\mathcal{B}$ for any $\mathsf{B} \in \mathcal{B}$, then $(V, \mathcal{B})$ is said to be *invariant* under σ. Equivalently, σ is said to be an *automorphism* of $(V, \mathcal{B})$. In particular, if σ is of order $v = |V|$, then $(V, \mathcal{B})$ is *cyclic*. In this case, we identify V with $\mathbb{Z}_v$ and denote $\mathsf{B} + t = [b_{ij} + t]_{r\times k}$ for any $t \in \mathbb{Z}_v$. Under the action of $\mathbb{Z}_v$, $\mathcal{B}$ can be partitioned into orbits. An orbit is said to be *full* if its length equals v, otherwise, *short*. A cyclic grid-block design containing no short orbit is said to be *strictly cyclic*. We can arbitrarily choose a grid-block from each orbit to represent the whole orbit. Such a representative of a (cyclic) orbit is called a *(cyclic) base grid-block*.

Example 1.5.5. We list the base grid-blocks of cyclic $(v, 2 \times 3, 1)$ grid-block designs of small v proposed in [23]. The base grid-blocks marked by $\star$ give rise to short orbits.

(i) For $v = 10$, we have $\mathsf{B}_1 = \begin{bmatrix} 0 & 1 & 8 \\ 6 & 5 & 3 \end{bmatrix}^\star$ as a base grid-block.

(ii) For $v = 19$, we have $\mathsf{B}_1 = \begin{bmatrix} 0 & 2 & 9 \\ 6 & 5 & 1 \end{bmatrix}$ as a base grid-block.

(iii) For $v = 28$, we have $\mathsf{B}_1 = \begin{bmatrix} 0 & 1 & 6 \\ 15 & 17 & 26 \end{bmatrix}$ and $\mathsf{B}_2 = \begin{bmatrix} 0 & 3 & 7 \\ 14 & 21 & 17 \end{bmatrix}^\star$ as base grid-blocks.

It is difficult to construct grid-block designs when one of r and k is large. In the previous studies, most constructions are based on recursive ones. Small grid-block designs are utilized as "input designs" (or "ingredient designs") for

Table 1.1: Previously known cyclic $(v, r \times k, 1)$ grid-block designs

$r \times k$	v	References
2×3	10, 19, 28, 37, 46.	Carter [23]
	For all $v \equiv 1 \pmod{18}$.	Wannasit and El-Zanati [116]
2×4	33, 65, 97, 193, 225, 257, 289, 321, 353.	Mutoh *et al.* [86]
2×5	51, 76, 101.	Li *et al.* [74]
2×6	73, 145, 433.	Wang and Colbourn [115]
3×3	For all $v \equiv 1, 9 \pmod{36}$.	Fu *et al.* [47]
3×4	21, 61, 181, 421.	Zhang *et al.* [131]
4×4	97, 193.	Zhang *et al.* [131]

the recursions, some of which are cyclic. We list the previously known results for cyclic $(v, r \times k, 1)$ grid-block designs in Table 1.1.

Infinite families (constructions) of cyclic grid-block designs are less known. It is remarkable that the existence of cyclic 3×3 grid-block designs has been completely solved by Fu *et al.* [47] by giving an explicit solution. They dealt with the rows and columns of a 3×3 grid-block as base blocks of a cyclic Steiner triple system. By an ingenious arrangement of the triples, they successfully set up the direct constructions of all base grid-blocks.

Recently, a construction of cyclic 2×3 grid-block designs has been proposed by Wannasit and El-Zanati [116]. As a tripartite graph having a ρ-tripartite labeling, $L_{2,3}$ is proved to cyclically decompose K_v for any $v \equiv 1 \pmod{18}$. Explicitly, the base grid-blocks of a cyclic $(v, 2 \times 3, 1)$ grid-design can be expressed by

$$\mathsf{B}_i = \begin{bmatrix} 1 & 18i & -18i+8 \\ -18i+14 & 0 & 18i-15 \end{bmatrix}$$

where $i \in \{1, 2, \dots, \frac{v-1}{18}\}$ (see [116] Theorem 4 and Table 1).

Besides the above mentioned constructions, the method of differences is more commonly used. In another word, strictly cyclic grid-block designs can be constructed from array type analogues of difference families. For a given $r \times k$ grid-block, each row generates $k(k-1)$ differences and each column generates $r(r-1)$ differences, so a total of $rk(r+k-2)$ differences are derived. In this manner, Fu *et al.* [47] called the collection of base grid-blocks as *a two-dimensional difference family* for a strictly cyclic grid-block design. Meanwhile, Mutoh, Jimbo, and Fu [85] considered their applications to resolvable grid-block designs and used the terminology *"grid-block difference family"*. We will use the terminology *"grid-block difference family"* and write an *$L_{r,k}$-difference family (DF)*, or a $(v, L_{r,k}, 1)$-DF for short.

Definition 1.5.6 (grid-block difference family)**.** Let G be an additive group of order v and let $\mathcal{B}$ be a collection of $r \times k$ grid-blocks with entries in G. $\mathcal{B}$ is called an $r \times k$ *grid-block difference family* (DF) over G, or simply a $(v, L_{r,k}, 1)$-DF, if there exists exactly one pair of collinear elements in $\mathcal{B}$, say (a, b), such that $a - b = x$ for any nonzero element x in G.

It is easy to deduce the following necessary conditions for the existence of a $(v, L_{r,k}, 1)$-DF:

Proposition 1.5.7. If a $(v, L_{r,k}, 1)$-DF exists, then $v \equiv 1 \pmod{rk(r+k-2)}$.

More results on existence, construction, and characterization of $L_{r,k}$-DFs will be proposed in Chapter 3.

1.6 Outline of this dissertation

In the next three chapters, we will focus on the existence and construction of affine-invariant quadruple systems, grid-block difference families, and resolvable grid-block coverings.

In Chapter 2, we investigate the constructions of affine-invariant strictly cyclic Steiner quadruple systems (AsSQSs) and affine-invariant 2-fold quadruple systems (TQSs). For a prime $p \equiv 1 \pmod 4$, Direct Construction A establishes an AsSQS($2p$), provided that a 1-factor of a graph exists, where the graph is defined by using a system of generators of the projective special linear group PSL$(2, p)$. Direct Construction B gives an AsSQS($2p$) which is 2-chromatic, provided that a rainbow 1-factor of a specific hypergraph exists. Accordingly, by proposing two recursive constructions of an AsSQSs($2p^m$) for a positive integer m, we prove that an AsSQS($2p^m$) exists, if the criteria developed for an AsSQS($2p$) are satisfied. In a similar way, the direct construction and recursive construction for affine-invariant TQSs are also given.

Chapters 3 and 4 are devoted to considering grid-block designs with the cyclic property and resolvability. In Chapter 3, we concentrate on grid-block difference families (DFs), which can be viewed as two-dimensional generalizations of DFs. Firstly, we give an intermediate algebraic consequence on the existence bound of an element satisfying certain cyclotomic conditions in a finite field. In many cases, this approach improves the bound due to Buratti and Pasotti [21]. In particular, this approach will be applied to improving the existence bound for grid-block DFs. Secondly, by considering Kronecker density via algebraic number theory, a series of cyclotomic constructions and characterizations of row-radical grid-block DFs are presented.

In Chapter 4, a construction of resolvable grid-block designs, packings, or coverings via grid-block DFs is proposed. Moreover, the optimality of grid-block covering is discussed and the optimal construction of 2×3 grid-block covering is provided.

In Chapter 5, we give concluding remarks and some problems for future study.

Chapter 2

Affine-invariant quadruple systems

In this chapter, we focus mainly on affine-invariant SQSs and TQSs, that is, cyclic 3-$(v, 4, \lambda)$ designs with $\lambda \in \{1, 2\}$ over $\mathbb{Z}_v$ which admit every unit of $\mathbb{Z}_v$ as a multiplier. We give two direct constructions for an AsSQS($2p$), and two recursive constructions for an AsSQS($2p^m$), where $p \equiv 1, 5 \pmod{12}$ is prime and m is a positive integer.

In Section 2.1, we introduce two families of graphs, namely, "LG graphs" and "CG graphs". An LG graph is defined on a 1-dimensional projective line (which is abbreviated to the letter "L") over a finite field $\mathbb{F}_q$. A CG graph is defined on the cross-ratio classes (which is abbreviated to the letter "C") of a projective line. The adjacencies in both LG and CG graphs are established by a set of generators of the projective special linear group PSL$(2, q)$. This new perspective would provide a possible way for making use of geometric group theory or combinatorial group theory to attack the complete proof of the existence of sSQSs and AsSQSs. In Section 2.1.3, we describe the relation between our CG graphs and "Köhler orbit graphs".

In Section 2.2.1, we give a presentation of blocks (quadruples and triples) over $\mathbb{Z}_{\frac{v}{2}} \times \mathbb{Z}_2$ to simplify our constructions. Then, under the above presentation, we present two direct Constructions 2.2.6 and 2.2.20 in Sections 2.2.2 and 2.2.3, respectively, where the former requires 1-factors of CG graphs defined in Section 2.1, and the latter is related to a hypergraph which can be regarded as a pairwise balanced design (PBD). In addition, the sSQSs obtained from Construction 2.2.20 are 2-chromatic, so that a few unknown parameters of 2-chromatic SQSs can be determined.

We use Section 2.3.1 to summarize some notation and useful preliminaries for the constructions below. Two recursive constructions are presented in Sections 2.3.2 and 2.3.3, showing that an AsSQS($2p^m$) can be constructed via an AsSQS($2p$) derived from direct Constructions 2.2.6 and 2.2.20.

In Section 2.4, we prove a necessary condition for the existence of an AsSQS(v)

for $v \equiv 2, 10 \pmod{24}$, and thereby establish a non-existence result.

Furthermore, direct and recursive constructions are presented for affine-invariant TQSs in Sections 2.5 and 2.6, respectively.

It is mentioned that sSQSs are closely related to optical orthogonal codes (OOCs). In fact, combinatorial designs, in particular cyclic designs, are widely used in many other areas, for example, designs of experiments, group testing [39], authentication codes [88, 110], filing schemes [6, 126], etc. For the applications to these areas, it is desirable to generate the blocks with less storage and time. Also, for a given t-subset (for example, a pair, a triple, etc.) T of the point set V, it is usually required to find the blocks containing the certain T. The affine-invariant property works effectively for these problems. Finally, Section 2.7 is devoted to giving a brief explanation on these approaches.

Throughout this chapter, we always suppose p is a prime satisfying $p \equiv 1 \pmod 4$. Besides the standard notation, we use the symbols $\uplus$ and $\cup$ to denote the union of multisets and the disjoint union of sets, respectively.

2.1 Graphs associated with $\mathrm{PSL}(2, q)$

In this section, we define two families of graphs, namely, LG graphs and CG graphs. An LG graph can be defined on any finite set V with a group acting on it. A CG graph can be derived from a specific LG graph defined on the projective line over a finite field, and plays an essential role for our constructions for affine-invariant sSQSs and TQSs.

Hereafter, when saying a graph, we mean an undirected graph in which multiple edges and self-loops are allowed. More precisely, the edge set of a graph is considered as a multi-set, and a self-loop is represented by a singleton in the edge set. The degree of a vertex, say x, is defined as the number of edges, including multiple edges and self-loops, which contain x.

For more notion of graphs and hypergraphs, the reader is referred to the textbooks [26, 37] for details.

2.1.1 LG graphs

First, we introduce the most general definition of an LG graph and present a series of its basic properties.

Definition 2.1.1 (LG graph)**.** Let V be a finite set, and let G be a group acting on V such that $V^G \subseteq V$. Let Σ be a finite subset of G consisting of involutions. $\mathrm{LG}(V, \Sigma)$ is defined to be the graph (V, E) with edge set $E = \{\{x, x^\sigma\} \mid x \in V, \sigma \in \Sigma\}$. Multiple edges and self-loops are allowed, and thus E is treated as a multiset.

Proposition 2.1.2. With the notation in Definition 2.1.1, the following hold:

(i) If Σ consists of involutions in G and $\Sigma' \subset \Sigma$, then $\mathrm{LG}(V, \Sigma')$ is an edge-induced subgraph of $\mathrm{LG}(V, \Sigma)$.

(ii) $\mathrm{LG}(V, \Sigma)$ has a self-loop at vertex $x \in V$ if and only if x is a fixed point of some $\sigma \in \Sigma$.

(iii) Suppose $|\Sigma| \geq 2$. $\mathrm{LG}(V, \Sigma)$ has multiple edges $\{x, y\} \in E$ only if both x and y are fixed points of $\sigma_1\sigma_2$ for distinct $\sigma_1, \sigma_2 \in \Sigma$, where the group G is written multiplicatively.

(iv) Every vertex of $\mathrm{LG}(V, \Sigma)$ is of degree $|\Sigma|$.

(v) $\mathrm{LG}(V, \Sigma)$ consists of r vertex-disjoint subgraphs, each of which has a vertex set identical with an orbit of V under the action of $\langle\Sigma\rangle$, where r is the number of orbits.

(vi) If G acts transitively on V and Σ is a generating set of G, then $\mathrm{LG}(V, \Sigma)$ is connected.

Proof. (i) and (ii) follow straightforwardly from Definition 2.1.1.

(iii) By Definition 2.1.1, $\{x, y\} \in E$ if and only if $y = x^\sigma$ for some $\sigma \in \Sigma$. Suppose $\{x, y\}$ appears more than once in E. In another word, there exist $\sigma_1, \sigma_2 \in \Sigma$, such that $x^{\sigma_1} = x^{\sigma_2} = y$. Since σ_1 and σ_2 are involutions, we also have $y^{\sigma_1} = y^{\sigma_2} = x$. This implies both x and y are fixed points of $\sigma_1\sigma_2$.

(iv) In fact, any edge of $\mathrm{LG}(V, \Sigma)$ is an orbit of V under the action of some $\sigma \in \Sigma$. Hence, for any $\sigma \in \Sigma$, each vertex has degree 1 in the subgraph $\mathrm{LG}(V, \{\sigma\})$ (cf. (i)). When multiple edges and self-loops are counted (cf. (ii) and (iii)), it is clear that each vertex of $\mathrm{LG}(V, \Sigma)$ has degree $|\Sigma|$.

(v) Let $V_1, V_2, \ldots, V_r$ denote the orbits of V under the action of $\langle\Sigma\rangle$. Then, $\mathrm{LG}(V_i, \Sigma)$ is obviously a vertex-induced subgraph of $\mathrm{LG}(V, \Sigma)$ for each $1 \leq i \leq r$. Let E_i denote the edge set of $\mathrm{LG}(V_i, \Sigma)$. Note that x and x^σ always lie in the same orbit under the action of $\langle\Sigma\rangle$ for any $x \in V$ and $\sigma \in \Sigma$. Thus, we have $E = \{\{x, x^\sigma\} \mid x \in \dot{\bigcup}_{i=1}^r V_i, \sigma \in \Sigma\} = \dot{\bigcup}_{i=1}^r \{\{x, x^\sigma\} \mid x \in V_i, \sigma \in \Sigma\} = \dot{\bigcup}_{i=1}^r E_i$.

(vi) Every $\tau \in G$ can be represented by a sequence of generators in Σ, say $\tau = \sigma_\ell \sigma_{\ell-1} \cdots \sigma_1$, where $\sigma_i \in \Sigma$ for $1 \leq i \leq \ell$. In terms of graphs, there exists a walk from u to u^τ of length ℓ for any vertex u of $\mathrm{LG}(V, \Sigma)$. Conversely, by the transitivity of G, for any $u, v \in V$, there must exist $\tau \in G$, such that $v = u^\tau$. In other words, there exists a walk from u to v for any distinct vertices u, v. Therefore, $\mathrm{LG}(V, \Sigma)$ is connected.

$\square$

Let $\mathbf{P}^1(\mathbb{F}_q)$ denote the *projective line* over $\mathbb{F}_q$ which can be identified with the line $\mathbb{F}_q$ extended by a point at infinity, namely, $\mathbb{F}_q \cup \{\infty\}$. Let

$$\sigma : x \mapsto \frac{ax + b}{cx + d}$$

be a *fractional linear transformation* on $\mathbf{P}^1(\mathbb{F}_q)$ with $a, b, c, d \in \mathbb{F}_q$ and $ad-bc = 1$. Then all such transformations form a group under composition which is known as the *projective special linear group* of degree 2, and is denoted by $\mathrm{PSL}(2, q)$, where $\sigma(\infty) = \frac{a}{c}$, $\sigma(-\frac{d}{c}) = \infty$ if $c \neq 0$, and $\sigma(\infty) = \infty$ if $c = 0$.

In particular, take

$$\sigma_{\boldsymbol{A}} : x \mapsto 1 - x, \quad \sigma_{\boldsymbol{B}} : x \mapsto \frac{1}{x}, \quad \text{and} \quad \sigma_{\boldsymbol{C}} : x \mapsto \frac{1-x}{1-2x}. \tag{2.1}$$

It is easy to see that $\sigma_{\boldsymbol{A}}$, $\sigma_{\boldsymbol{B}}$, and $\sigma_{\boldsymbol{C}}$ are involutions. Now we begin to consider the graph $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_q), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$.

Example 2.1.3. The graphs $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$ for $p = 13$ and $p = 29$ are shown in Figures 2.1 and 2.2, respectively, where the edges labeled by $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{C}$ are contained in $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_{\boldsymbol{A}}\})$, $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_{\boldsymbol{B}}\})$, and $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_{\boldsymbol{C}}\})$, respectively.

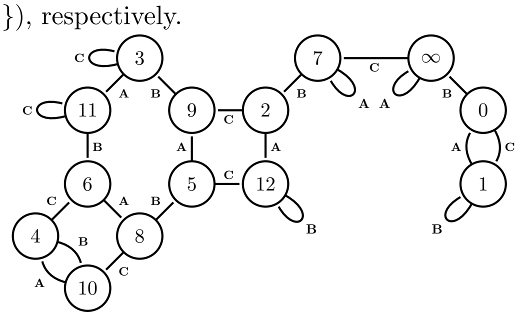

Figure 2.1: The graph $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_{13}), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$

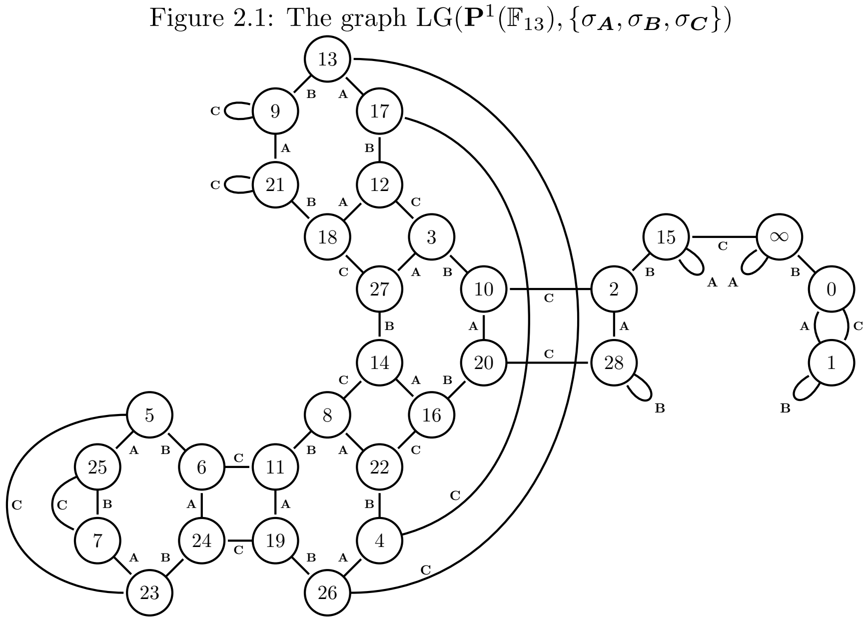

Figure 2.2: The graph $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_{29}), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$

Example 2.1.4. The graph $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_q), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$ for $q = 25$ is shown in Figures 2.3, where $\mathbb{F}_{25}$ is considered as $\mathbb{F}_5[\alpha]/(\alpha^2 + 2)$, and the edges labeled by $\boldsymbol{A}$, $\boldsymbol{B}$, and $\boldsymbol{C}$ are contained in $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_q), \{\sigma_{\boldsymbol{A}}\})$, $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_q), \{\sigma_{\boldsymbol{B}}\})$, and $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_q), \{\sigma_{\boldsymbol{C}}\})$, respectively. This graph consists of two connected components, one of which is $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_5), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$.

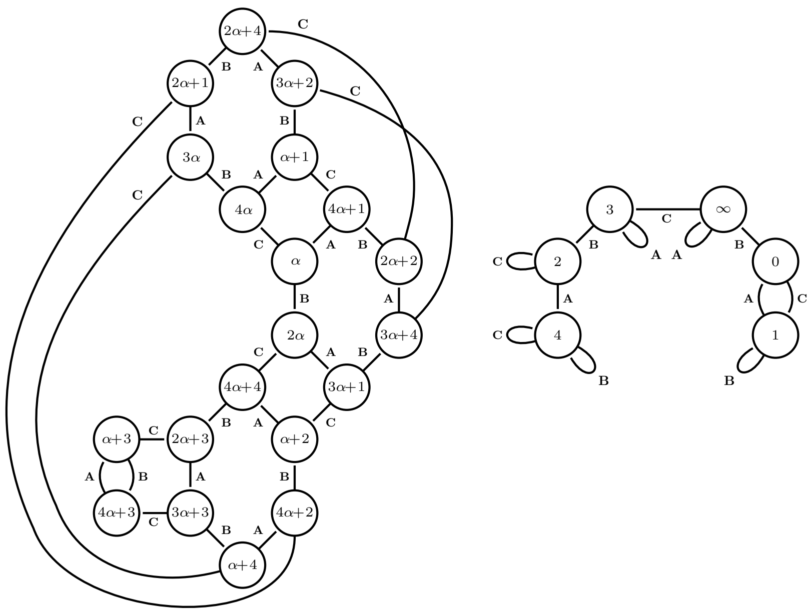

Figure 2.3: The graph $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_{25}), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$

Lemma 2.1.5. *Let $p \equiv 1 \pmod 4$ be a prime. Then $\{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\}$ is a generating set of $\mathrm{PSL}(2, p)$, where $\sigma_{\boldsymbol{A}}$, $\sigma_{\boldsymbol{B}}$, and $\sigma_{\boldsymbol{C}}$ follow the definitions in* (2.1).

Proof. The group $\mathrm{PSL}(2, p)$ can also be interpreted as a matrix group, namely,

$$\mathrm{PSL}(2, p) = \left\{ M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| \, a, b, c, d \in \mathbb{F}_p, \det M = 1 \right\}.$$

For any $\delta \in \mathbb{F}_p^*$, since $\frac{ax+b}{cx+d} = \frac{\delta ax + \delta b}{\delta cx + \delta d}$, we identify δM with M when $M \in \mathrm{PSL}(2, p)$ is considered as a matrix. In this proof, we use the matrix representation. Then $\sigma_{\boldsymbol{A}}$, $\sigma_{\boldsymbol{B}}$, and $\sigma_{\boldsymbol{C}}$ correspond to three matrices over $\mathbb{F}_p$ respectively, namely,

$$\boldsymbol{A} = \begin{pmatrix} -1 & 1 \\ 0 & 1 \end{pmatrix}, \quad \boldsymbol{B} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \text{and} \quad \boldsymbol{C} = \begin{pmatrix} 1 & -1 \\ 2 & -1 \end{pmatrix}.$$

Note that -1 is a square in $\mathbb{F}_p$ if and only if $p \equiv 1 \pmod 4$. Since $\det \boldsymbol{A} = \det \boldsymbol{B} = -1$ and $\det \boldsymbol{C} = 1$, by identifying $\boldsymbol{A}$ (resp. $\boldsymbol{B}$) with $\sqrt{-1}\boldsymbol{A}$ (resp. $\sqrt{-1}\boldsymbol{B}$), we have $\boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \in \mathrm{PSL}(2, p)$. To complete the proof, we employ a theorem due to Behr and Mennicke [5] (see also Coxeter and Moser [36] § 7.5) who showed that, for odd prime p, $\mathrm{PSL}(2,p)$ can be represented by the system of generators and relations

$$\boldsymbol{S}^p = \boldsymbol{T}^2 = (\boldsymbol{ST})^3 = (\boldsymbol{S}^2\boldsymbol{T}\boldsymbol{S}^{\frac{1}{2}(p+1)}\boldsymbol{T})^3 = \boldsymbol{I}, \tag{2.2}$$

where $\boldsymbol{I}$ is the identity matrix. Let $\boldsymbol{S} = \boldsymbol{CBA} = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ and $\boldsymbol{T} = \boldsymbol{ABCBA} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. Since $\langle \boldsymbol{S}, \boldsymbol{T} \rangle \leq \langle \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \rangle \leq \mathrm{PSL}(2,p)$, it remains to show that $\boldsymbol{S}, \boldsymbol{T}$ satisfy (2.2). It is easy to see $\boldsymbol{T}^2 = -\boldsymbol{I}$, $\boldsymbol{S}^p \equiv \boldsymbol{I} \pmod p$, and $(\boldsymbol{S}^2\boldsymbol{T}\boldsymbol{S}^{\frac{1}{2}(p+1)}\boldsymbol{T})^3 \equiv \boldsymbol{I} \pmod p$, where $\boldsymbol{I}$ and $-\boldsymbol{I}$ are identical in $\mathrm{PSL}(2,p)$. Thus $\langle \boldsymbol{S}, \boldsymbol{T} \rangle = \mathrm{PSL}(2,p)$ which implies $\langle \boldsymbol{A}, \boldsymbol{B}, \boldsymbol{C} \rangle = \mathrm{PSL}(2,p)$. □

In order to examine the special vertices of $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_q), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$, we need the following lemma:

Lemma 2.1.6. *Let q be an odd prime power. Then,*

(i) There exists $\chi \in \mathbb{F}_q$ such that $\chi^{\sigma_{\boldsymbol{C}}} = \chi$ if and only if $q \equiv 1 \pmod 4$.

(ii) There exists $\mu \in \mathbb{F}_q$ such that $\mu^{\sigma_{\boldsymbol{C}}} = \mu^{\sigma_{\boldsymbol{B}}}$ if and only if $q \equiv \pm 1 \pmod 5$.

(iii) There exists $\xi \in \mathbb{F}_q$ such that $\xi^{\sigma_{\boldsymbol{A}}} = \xi^{\sigma_{\boldsymbol{B}}}$ if and only if $q \equiv 1 \pmod 3$.

Proof. This is equivalent to studying the roots of the equations

$$2\chi^2 - 2\chi + 1 = 0, \quad \mu^2 - 3\mu + 1 = 0, \quad \text{and} \quad \xi^2 - \xi + 1 = 0, \tag{2.3}$$

which can be formally written by

$$\chi = \frac{1+\sqrt{-1}}{2}, \quad \mu = \frac{3+\sqrt{5}}{2}, \quad \text{and} \quad \xi = \frac{1+\sqrt{-3}}{2}. \tag{2.4}$$

These expressions respectively require -1, 5, and -3 to be squares in $\mathbb{F}_q$. If $q = p$ is a prime, it can be obtained by using the law of quadratic reciprocity that -1 (resp., 5 or -3) is a square modulo p if and only if $p \equiv 1 \pmod 4$ (resp., $p \equiv \pm 1 \pmod 5$ or $p \equiv 1 \pmod 3$). In the extension field $\mathbb{F}_q$ with $q = p^n$, $n \geq 1$, if $p \equiv 1 \pmod 4$, then -1 is known to be a square in the subfield $\mathbb{F}_p \subset \mathbb{F}_q$. On the other hand, if $p \equiv 3 \pmod 4$, then the polynomial $x^2 + 1$ is irreducible over $\mathbb{F}_p$, and its splitting field is nothing but $\mathbb{F}_{p^2}$. Hence, -1 is a square in $\mathbb{F}_{p^2}$ when $p \equiv -1 \pmod 4$. In summary, -1 is a square in $\mathbb{F}_{p^n}$ with p odd, if and only if $p \equiv 1 \pmod 4$ or n is even, that is, $p^n \equiv 1 \pmod 4$. In the same manner, it can be shown that 5 and -3 are squares in $\mathbb{F}_q$ if and only if $q \equiv \pm 1 \pmod 5$ and $q \equiv 1 \pmod 3$, respectively. □

As a direct consequence of Proposition 2.1.2, we summarize the properties of $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$ as follows:

Proposition 2.1.7. The following properties of $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$ hold for $p \equiv 1 \pmod 4$.

(i) There is a self-loop at vertex $x \in V$ if and only if $x \in \{2^{-1}, \infty\} \cup \{1, -1\} \cup \{\chi, 1-\chi\}$, where $\chi = \frac{1+\sqrt{-1}}{2}$ is a root of $2\chi^2 - 2\chi + 1 = 0$.

(ii) There are double edges $\{0, 1\}$. If $p \equiv 1 \pmod 3$, there are double edges $\{\xi, 1-\xi\}$, where $\xi = \frac{1+\sqrt{-3}}{2}$ is a root of $\xi^2 - \xi + 1 = 0$. If $p \equiv \pm 1 \pmod 5$, there are double edges $\{\mu, \mu^{-1}\}$, where $\mu = \frac{3+\sqrt{5}}{2}$ is a root of $\mu^2 - 3\mu + 1 = 0$.

(iii) Every vertex is of degree 3.

(iv) $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$ is connected.

Proof. (i) and (ii) follow from Proposition 2.1.2 (ii) and (iii) by noting that the fixed points of $\sigma_{\boldsymbol{A}}$, $\sigma_{\boldsymbol{B}}$, $\sigma_{\boldsymbol{C}}$, $\sigma_{\boldsymbol{A}}\sigma_{\boldsymbol{C}}$, $\sigma_{\boldsymbol{A}}\sigma_{\boldsymbol{B}}$, and $\sigma_{\boldsymbol{B}}\sigma_{\boldsymbol{C}}$ are $\{2^{-1}, \infty\}$, $\{1, -1\}$, $\{\chi, 1-\chi\}$, $\{0, 1\}$, $\{\xi, 1-\xi\}$, and $\{\mu, \mu^{-1}\}$, respectively, where the existence criteria for χ, μ, and ξ agree with Lemma 2.1.6.

(iii) is a direct conclusion of Proposition 2.1.2 (iv). Lemma 2.1.5 indicates that $\{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\}$ is a generating set of $\mathrm{PSL}(2, p)$. Moreover, $\mathrm{PSL}(2, p)$ is well-known to be transitive. Thus, $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}}, \sigma_{\boldsymbol{C}}\})$ is connected by Proposition 2.1.2 (vi). $\square$

2.1.2 CG graphs

Let $x \in \mathbf{P}^1(\mathbb{F}_q)$ and let $C(x)$ denote the orbit of x under the action of the subgroups $\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}} \rangle$, i.e.,

$$C(x) = \{x^\sigma \mid \sigma \in \langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}} \rangle\} = \left\{ x, \frac{1}{x}, \frac{x-1}{x}, \frac{x}{x-1}, \frac{1}{1-x}, 1-x \right\}. \tag{2.5}$$

In projective geometry, $C(x)$ is also known as the *cross-ratio class* with respect to x. Since $C(x)$ is essentially a $\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{B}} \rangle$-orbit of $x \in \mathbf{P}^1(\mathbb{F}_q)$, we have

$$|C(x)| = \begin{cases} 2 & \text{if } x \in \{\xi, 1-\xi\}, \\ 3 & \text{if } x \in \{0, 1, \infty\} \cup \{-1, 2, 2^{-1}\}, \\ 6 & \text{otherwise.} \end{cases} \tag{2.6}$$

For $p \equiv 5 \pmod{12}$, $\mathbf{P}^1(\mathbb{F}_q)$ can be partitioned into $\{0, 1, \infty\}$, $\{-1, 2, 2^{-1}\}$, and other $\frac{q-5}{6}$ cross-ratio classes of size 6. For $p \equiv 1 \pmod{12}$, $\mathbf{P}^1(\mathbb{F}_q)$ can be partitioned into $\{0, 1, \infty\}$, $\{-1, 2, 2^{-1}\}$, $\{\xi, 1-\xi\}$, and other $\frac{q-7}{6}$ cross-ratio classes of size 6, where $\xi = \frac{1+\sqrt{-3}}{2}$ is a root of $\xi^2 - \xi + 1 = 0$.

We remove the cross-ratio classes of odd sizes and let

$$\Omega_q = \mathbb{F}_q \setminus \{0, 1, -1, 2, 2^{-1}\}. \tag{2.7}$$

We need a lemma to ensure Definition 2.1.9 is well-defined.

Lemma 2.1.8. *For any $x \in \Omega_q$, let $R(x) = \big\{\{u, v\} \mid v = u^{\sigma_C}, u \in C(x), v \in C(x^{\sigma_C})\big\}$. Then the cardinality of $R(x)$ is either 2 or 4. In particular, if $C(x) = C(x^{\sigma_C})$, then $|R(x)| = 2$ and $x \in \{\mu, \mu^{-1}, 1-\mu, 1-\mu^{-1}, \chi, 1-\chi\}$, where $\mu = \frac{3+\sqrt{5}}{2}$ is a root of $\mu^2 - 3\mu + 1 = 0$, and $\chi = \frac{1+\sqrt{-1}}{2}$ is a root of $2\chi^2 - 2\chi + 1 = 0$.*

Proof. It is clear that $\{x, x^{\sigma_C}\} \in R(x)$. Moreover, we have $\{1-x, 1-x^{\sigma_C}\} \in R(x)$. Hence, $|R(x)|$ is even unless $\{x, x^{\sigma_C}\} = 1 - \{x, x^{\sigma_C}\}$, which implies $x \in \{0, 1, 2^{-1}\}$. Therefore, $|R(x)| \geq 2$ is even for any $x \in \Omega_q$.

If $C(x)$ coincides with $C(x^{\sigma_C})$, then there must exist $\tau \in \langle \sigma_A, \sigma_B \rangle$ such that $x^\tau = x^{\sigma_C}$, which implies $x \in \{\mu, \mu^{-1}, 1-\mu, 1-\mu^{-1}, 0, 1, \chi, 1-\chi\}$. Note that x is in Ω_q which does not contain $\{0, 1\}$. Thus, for any $x \in \{\mu, \mu^{-1}, 1-\mu, 1-\mu^{-1}\}$, $R(x) = \big\{\{\mu, \mu^{-1}\}, \{1-\mu, 1-\mu^{-1}\}\big\}$. For any $x \in \{\chi, 1-\chi\}$, $R(x) = \big\{\{\chi\}, \{1-\chi\}\big\}$. In both cases, we have $|R(x)| = 2$.

Then, suppose $C(x)$ is disjoint from $C(x^{\sigma_C})$ and $R(x) \geq 4$. It should satisfy $(x^{\sigma_B})^{\sigma_C} = (x^{\sigma_C})^\tau$ or $((1-x)^{\sigma_B})^{\sigma_C} = (x^{\sigma_C})^\tau$ for some $\tau \in \langle \sigma_A, \sigma_B \rangle$. For $x \in \Omega_q$, this criterion is satisfied only if $x \in C(\frac{1}{\sqrt{2}}) \cup C(-\frac{1}{\sqrt{2}})$ when $q \equiv \pm 1 \pmod 8$. In this case, we have $|R(x)| = 4$. □

Definition 2.1.9 (CG graph)**.** Let X be a subset of Ω_q. Let $V = \{C(x) \mid x \in X\}$ and let E be a multiset of subsets of V consisting of

$$\{C(x), C(x^{\sigma_C})\} \text{ for any } x \in X$$

with multiplicity $\frac{1}{2}\#\big\{\{u, v\} \mid v = u^{\sigma_C}, u \in C(x), v \in C(x^{\sigma_C})\big\}$. Then (V, E) is an incidence structure which can be seen as a graph with multiple edges and self-loops, and is denoted by $\mathrm{CG}(X)$.

In particular, using $\mathrm{LG}(\Omega_q, \{\sigma_A, \sigma_B, \sigma_C\})$, we have an equivalent definition of $\mathrm{CG}(\Omega_q)$. First, contract each component (corresponding to a cross-ratio class) of $\mathrm{LG}(\Omega_q, \{\sigma_A, \sigma_B\})$ into a single vertex. Then, contract each pair of edges in $\mathrm{LG}(\Omega_q, \{\sigma_C\})$ into a single edge if they are contained in the same component of $\mathrm{LG}(\Omega_q, \{\sigma_A, \sigma_C\})$. The resulting graph is $\mathrm{CG}(\Omega_q)$.

When $p \equiv 1 \pmod 4$, the connectivity of $\mathrm{CG}(\Omega_p)$ can be easily derived from the connectivity of the vertex-induced subgraph of $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_A, \sigma_B, \sigma_C\})$ on Ω_p, where $\mathrm{LG}(\mathbf{P}^1(\mathbb{F}_p), \{\sigma_A, \sigma_B, \sigma_C\})$ is connected by Proposition 2.1.7 (iv).

Since $\Omega_p = \emptyset$ when $p = 5$, we assume $p > 5$ for the following discussion of $\mathrm{CG}(\Omega_p)$.

Proposition 2.1.10. For prime $p \equiv 1 \pmod 4$ and $p > 5$, the following properties on $\mathrm{CG}(\Omega_p)$ hold:

(i) There is a self-loop at vertex C if and only if $C = C(\chi)$ or $C = C(\mu)$, where $\chi = \frac{1+\sqrt{-1}}{2}$ is a root of $2\chi^2 - 2\chi + 1 = 0$, and $\mu = \frac{3+\sqrt{5}}{2}$ is a root of $\mu^2 - 3\mu + 1 = 0$ which requires $p \equiv 1, 29, 41, 49 \pmod{60}$.

(ii) Every vertex has degree 3 except $C(3)$, $C(\mu)$, and $C(\xi)$, where $C(3)$ and $C(\mu)$ are of degree 2, and $C(\xi)$ is of degree 1, where where $\xi = \frac{1+\sqrt{-3}}{2}$ is a root of $\xi^2 - \xi + 1 = 0$;

Table 2.1: Special vertices of $\mathrm{CG}(\Omega_p)$ for $p \equiv 1 \pmod 4$

	$C(3)$	$C(\chi)$	$C(\mu)$	$C(\xi)$
$p \equiv 29, 41 \pmod{60}$	✓	✓	✓	
$p \equiv 17, 53 \pmod{60}$	✓	✓		
$p \equiv 1, 49 \pmod{60}$	✓	✓	✓	✓
$p \equiv 13, 37 \pmod{60}$	✓	✓		✓
Degree	2	3	2	1
Incident with a self-loop		✓	✓	
Remarks (cf. Lemma 2.1.6)	$3^{\sigma_B} = 2^{\sigma_C}$	$\chi^{\sigma_C} = \chi$	$\mu^{\sigma_C} = \mu^{\sigma_B}$	$\xi^{\sigma_A} = \xi^{\sigma_B}$

Proof. (i) $\{C(x)\}$ forms a self-loop if and only if there exists $u \in C(x)$, such that $u^{\sigma_C} \in C(x)$, which implies $C(x) = C(\chi)$ or $C(\mu)$ by Lemma 2.1.8. In addition, 5 is a square modulo p if and only if $p \equiv \pm 1 \pmod 5$. Combined with $p \equiv 1, 5 \pmod{12}$, we have $p \equiv 1, 29, 41, 49 \pmod{60}$.

(ii) Let $\deg C(x)$ denote the degree of $C(x)$ in $\mathrm{CG}(\Omega_q)$. It is easy to see that $\deg C(\mu) = 2$, and $\deg C(\chi) = 3$ except when $q = 13$, in which case $C(\chi) = C(3)$ is of degree 2. Now we suppose $C(x)$ is not incident with a self-loop. By Definition 2.1.9 of $\mathrm{CG}(\Omega_q)$, we have

$$\begin{aligned}\deg C(x) &= \tfrac{1}{2}\#\big\{C(u^{\sigma_C}) \text{ is a vertex other than } C(x) \mid u \in C(x)\big\} \\ &= \tfrac{1}{2}\,|C(x)| - \tfrac{1}{2}\#\{u^{\sigma_C} \notin \Omega_q \mid u \in C(x)\}. \end{aligned} \tag{2.8}$$

For any $x \in \Omega_q$, $x^{\sigma_C} \notin \Omega_q$ if and only if $x \in \{3^{-1}, 1 - 3^{-1}\} \subset C(3)$. Hence, it follows from (2.6) and (2.8) that $\deg C(3) = 2$, $\deg C(\xi) = 1$, and $\deg C(x) = 3$ for any other $C(x)$ without a self-loop.

□

We summarize the degrees of $\mathrm{CG}(\Omega_p)$ in Table 2.1. For showing the existence of 1-factors of $\mathrm{CG}(\Omega_p)$, we need the following theorem, which can be seen as a stronger version of the famous Petersen's theorem [90] in graph theory:

Theorem 2.1.11 (Plesník [94], see also [130] Theorem 1.44, [1] Theorem 2.39)**.** *Any 2-edge-connected 3-regular graph (multigraphs without self-loops) has a 1-factor excluding any pair of edges.*

Theorem 2.1.12. *For $p \equiv 1, 5 \pmod{12}$ and $p \not\equiv 1, 49 \pmod{60}$, $\mathrm{CG}(\Omega_p)$ has a 1-factor if there is no bridge except its pendant edges.*

Proof. Removing the self-loops and adding some auxiliary edges in $\mathrm{CG}(\Omega_p)$, we can obtain a 3-regular graph as follows:

(a) If $p \equiv 29, 41 \pmod{60}$, we add auxiliary edges $\{C(3), C(\mu)\}$ and $\{C(\chi), C(\mu)\}$.

(b) If $p \equiv 5 \pmod{12}$ and $p \not\equiv 29, 41 \pmod{60}$, we add an auxiliary edge $\{C(3), C(\chi)\}$.

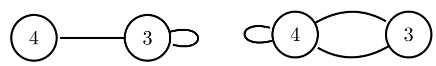

Figure 2.4: $\mathrm{CG}(\Omega_{13})$ and $\mathrm{CG}(\Omega_{17})$

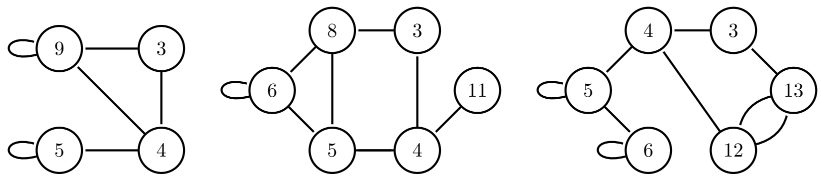

Figure 2.5: $\mathrm{CG}(\Omega_{29})$, $\mathrm{CG}(\Omega_{37})$, and $\mathrm{CG}(\Omega_{41})$

(c) If $p \equiv 1 \pmod{12}$ and $p \not\equiv 1, 49 \pmod{60}$, we add auxiliary edges $\{C(3), C(\xi)\}$ and $\{C(\chi), C(\xi)\}$.

We denote the resulting graph by $\mathrm{CG}^{\dagger}(\Omega_p)$. Since there are no more than two auxiliary edges for all these cases, by Theorem 2.1.11, if $\mathrm{CG}^{\dagger}(\Omega_p)$ is bridgeless (2-edge-connected), there must exist a 1-factor excluding all auxiliary edges, which is a 1-factor of $\mathrm{CG}(\Omega_p)$ as well. $\square$

The following results are verified by computers:

Lemma 2.1.13. $\mathrm{CG}(\Omega_p)$ *has a 1-factor for all primes* $p < 10^5$ *with* $p \equiv 1 \pmod{4}$.

Example 2.1.14. The graphs $\mathrm{CG}(\Omega_p)$ for all primes $p < 100$ with $p \equiv 1, 5 \pmod{12}$ are illustrated in Figures 2.4–2.9, where the number x at each vertex stands for $C(x)$, namely the cross-ratio class with respect to x.

Remark. For every prime $p \equiv 1 \pmod{4}$ less than 10^5 and $p \neq 41$, $\mathrm{CG}(\Omega_p)$ has no bridge except its pendant edges. $\mathrm{CG}(\Omega_{41})$ has a bridge $\{C(\chi), C(\mu)\}$. However, $\mathrm{CG}(\Omega_{41})$ has 1-factors.

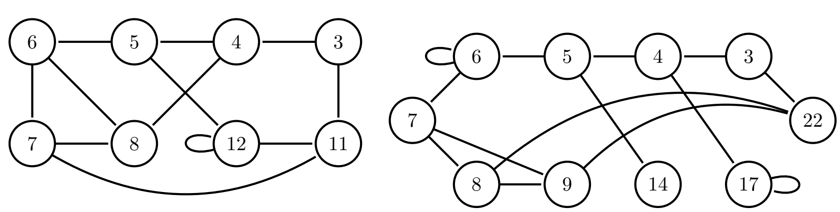

Figure 2.6: $\mathrm{CG}(\Omega_{53})$ and $\mathrm{CG}(\Omega_{61})$

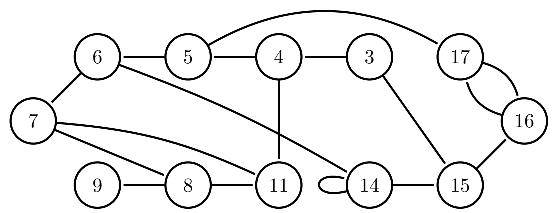

Figure 2.7: CG(Ω_{73})

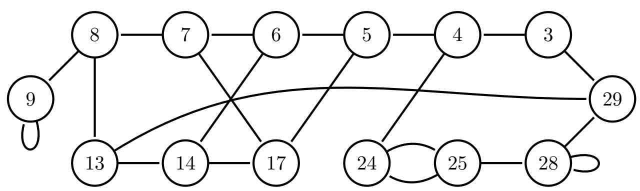

Figure 2.8: CG(Ω_{89})

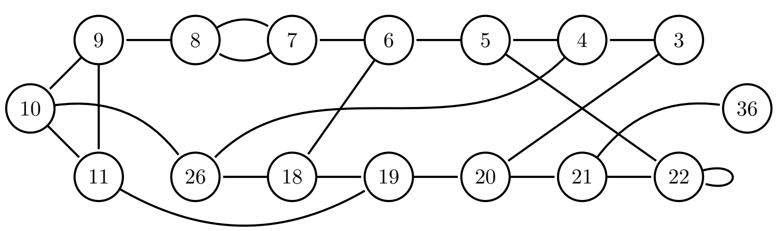

Figure 2.9: CG(Ω_{97})

2.1.3 Further remarks on CG graphs

In the original work of Köhler [65], he defined

$$K(x) = \left\{ x, -1-x, -\frac{1}{1+x}, -\frac{x}{1+x}, -1-\frac{1}{x}, \frac{1}{x} \right\} \tag{2.9}$$

as a vertex of "Köhler orbit graphs". By using the notation of $K(x)$, we could denote three mappings over $\mathbb{F}_p \cup \{\infty\}$ (cf. (2.1)):

$$\tau_{\boldsymbol{A}} : x \mapsto -1-x,\ \tau_{\boldsymbol{B}} : x \mapsto \frac{1}{x}, \text{ and } \tau_{\boldsymbol{C}} : x \mapsto \frac{-x-1}{2x+1}. \tag{2.10}$$

Then, one can observe that $K(x) = \{x^\tau \mid \tau \in \langle \tau_{\boldsymbol{A}}, \tau_{\boldsymbol{B}} \rangle\}$. In particular, $K(0) = \{0, -1, \infty\}$, and $K(1) = \{1, -2, -2^{-1}\}$. It is easily seen that

$$K(x) = -C(-x) = -\left\{ -x, 1+x, \frac{1}{1+x}, \frac{x}{1+x}, 1+\frac{1}{x}, -\frac{1}{x} \right\}.$$

By using $x \mapsto -x \pmod p$ $(\infty \mapsto \infty)$ as the isomorphism, we can see that CG graphs and "Köhler orbit graphs" are isomorphic. Accordingly, the results obtained from Siemon's number theoretic conjecture (see [106, 108]) are also applicable to CG graphs.

Actually, it is beneficial to use $C(x)$ (cross-ratio classes) instead of $K(x)$ in our study. Especially, the complicated recursive Construction 2.3.10 for $p \equiv 1 \pmod{12}$ could be more reader-friendly. This is why we "redefine" those graphs to make the present work self-contained.

Remark. There is a slight difference between those two kinds of graphs. For $p \equiv 5 \pmod{12}$, Siemon [105] forbade the multiple edges, and classified the "Köhler orbit graphs" into four classes according to the congruence criteria of p. In contrast, LG and CG graphs allow the multiple edges, so the cases are fewer (cf. Proposition 2.1.10). Actually, the multiple edges have no effect on the constructions.

It should be pointed out that the adjacency of "Köhler orbit graphs" relies on the notion of "difference cycles", which are not purely algebraic. Even though the two families of graphs are isomorphic, the definition of $\sigma_{\boldsymbol{C}}$ used for adjacencies of our CG graphs (which does not have an analogue in "Köhler orbit graphs") plays an important role in our construction below, particularly in the case when $p \equiv 1 \pmod{12}$.

So far, no efficient way is known for proving the existence of 1-factor of $\mathrm{CG}(\Omega_p)$ theoretically. The proof may need to use deep mathematics in group theory and/or analytic number theory. Hence, we use computers to verify that the auxiliary graph $\mathrm{CG}^\dagger(\Omega_p)$ is 2-connected for all prime $p < 10^5$ with $p \equiv 1 \pmod 4$.

Theorem 2.1.15. *There exists an AsSQS$(2p)$ for all prime $p < 10^5$ with $p \equiv 1 \pmod 4$.*

2.2 Affine-invariant strictly cyclic Steiner quadruple systems over $\mathbb{Z}_{2p}$

In this section, we begin to consider an affine-invariant sSQS (strictly cyclic Steiner quadruple system) of order v, provided that $v \equiv 2, 10 \pmod{24}$.

Before proceeding further, we introduce some frequently used notation in this section. Let $x \in \mathscr{P}(\mathbb{F}_p)$. Firstly, we recall (2.5) that

$$C(x) = \left\{ x, \frac{1}{x}, \frac{x-1}{x}, \frac{x}{x-1}, \frac{1}{1-x}, 1-x \right\}$$

is the cross-ratio class with respect to x. Secondly, let $\mathrm{orb}_{\boldsymbol{AC}}(x)$ denote the orbit of x under the action of the subgroups $\langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{C}} \rangle$, i.e.,

$$\mathrm{orb}_{\boldsymbol{AC}}(x) = \{x^{\sigma} \mid \sigma \in \langle \sigma_{\boldsymbol{A}}, \sigma_{\boldsymbol{C}} \rangle\} = \left\{ x, 1-x, \frac{x}{2x-1}, \frac{x-1}{2x-1} \right\}. \tag{2.11}$$

Lastly, we simply denote

$$\bar{x} = x^{\sigma_{\boldsymbol{C}}} = \frac{1-x}{1-2x} \quad \text{and} \quad \overline{C}(x) = C(x) \cup C(\bar{x}).$$

2.2.1 Block presentations

Let v be a positive integer with $v \equiv 2, 10 \pmod{24}$, which is the necessary condition for the existence of an sSQS(v) (see Proposition 1.3.1). Let $n = \frac{v}{2}$, then $n \equiv 1, 5 \pmod{12}$ is odd. Since

$$\mathbb{Z}_{2n} \cong \mathbb{Z}_n \times \mathbb{Z}_2 = \{(x, y) \mid x \in \mathbb{Z}_n, y \in \mathbb{Z}_2\},$$

we can identify the point set $\mathbb{Z}_v = \mathbb{Z}_{2n}$ with $\mathbb{Z}_n \times \mathbb{Z}_2$, and denote the point (x, y) by x_y for convenience. Addition and multiplication over $\mathbb{Z}_n \times \mathbb{Z}_2$ are defined as $x_y + x'_{y'} = (x + x')_{(y+y')}$ and $x_y x'_{y'} = (xx')_{(yy')}$, where $x + x'$, xx' are reduced modulo n, and $y + y'$, yy' are reduced modulo 2.

For an sSQS $(\mathbb{Z}_n \times \mathbb{Z}_2, \mathcal{B})$, let $B_1 = \{a_0, b_0, c_1, d_1\}$, $B_2 = \{a_0, b_0, c_0, d_1\}$, and $B_3 = \{a_0, b_0, c_0, d_0\}$ be blocks in $\mathcal{B}$. By the cyclic property, $B_1 + 0_1 = \{a_1, b_1, c_0, d_0\}$, $B_2 + 0_1 = \{a_1, b_1, c_1, d_0\}$, and $B_3 + 0_1 = \{a_1, b_1, c_1, d_1\}$ are also contained in $\mathcal{B}$. Accordingly, we classify all quadruples into three types distinguished by using semicolons to separate the points.

- Type I: All quadruples of the form $\{a_0, b_0, c_1, d_1\}$, simply denoted by $\{a, b; c, d\}$, where $a \neq b$ and $c \neq d$.
- Type II: All quadruples of the form $\{a_0, b_0, c_0, d_1\}$ or $\{a_1, b_1, c_1, d_0\}$, simply denoted by $\{a, b, c; d\}$, where a, b, and c are pairwise distinct.
- Type III: All quadruples of the form $\{a_0, b_0, c_0, d_0\}$ or $\{a_1, b_1, c_1, d_1\}$, simply denoted by $\{a, b, c, d\}$, where a, b, c, and d are pairwise distinct.

Similarly, all triples of the form $\{a_0, b_0, c_0\}$ or $\{a_1, b_1, c_1\}$ are called *pure triples*, simply denoted by $\{a, b, c\}$, and all triples of the form $\{a_0, b_0, c_1\}$ or $\{a_1, b_1, c_0\}$ are called *mixed triples*, and simply denoted by $\{a, b; c\}$. Clearly, pure triples are contained in Type II and (or) Type III quadruples, and mixed triples are contained in Type I and (or) Type II quadruples.

Notice that

$$\mathbb{Z}_{2n}^{\times} \cong \mathbb{Z}_n^{\times} \times \mathbb{Z}_2^{\times} = \{x_1 \mid x \in \mathbb{Z}_n^{\times}\}.$$

For an AsSQS($2n$), every element $x_1 \in \mathbb{Z}_n^{\times} \times \mathbb{Z}_2^{\times}$ should be a multiplier. Hence we can simply omit the subscripts of multipliers as well. In what follows, we use these simple notation of quadruples and triples without subscripts.

2.2.2 Direct construction A

Let $p \equiv 1, 5 \pmod{12}$ be prime, and suppose $(\mathbb{Z}_{2p}, \mathcal{B})$ is an AsSQS. Then, $\mathbb{Z}_p^* = \mathbb{Z}_p^{\times}$. For pairwise distinct elements $a, b, c, d \in \mathbb{Z}_p^*$, let $B_1 = \{a, b; c, d\} \in \mathcal{B}$. By the affine-invariant property,

$$B_1' := (a^{-1}b - 1)^{-1}(a^{-1}B_1 - 1) = \{0, 1; (c-a)(b-a)^{-1}, (d-a)(b-a)^{-1}\}$$

must be contained in $\mathcal{O}_A(B_1)$. So B_1' can be chosen as a base block of the affine orbit. Similarly, in each affine orbit, regardless of Type I, II, or III, there must exist a block containing $\{0, 1\}$. Therefore, it suffices to find base blocks of the form $\{0, 1; a, b\}$, $\{0, 1, c; d\}$, and $\{0, 1, e, f\}$ such that all the pure triples in $\big\{\{0, 1, x\} \mid x \in \mathbb{Z}_p \setminus \{0, 1\}\big\}$ and all the mixed triples in $\big\{\{0, 1; y\} \mid y \in \mathbb{Z}_p\big\}$ are covered exactly once in their affine orbits.

In order to cover the pure triple $\{0, 1, -1\}$, we have the following lemma:

Lemma 2.2.1 (Type II)**.** *Let $(\mathbb{Z}_{2p}, \mathcal{B})$ be an AsSQS. Then there exists a Type II quadruple $\{0, 1, -1; 0\} \in \mathcal{B}$.*

Proof. Obviously, the pure triple $\{0, 1, -1\}$ cannot be covered by any Type I quadruple. Now, we show that $\{0, 1, -1\}$ cannot be covered by a Type III quadruple either. Assume there exists a Type III quadruple containing $\{0, 1, -1\}$, say $B = \{0, 1, -1, x\} \in \mathcal{B}$. Then we have $-B = \{0, -1, 1, -x\} \in \mathcal{B}$, which implies $x = -x$. Hence $x = 0$, in which case $B = \{0, 1, -1\}$ becomes a triple. Then, we suppose there is a Type II quadruple $\{0, 1, -1; y\} \in \mathcal{B}$. Thus $\{0, -1, 1; -y\} \in \mathcal{B}$ which implies $y = 0$. Therefore, the only possible quadruple containing $\{0, 1, -1\}$ is $\{0, 1, -1; 0\}$. $\square$

In $\mathcal{O}_A(\{0, 1, -1; 0\})$, there are another two quadruples containing $\{0, 1\}$, namely $\{1, 0, 2; 1\}$ and $\{2^{-1}, 0, 1; 2^{-1}\}$. Thus it remains to consider the mixed triple $\{0, 1; y\}$ for every $y \in \mathbb{Z}_p \setminus \{0, 1, 2^{-1}\}$, and the pure triple $\{0, 1, x\}$ for every $x \in \mathbb{Z}_p \setminus \{0, 1, -1, 2, 2^{-1}\}$.

Remark. Köhler [65] and Siemon [103] used geometric representations for the triples and quadruples, namely, triangles and quadrilaterals. Lemma 2.2.1 can also follow from Siemon [103] §2 concerning right triangles and equilateral triangles (cf. Section 2.1.3).

In this subsection, we intend to cover all the remaining mixed and pure triples by Type I and III quadruples, respectively. Firstly, we can obtain all Type I base blocks as follows.

Lemma 2.2.2 (Type I)**.** *Let* $\left\{b_1, b_2, \ldots, b_{\frac{p-5}{4}}\right\}$ *be a system of representatives of*

$$\left\{\mathrm{orb}_{\boldsymbol{AC}}(b) \,\middle|\, b \in \mathbb{Z}_p \setminus \{0, 1, 2^{-1}, \chi, 1-\chi\}\right\}. \tag{2.12}$$

Let $B_b^{(1)} = \{0, 1; b, 1-b\}$ *and*

$$\mathcal{B}_1 = \left\{B_{b_i}^{(1)} \,\middle|\, i \in \left[\tfrac{p-5}{4}\right]\right\} \cup \{B_\chi^{(1)}\}.$$

Then, $\bigcup_{B \in \mathcal{B}_1} \mathcal{O}_A(B)$ *covers the mixed triple* $\{0, 1; y\}$ *exactly once for every* $y \in \mathbb{Z}_p \setminus \{0, 1, 2^{-1}\}$.

Proof. There are only two quadruples containing $\{0, 1\}$ in $\mathcal{O}_A(B_b^{(1)})$, namely $B_b^{(1)} = \{0, 1; b, 1-b\}$ and $\{\frac{-b}{1-2b}, \frac{1-b}{1-2b}; 0, 1\}$. Hence, all the mixed triples contained in $\mathcal{O}_A(B_b^{(1)})$ are $\{\{0, 1; y\} \mid y \in \mathrm{orb}_{\boldsymbol{AC}}(b)\}$. In particular, $\mathrm{orb}_{\boldsymbol{AC}}(0) = \{0, 1\}$, $\mathrm{orb}_{\boldsymbol{AC}}(2^{-1}) = \{2^{-1}, \infty\}$, and $\mathrm{orb}_{\boldsymbol{AC}}(\chi) = \{\chi, 1-\chi\}$. Thus,

$$\dot{\bigcup_{i=1}^{\frac{p-5}{4}}} \mathrm{orb}_{\boldsymbol{AC}}(b_i) \cup \mathrm{orb}_{\boldsymbol{AC}}(\chi) = \bigcup_{b \in \mathbb{Z}_p \setminus \{0,1,2^{-1}\}} \mathrm{orb}_{\boldsymbol{AC}}(b) = \mathbb{Z}_p \setminus \{0, 1, 2^{-1}\},$$

which implies that each mixed triple containing $\{0, 1\}$ appears exactly once in $\bigcup_{B \in \mathcal{B}_1} \mathcal{O}_A(B)$. □

Remark. Köhler [65] separated the "Köhler graph" into two components, KG_1 and KG_2, where KG_1 was proved to have a 1-factor by Siemon [103]. Lemma 2.2.2 can also follow from Siemon [103] §3 applied to KG_1 (cf. Section 2.1.3).

It has been shown that $\Omega_p = \mathbb{Z}_p \setminus \{0, 1, -1, 2, 2^{-1}\}$ can be partitioned into cross-ratio classes. Moreover, each edge in the graph $\mathrm{CG}(\Omega_p)$ can be written as $\{C(a), C(\bar{a})\}$ for some $a \in \Omega_p$, where $C(a)$ is the cross-ratio class with respect to a. Suppose $\mathrm{CG}(\Omega_p)$ has a 1-factor, then the edge set of the 1-factor gives a partition of Ω_p into pairs of cross-ratio classes. Moreover, when $p \equiv 1 \pmod{12}$, by Proposition 2.1.10 (ii), there is a pendant edge incident with $C(\xi)$, which must be contained in the 1-factor. We propose the base block corresponding to this pendant edge as follows:

Lemma 2.2.3 (Type III$^\xi$)**.** *Suppose* $p \equiv 1 \pmod{12}$*. If* $\mathrm{CG}(\Omega_p)$ *has a 1-factor* F *containing the edge* $\{C(\xi), C(\bar{\xi})\}$*, where* ξ *is a root of* $\xi^2 - \xi + 1 = 0$ *over* $\mathbb{Z}_p$*. Let* $B_\xi^{(3)} = \{0, 1, \xi, \bar{\xi}\}$*. Then,* $\mathcal{O}_A(B_\xi^{(3)})$ *covers the pure triple* $\{0, 1, x\}$ *exactly once for every* $x \in \overline{C}(\xi)$.

Proof. All the quadruples containing $\{0,1\}$ in $\mathcal{O}_A(B_\xi^{(3)})$ can be determined explicitly, namely, $\left\{0,1,\xi,\frac{1}{1+\xi^{-1}}\right\}$, $\left\{0,\xi^{-1},1,\frac{1}{1+\xi}\right\}$, $\left\{0,1+\xi^{-1},1+\xi,1\right\}$, and $\left\{1,-\xi^{-1},-\xi,0\right\}$. Note that

$$C(\bar{\xi}) = \left\{\frac{1}{1+\xi^{-1}}, 1+\xi^{-1}, -\xi^{-1}, -\xi, 1+\xi, \frac{1}{1+\xi}\right\}.$$

Hence, the pure triple $\{0,1,x\}$ for every $x \in \overline{C}(\xi) = C(\xi) \cup C(\bar{\xi})$ appears exactly once in $\mathcal{O}_A(B_\xi^{(3)})$. $\square$

The graph $\mathrm{CG}(\Omega_p)$ has $\frac{p-1}{6}$ vertices if $p \equiv 1 \pmod{12}$, and $\frac{p-5}{6}$ vertices if $p \equiv 5 \pmod{12}$. Hence, besides the previously discussed edge $\{C(\xi), C(\bar{\xi})\}$ when $p \equiv 1 \pmod{12}$, a 1-factor of $\mathrm{CG}(\Omega_p)$ has ℓ_p edges, where

$$\ell_p = \begin{cases} \frac{p-5}{12}, & \text{if } p \equiv 5 \pmod{12}, \\ \frac{p-13}{12}, & \text{if } p \equiv 1 \pmod{12}. \end{cases} \tag{2.13}$$

We can obtain all the other Type III base blocks as follows:

Lemma 2.2.4 (Type III). *Assume that $\mathrm{CG}(\Omega_p)$ has a 1-factor F. Let a_1, a_2, $\ldots$, a_{ℓ_p} be elements in Ω_p with $a_i \notin C(\xi) \cup C(\bar{\xi})$ for each $i \in [\ell_p]$, such that*

$$\left\{\{C(a_1), C(\overline{a_1})\}, \{C(a_2), C(\overline{a_2})\}, \ldots, \{C(a_{\ell_p}), C(\overline{a_{\ell_p}})\}\right\} = E(F) \setminus \{C(\xi), C(\bar{\xi})\},$$

where $E(F)$ is the edge set of F. Let $B_{a_i}^{(3)} = \{0,1,a_i,1-a_i\}$ and $\mathcal{B}_3 = \left\{B_{a_i}^{(3)} \,\middle|\, i \in [\ell_p]\right\}$. Then $\bigcup_{B \in \mathcal{B}_3} \mathcal{O}_A(B)$ covers the pure triple $\{0,1,x\}$ exactly once for every $x \in \Omega_p \setminus \overline{C}(\xi)$.

Proof. For $a \notin \overline{C}(\xi)$, all the quadruples containing $\{0,1\}$ in $\mathcal{O}_A(B_a^{(3)})$ are $\{0,1,a,1-a\}$, $\left\{0,\frac{1}{a},1,\frac{\bar{a}}{\bar{a}-1}\right\}$, $\left\{1,\frac{a-1}{a},0,\frac{1}{1-\bar{a}}\right\}$, $\left\{0,\frac{1}{1-a},\frac{\bar{a}-1}{\bar{a}},1\right\}$, $\left\{1,\frac{a}{a-1},\frac{1}{\bar{a}},0\right\}$, and $\{\bar{a},1-\bar{a},1,0\}$. Therefore, the pure triple $\{0,1,x\}$ appears in $\mathcal{O}_A(B_a^{(3)})$ for every $x \in \overline{C}(a)$. Furthermore, each pure triple $\{0,1,x\}$ appears exactly once if $|C(a)| = |C(\bar{a})| = 6$ holds. In fact, as shown in (2.6), all the cross-ratio classes are of size 6 except $C(-1) = \{-1,2,2^{-1}\}$, $C(0) = \{0,1,\infty\}$, and $C(\xi) = \{\xi, 1-\xi\}$.

$\square$

To summarize, we propose Theorem 2.2.5 and Construction 2.2.6, which directly follow from Lemmas 2.2.1, 2.2.2, 2.2.3, and 2.2.4. Theorem 2.2.5 indicates that $\mathrm{AsSQS}(v)$, which has a stronger "symmetry", does not require stronger criteria than $\mathrm{sSQS}(v)$.

Theorem 2.2.5. *Let $p \equiv 1 \pmod 4$ be a prime. If $\mathrm{CG}(\Omega_p)$ has a 1-factor, then there exists an AsSQS$(2p)$.*

Table 2.2: The base blocks of an $\mathrm{AsSQS}^A(2p)$ for $p \equiv 5 \pmod{12}$

Type	Base blocks	# Base blocks	# Cyclic orbits	Lemmas
I'	$\{0,1;\chi,1-\chi\}$	1	$\frac{p-1}{4}$	Lemma 2.2.2
I	$\{0,1;b_i,1-b_i\}$	$i \in \left[\frac{p-5}{4}\right]$	$\frac{p-1}{2}$	Lemma 2.2.2
II'	$\{0,1,-1;0\}$	1	$\frac{p-1}{2}$	Lemma 2.2.1
III	$\{0,1,a_i,1-a_i\}$	$i \in \left[\frac{p-5}{12}\right]$	$\frac{p-1}{2}$	Lemma 2.2.4
Total		$\frac{p+1}{3}$	$\frac{(p-1)(2p-1)}{12}$	

Table 2.3: The base blocks of an $\mathrm{AsSQS}^A(2p)$ for $p \equiv 1 \pmod{12}$

Type	Base blocks	# Base blocks	# Cyclic orbits	Lemmas
I'	$\{0,1;\chi,1-\chi\}$	1	$\frac{p-1}{4}$	Lemma 2.2.2
I	$\{0,1;b_i,1-b_i\}$	$i \in \left[\frac{p-5}{4}\right]$	$\frac{p-1}{2}$	Lemma 2.2.2
II'	$\{0,1,-1;0\}$	1	$\frac{p-1}{2}$	Lemma 2.2.1
III^ξ	$\{0,1,\xi,\bar{\xi}\}$	1	$\frac{p-1}{3}$	Lemma 2.2.3
III	$\{0,1,a_i,1-a_i\}$	$i \in \left[\frac{p-13}{12}\right]$	$\frac{p-1}{2}$	Lemma 2.2.4
Total		$\frac{p+2}{3}$	$\frac{(p-1)(2p-1)}{12}$	

Construction 2.2.6. If $\mathrm{CG}(\Omega_p)$ has a 1-factor, choose $a_1, a_2, \ldots, a_{\lfloor \frac{p}{12} \rfloor}$ as in Lemma 2.2.4. Choose $b_1, b_2, \ldots, b_{\frac{p-1}{4}}$ as in Lemma 2.2.2. Then all the base blocks of $\mathrm{AsSQS}(2p)$ are given as follows:

(i) For $p \equiv 1 \pmod{12}$,

Type I, $\{0,1;b_i,1-b_i\}$, for $i \in \left[\frac{p-1}{4}\right]$,
Type II', $\{0,1,-1;0\}$,
Type III^ξ, $\{0,1,\xi,\bar{\xi}\}$,
Type III, $\{0,1,a_i,1-a_i\}$, for $i \in \left[\frac{p-13}{12}\right]$, $a_i \notin \overline{C}(\xi)$,

where ξ is a root of $x^2 - x + 1 = 0$ over $\mathbb{Z}_p$.

(ii) For $p \equiv 5 \pmod{12}$,

Type I, $\{0,1;b_i,1-b_i\}$, for $i \in \left[\frac{p-1}{4}\right]$,
Type II', $\{0,1,-1;0\}$,
Type III, $\{0,1,a_i,1-a_i\}$, for $i \in \left[\frac{p-5}{12}\right]$.

In Table 2.2 and Table 2.3, we summarize the number of base blocks of each type (in the column with header "# Base blocks"), and the numbers of cyclic orbits contained in the affine orbit of a base block B of a given type (in the column with header "# Cyclic orbits"), that is, $\frac{|\mathcal{O}_A(B)|}{2p}$.

Moreover, we denote an $\mathrm{AsSQS}(2p)$ obtained from Constructions 2.2.6 by $\mathrm{AsSQS}^A(2p)$.

By utilizing Theorem 2.1.12 and Lemma 2.1.13, respectively, we have the following as corollaries of Theorem 2.2.5:

Corollary 2.2.7. *For prime* $p \equiv 1 \pmod 4$ *and* $p \not\equiv 1, 49 \pmod{60}$, *if* $\mathrm{CG}(\Omega_p)$ *is bridgeless, then there exists an* $AsSQS^A(2p)$.

Corollary 2.2.8. *There exists an* $AsSQS^A(2p)$ *for all primes* $p < 10^5$ *satisfying* $p \equiv 1 \pmod 4$.

Example 2.2.9. Let $p = 17$. Then $\mathcal{B}_1$ consists of

$$\{0,1;7,11\}, \{0,1;4,14\}, \{0,1;5,13\}, \{0,1;6,12\},$$

and $\mathcal{B}_3$ consists of

$$\{0,1,3,15\},$$

where $\chi = 7$ (cf. Figure 2.4).

Example 2.2.10. Let $p = 29$. Then $\mathcal{B}_1$ consists of

$$\{0,1;9,21\}, \{0,1;13,17\}, \{0,1;12,18\}, \{0,1;10,20\},$$

$$\{0,1;14,16\}, \{0,1;11,19\}, \{0,1;7,25\},$$

and $\mathcal{B}_3$ consists of

$$\{0,1,3,27\}, \{0,1,11,19\}$$

which correspond to the edges $\{C(3), C(9)\}$ and $\{C(4), C(5)\}$ of $\mathrm{CG}(\Omega_{29})$, respectively, where $\chi = 9$ (cf. Figure 2.5).

Example 2.2.11. Let $p = 41$. Then $\mathcal{B}_1$ consists of

$$\{0,1;5,37\}, \{0,1;14,28\}, \{0,1;17,25\}, \{0,1;18,24\},$$

$$\{0,1;8,34\}, \{0,1;10,32\}, \{0,1;15,27\}, \{0,1;20,22\},$$

$$\{0,1;13,29\}, \{0,1;19,23\},$$

and $\mathcal{B}_3$ consists of

$$\{0,1,3,39\}, \{0,1,4,38\}, \{0,1,10,32\}$$

which correspond to the edges $\{C(3), C(13)\}$, $\{C(4), C(12)\}$, and $\{C(5), C(6)\}$ of $\mathrm{CG}(\Omega_{41})$, respectively, where $\chi = 5$ (cf. Figure 2.5).

2.2.3 Direct construction B

Yoshikawa [129] proposed an idea for constructing AsSQS($2p$) by using Type II quadruples as much as possible, and showed that such AsSQS($2p$) exists for all primes $17 \leq p < 100$ satisfying $p \equiv 1 \pmod 4$ by computer search. In this subsection, we present Yoshikawa's idea somewhat differently and provide a combinatorial criterion for those constructions.

Let $p \equiv 1, 5 \pmod{12}$ be prime and suppose $(\mathbb{Z}_{2p}, \mathcal{B})$ is an AsSQS without Type III quadruples. If we color the point $x \in \mathbb{Z}_{2p}$ in red if $x \equiv 0 \pmod 2$ and in blue if $x \equiv 1 \pmod 2$, it is clear that Type III quadruples are monochromatic and the other two types are not. By assigning two colors to all the points, if an SQS does not have any monochromatic quadruple, then the SQS is said to be 2-*chromatic* (see [59, 92]). Hence, an AsSQS having no Type III quadruples must be 2-chromatic. Note that, under the assumptions in this subsection, Lemma 2.2.1 remains true, that is, $\{0, 1, -1; 0\} \in \mathcal{B}$.

Lemma 2.2.12 (Type I). *There exists exactly one affine orbit of Type I quadruples, say $\mathcal{O}_A(B)$, where $B = \{0, 1; \chi, 1-\chi\}$, and $\chi = \frac{1+\sqrt{-1}}{2}$ is a root of $2\chi^2 - 2\chi + 1 = 0$ over $\mathbb{Z}_p$.*

Proof. The total numbers of pure triples $\{0, 1, x\}$ and mixed triples $\{0, 1; y\}$ are $p-2$ and p, respectively. Under the assumption that there is no Type III quadruple, there must be exactly two mixed triples not covered by Type II quadruples, say $\{0, 1; y_1\}$ and $\{0, 1; y_2\}$. Let $B = \{0, 1; y_1, y_2\}$ be a quadruple in $\mathcal{B}$. Then there should not exist any other triple containing $\{0, 1\}$ in $\mathcal{O}_A(B)$. Note that $1 - B = \{1, 0; 1-y_1, 1-y_2\} \in \mathcal{O}_A(B)$. Then we have $\{y_1, y_2\} = \{1-y_1, 1-y_2\}$ which implies $y_1 + y_2 = 1$. For $B = \{0, 1; y_1, 1-y_1\}$, similarly to the proof of Lemma 2.2.2, $\mathrm{orb}_{\boldsymbol{AC}}(y_1)$ should be of size two (cf. (2.11)). Thus we have $y_1 \in \{0, 1\}$ or $y_1 \in \{\chi, 1-\chi\}$, in which the former contradicts Lemma 2.2.1. □

Let $B = \{0, 1, x; y\}$ be a Type II quadruple. Then there are six quadruples containing $\{0, 1\}$ in $\mathcal{O}_A(B)$, namely,

$$\{0, 1, x;\ y\}, \{1, 0, 1-x;\ 1-y\}, \left\{\frac{1}{1-x}, 0, 1;\ \frac{1-y}{1-x}\right\},$$

$$\left\{\frac{x}{x-1}, 1, 0;\ \frac{x-y}{x-1}\right\}, \left\{1, \frac{x-1}{x}, 0;\ \frac{x-y}{x}\right\}, \text{ and } \left\{0, \frac{1}{x}, 1;\ \frac{y}{x}\right\}.$$

Clearly, $\mathcal{O}_A(B)$ covers the pure triple $\{0, 1, a\}$ for every $a \in C(x)$ and the mixed triple $\{0, 1; b\}$ for every $b \in H(x, y)$, where $C(x)$ is the cross-ratio class with respect to x and

$$H(x, y) = \left\{y, \frac{y}{x}, \frac{x-y}{x}, \frac{x-y}{x-1}, \frac{1-y}{1-x}, 1-y\right\}. \tag{2.14}$$

Lemma 2.2.13 (Type II$^\xi$). *For $p \equiv 1 \pmod{12}$, $\{0, 1, \xi; \bar{\xi}\} \in \mathcal{B}$ holds, where ξ is a root of $\xi^2 - \xi + 1 = 0$ over $\mathbb{Z}_p$, and $\bar{\xi} = \frac{\xi}{\xi+1}$.*

Proof. By (2.6), $C(\xi) = \{\xi, 1-\xi\}$ is of size two. Under the assumption that there is no Type III quadruple, we suppose $B = \{0, 1, \xi; y\} \in \mathcal{B}$. All the quadruples containing $\{0, 1, \xi\}$ in $\mathcal{O}_A(B)$ should be identical, that is, $\{0, 1, \xi; y\}$, $\{0, 1, \xi; \xi(1-y)\}$, and $\{0, 1, \xi; 1-\xi^{-1}y\}$ are identical. Hence, we have $y = \frac{\xi}{\xi+1}$. □

Let

$$\Omega_p^* = \begin{cases} \mathbb{Z}_p \setminus \left\{0, 1, -1, 2, 2^{-1}, \xi, 1-\xi\right\}, & \text{for } p \equiv 1 \pmod{12}, \\ \mathbb{Z}_p \setminus \left\{0, 1, -1, 2, 2^{-1}\right\}, & \text{for } p \equiv 5 \pmod{12}, \end{cases} \tag{2.15}$$

$$\Lambda_p = \begin{cases} \mathbb{Z}_p \setminus \left\{0, 1, 2^{-1}, \chi, 1-\chi, \bar{\xi}, 1-\bar{\xi}\right\}, & \text{for } p \equiv 1 \pmod{12}, \\ \mathbb{Z}_p \setminus \left\{0, 1, 2^{-1}, \chi, 1-\chi\right\}. & \text{for } p \equiv 5 \pmod{12}. \end{cases} \tag{2.16}$$

It is clear that $\left|\Omega_p^*\right| = |\Lambda_p|$ is divisible by 6. By combining Lemmas 2.2.1, 2.2.12, and 2.2.13, it is straightforward to get the following:

Lemma 2.2.14 (Type II)**.** *An AsSQS(2p) having no Type III quadruples exists if and only if there exists $(x_i, y_i) \in \Omega_p^* \times \Lambda_p$ for each $i \in \left[\frac{|\Lambda_p|}{6}\right]$, such that*

$$\biguplus_{i=1}^{|\Lambda_p|/6} C(x_i) = \Omega_p^* \quad \text{and} \quad \biguplus_{i=1}^{|\Lambda_p|/6} H(x_i, y_i) = \Lambda_p.$$

It is easily seen from (2.6) and (2.15) that Ω_p^* can be partitioned into cross-ratio classes of size 6. Next, we intend to partition Λ_p into $H(x, y)$. Let $z = \frac{y}{x}$, then $H(x, y)$ can be rewritten as

$$H\left(\frac{y}{z}, y\right) = \left\{y, z, 1-z, \frac{y(1-z)}{y-z}, \frac{z(1-y)}{z-y}, 1-y\right\}. \tag{2.17}$$

For $y, z \in \mathbb{Z}_p$, we define a mapping $\diamond : \mathbb{Z}_p \times \mathbb{Z}_p \to \mathbb{Z}_p \cup \{\infty\}$ as a binary operator, such that $y \diamond z = \frac{y(1-z)}{y-z}$, and $y \diamond z = \infty$ if $y = z$. The following properties can be easily derived:

Proposition 2.2.15. For any distinct $y, z \in \mathbb{Z}_p \setminus \{0, 1\}$, the following hold:

(i) $(1-y) \diamond (1-z) = z \diamond y$;

(ii) $y \diamond z + z \diamond y = 1$;

(iii) The solutions of $y \diamond x = z$ and $x \diamond y = z$ with respect to x are $x = y \diamond z$ and $x = y \diamond (1-z)$, respectively.

In order to establish a hypergraph representation and convert the partition problem to a similar hypergraph factor problem (cf. the graph $\mathrm{CG}(\Omega_p)$), we need some notation and propositions. For a given $x \in \mathbb{Z}_p$, denote

$$[\![x]\!] = \begin{cases} x \pmod{p} & \text{if } x \in \{1, 2, \ldots, \frac{p+1}{2}\}, \\ 1-x \pmod{p} & \text{if } x \in \{\frac{p+3}{2}, \frac{p+5}{2}, \ldots, p-1, 0\}. \end{cases} \tag{2.18}$$

For a subset $X \subseteq \mathbb{Z}_p$, denote

$$[\![X]\!] = \{[\![x]\!] \mid x \in X\}.$$

For distinct $y, z \in \mathbb{Z}_p$, define

$$J(y,z) = [\![H(\tfrac{y}{z}, y)]\!] = \{[\![y]\!], [\![z]\!], [\![y \diamond z]\!]\} \tag{2.19}$$

It is easy to observe that $\dot\bigcup_{i=1}^{|\Lambda_p|/6} H(x_i, y_i) = \Lambda_p$ if and only if

$$\dot\bigcup_{i=1}^{|\Lambda_p|/6} J(y_i, z_i) = [\![\Lambda_p]\!],$$

where $z_i = y_i/x_i$.

Lemma 2.2.16. *Let*

$$\mathcal{B} = \{J(y,z) |\, y, z \in \mathbb{Z}_p \setminus \{0,1\}, y \neq z\}\,. \tag{2.20}$$

(i) For any distinct $y, z \in \mathbb{Z}_p \setminus \{0,1\}$ with $y + z \neq 1$, the pair $\{[\![y]\!], [\![z]\!]\}$ appears exactly λ times in $\mathcal{B}$, where $\lambda = \begin{cases} 1 & \textit{if } 2^{-1} \in \{y,z\}, \\ 2 & \textit{otherwise.} \end{cases}$

(ii) For any $B \in \mathcal{B}$, $\#\big\{C\left(\frac{u}{v}\right) \big|\, u, v \in \mathbb{Z}_p \setminus \{0,1\}, J(u,v) = B\big\} \leq 2$.

Proof. (i) The pair $\{[\![y]\!], [\![z]\!]\}$ is contained in $J(y,z)$ and $J(y, 1-z)$, whose third elements are determined by $w_1 = [\![y \diamond z]\!]$ and $w_2 = [\![y \diamond (1-z)]\!]$, respectively. Suppose w satisfies $J(a,w) = \{[\![a]\!], [\![w]\!], [\![b]\!]\}$ or $J(w,a) = \{[\![w]\!], [\![a]\!], [\![b]\!]\}$, where $\{a, b\} \in \{y, 1-y\} \times \{z, 1-z\} \cup \{z, 1-z\} \times \{y, 1-y\}$. By Proposition 2.2.15 (iii), the set of all possible values of w is given by

$$W = \{a \diamond b \mid \{a,b\} \in \{y, 1-y\} \times \{z, 1-z\} \cup \{z, 1-z\} \times \{y, 1-y\}\}.$$

By using Proposition 2.2.15 (ii) and (i) successively, we have

$$\begin{aligned} [\![W]\!] &= \{[\![a \diamond b]\!] \mid \{a,b\} \in \{y, 1-y\} \times \{z, 1-z\}\} \\ &= \{[\![y \diamond z]\!], [\![y \diamond (1-z)]\!]\} = \{w_1, w_2\}. \end{aligned}$$

Moreover, $w_1 = w_2$ if and only if $z = 2^{-1}$ or $y = 2^{-1}$.

(ii) For a given $B = \{[\![y]\!], [\![z]\!], [\![y \diamond z]\!]\}$, all the possible unordered pairs (u,v) chosen from $\{y, 1-y, z, 1-z, y \diamond z, z \diamond y\}$ satisfying $J(u,v) = J(y,z)$ are (y,z), $(1-y, 1-z)$, $(y, y \diamond z)$, $(1-y, z \diamond y)$, $(z, z \diamond y)$, and $(1-z, y \diamond z)$. By calculating the cross-ratio classes with respect to the quotients of all these pairs, we have $C\left(\frac{y}{z}\right) = C\left(\frac{1-y}{z \diamond y}\right) = C\left(\frac{1-z}{y \diamond z}\right)$ and $C\left(\frac{1-y}{1-z}\right) = C\left(\frac{y}{y \diamond z}\right) = C\left(\frac{z}{z \diamond y}\right)$, which completes the proof.

□

Remark. From the viewpoint of hypergraphs, we consider the vertex-induced sub-hypergraph of $([\![\mathbb{Z}_p]\!] \setminus \{0,1\}, \mathcal{B})$ on $[\![\Lambda_p]\!]$, whose edge set (treated as a multiset) is

$$\mathcal{B}^* = \big\{B^* = B \setminus [\![\mathbb{Z}_p \setminus \Lambda_p]\!] \big|\, B \in \mathcal{B}, |B^*| \geq 2\ \big\}.$$

Since $2^{-1} \notin \Lambda_p$, by Lemma 2.2.16, $([\![\Lambda_p]\!], \mathcal{B}^*)$ is a $(\frac{|\Lambda_p|}{2}, \{2,3\}, 2)$ pairwise balanced design (PBD).

Definition 2.2.17. Let $\mathcal{B}^{\triangle}$ denote the collection of all triples in $\mathcal{B}^*$, i.e.,

$$\mathcal{B}^{\triangle} = \left\{ B^* = B \setminus [\![\mathbb{Z}_p \setminus \Lambda_p]\!] \,\middle|\, B \in \mathcal{B}, |B^*| = 3 \right\}. \tag{2.21}$$

Let

$$\mathcal{C} = \left\{ C(x) \mid x \in \Omega_p^* \right\}. \tag{2.22}$$

Let γ_0 denote a mapping from $\mathcal{B}^{\triangle}$ to $2^{\mathcal{C}}$ such that

$$\gamma_0(B) = \left\{ C\left(\frac{u}{v}\right) \,\middle|\, u, v \in \Lambda_p, J(u,v) = B \right\}.$$

Then, $([\![\Lambda_p]\!], \mathcal{B}^{\triangle}, \gamma_0)$ is an edge-colored hypergraph.

It follows from Lemma 2.2.16 (ii) that $|\gamma_0(B)| \leq 2$ for every $B \in \mathcal{B}^{\triangle}$. Thus, it suffices to investigate an equivalent edge-colored hypergraph whose color-set is $\mathcal{C}$.

Definition 2.2.18. Let $\mathcal{B}_2^{\triangle}$ be the multiset obtained by doubling all triples in $\mathcal{B}^{\triangle}$, i.e., $\mathcal{B}_2^{\triangle} = \mathcal{B}^{\triangle} \uplus \mathcal{B}^{\triangle}$. Let γ be a mapping from $\mathcal{B}_2^{\triangle}$ to $\mathcal{C}$, such that for given $B = B' = \{[\![y]\!], [\![z]\!], [\![y \diamond z]\!]\} \in \mathcal{B}_2^{\triangle}$,

$$\gamma(B) = C\left(\frac{y}{z}\right) \quad \text{and} \quad \gamma\left(B'\right) = C\left(\frac{1-y}{1-z}\right),$$

where $\{C(\frac{y}{z}), C(\frac{1-y}{1-z})\} = \gamma_0(B)$ for $B \in \mathcal{B}^{\triangle}$. Then $([\![\Lambda_p]\!], \mathcal{B}_2^{\triangle}, \gamma)$ is an edge-colored hypergraph.

Suppose $\mathcal{F} \subseteq \mathcal{B}^{\triangle}$ is a 1-factor of $([\![\Lambda_p]\!], \mathcal{B}_2^{\triangle}, \gamma)$. If $\gamma(F_1) \neq \gamma(F_2)$ for any distinct $F_1, F_2 \in \mathcal{F}$, then $\mathcal{F}$ is said to be *a rainbow 1-factor*. To sum it all up, we propose Theorem 2.2.19 and Construction 2.2.20, using Lemmas 2.2.1, 2.2.12, 2.2.13, and 2.2.14.

Theorem 2.2.19. *An AsSQS($2p$) having no Type III quadruples exists if the edge-colored hypergraph $([\![\Lambda_p]\!], \mathcal{B}_2^{\triangle}, \gamma)$ has a rainbow 1-factor.*

Proof. A 1-factor of $([\![\Lambda_p]\!], \mathcal{B}_2^{\triangle}, \gamma)$ gives rise to a partition of $[\![\Lambda_p]\!]$ into triples of the form $J(y,z)$. Moreover, it is clear that $\mathcal{C}$ is a partition of Ω_p^*, which is also the color-set of $([\![\Lambda_p]\!], \mathcal{B}_2^{\triangle}, \gamma)$. Since $\frac{|\Omega_p^*|}{6} = \frac{|[\![\Lambda_p]\!]|}{3}$, every edge in a rainbow 1-factor has a distinct color in $\mathcal{C}$. Hence, a rainbow 1-factor forms a partition of Ω_p^*. By Lemma 2.2.14, an AsSQS($2p$) having no Type III quadruples can be constructed as claimed. $\square$

Construction 2.2.20. When $([\![\Lambda_p]\!], \mathcal{B}_2^{\triangle}, \gamma)$ has a rainbow 1-factor with edge set

$$\mathcal{F} = \left\{ B_i = J(y_i, z_i) \,\middle|\, i \in \left[\frac{|\Lambda_p|}{6}\right] \right\},$$

such that

$$\dot{\bigcup_{i=1}^{|\Lambda_p|/6}} C\left(\frac{y_i}{z_i}\right) = \Omega_p^*,$$

Table 2.4: The base blocks of an $\mathrm{AsSQS}^B(2p)$ for $p \equiv 5 \pmod{12}$

Type	Base block	# Base blocks	# Cyclic orbits	Lemmas
I′	$\{0,1;\chi,1-\chi\}$	1	$\frac{p-1}{4}$	Lemma 2.2.12
II′	$\{0,1,-1;0\}$	1	$\frac{p-1}{2}$	Lemma 2.2.1
II	$\{0,1,a_i;b_i\}$	$i \in [\frac{p-5}{6}]$	$p-1$	Lemma 2.2.14
Total		$\frac{p+7}{6}$	$\frac{(p-1)(2p-1)}{12}$	

Table 2.5: The base blocks of an $\mathrm{AsSQS}^B(2p)$ for $p \equiv 1 \pmod{12}$

Type	Base block	# Base blocks	# Cyclic orbits	Lemmas
I′	$\{0,1;\chi,1-\chi\}$	1	$\frac{p-1}{4}$	Lemma 2.2.12
II′	$\{0,1,-1;0\}$	1	$\frac{p-1}{2}$	Lemma 2.2.1
II^ξ	$\{0,1,\xi;\bar{\xi}\}$	1	$\frac{p-1}{3}$	Lemma 2.2.13
II	$\{0,1,a_i;b_i\}$	$i \in [\frac{p-7}{6}]$	$p-1$	Lemma 2.2.14
Total		$\frac{p+11}{6}$	$\frac{(p-1)(2p-1)}{12}$	

let $a_i = \frac{y_i}{z_i}$ and $b_i = y_i$ for $i \in \left[\frac{|\Lambda_p|}{6}\right]$. The base blocks of an AsSQS($2p$) are given as follows:

(i) For $p \equiv 1 \pmod{12}$,

$$\begin{aligned} \text{Type I},\quad & \{0,1;\chi,1-\chi\}, \\ \text{Type II}',\quad & \{0,1,-1;0\}, \\ \text{Type II}^\xi,\quad & \{0,1,\xi;\bar{\xi}\}, \\ \text{Type II},\quad & \{0,1,a_i;b_i\} \text{ for } i \in \left[\tfrac{p-7}{6}\right], \end{aligned}$$

where ξ is a root of $\xi^2-\xi+1=0$ over $\mathbb{Z}_p$.

(ii) For $p \equiv 5 \pmod{12}$,

$$\begin{aligned} \text{Type I},\quad & \{0,1;\chi,1-\chi\}, \\ \text{Type II}',\quad & \{0,1,-1;0\}, \\ \text{Type II},\quad & \{0,1,a_i;b_i\} \text{ for } i \in \left[\tfrac{p-5}{6}\right], \end{aligned}$$

where χ is a root of $2\chi^2-2\chi+1=0$ over $\mathbb{Z}_p$.

In Table 2.4 and Table 2.5, we summarize the number of base blocks of each type (in the column with the header "# Base blocks"), and the numbers of cyclic orbits covered by the affine orbit of a given base block B in each type (in the column with the header "# Cyclic orbits"), that is, $\frac{|\mathcal{O}_A(B)|}{2p}$.

We denote an AsSQS($2p$) obtained from Construction 2.2.20 by $\mathrm{AsSQS}^B(2p)$.

Remark. As shown in Tables 2.2, 2.3, 2.4, and 2.5, the number of base blocks of an $\text{AsSQS}^B(2p)$ is approximately half of $\text{AsSQS}^A(2p)$ for a fixed p. However, the total numbers of cyclic orbits are the same. It is clear that an $\text{AsSQS}^A(2p)$ and an $\text{AsSQS}^B(2p)$ are non-isomorphic.

Example 2.2.21 (Non-existence)**.** Let $p = 13$, then $[\![\mathbb{Z}_p]\!]\backslash\{1\} = \{2, 3, 4, 5, 6, 7\}$. Since $2^{-1} = 7$, $\chi = 3$, and $\frac{1}{\xi+1} = 6$, we have $[\![\Lambda_p]\!] = \{2, 4, 5\}$. Then $([\![\Lambda_p]\!], \mathcal{B}^*)$ is a 2-$(3, 2, 2)$ design, where

$$
\begin{aligned}
\mathcal{B} =& \big\{\{2,3,4\},\{2,3,6\},\{2,5,6\},\{2,5,7\},\{3,4,5\},\{3,5,6\},\{4,6,7\}\big\} \\
& \cup \big\{\{2,4\},\{3,7\},\{4,5\},\{4,6\}\big\}, \\
\mathcal{B}^* =& \big\{\{2,4\},\{2,4\},\{2,5\},\{2,5\},\{4,5\},\{4,5\}\big\} \\
\mathcal{B}^{\triangle} =& \emptyset.
\end{aligned}
$$

Hence, there does not exist an $\text{AsSQS}^B(26)$.

Example 2.2.22. Let $p = 17$, then $[\![\mathbb{Z}_p]\!]\backslash\{1\} = \{2, 3, \ldots, 9\}$. Since $2^{-1} = 9$ and $\chi = 7$, we have $[\![\Lambda_p]\!] = \{2, 3, 4, 5, 6, 8\}$. Then $([\![\Lambda_p]\!], \mathcal{B}^*)$ is a $(6, \{2, 3\}, 2)$-PBD, where

$$
\begin{aligned}
\mathcal{B}^{\triangle} =& \big\{\{2,3,4\},\{2,3,8\},\{2,4,5\},\{3,5,6\},\{4,6,8\},\{5,6,8\}\big\}, \\
\mathcal{B}^* =& \big\{\{2,5\},\{2,6\},\{2,6\},\{2,8\},\{3,4\},\{3,5\},\{3,6\},\{3,8\},\{4,5\}, \\
& \{4,6\},\{4,8\},\{5,8\}\big\} \cup \mathcal{B}^{\triangle}.
\end{aligned}
$$

The hypergraph $([\![\Lambda_p]\!], \mathcal{B}_2^{\triangle}, \gamma)$ has a rainbow 1-factor

$$
\mathcal{F} = \big\{\{2,3,4\},\{5,6,8\}\big\} \subset \mathcal{B}^{\triangle}
$$

such that $\gamma(\{2, 3, 4\}) = C(3/2) = C(10)$ and $\gamma(\{5, 6, 8\}) = C(5/8) = C(7)$, where $C(10) \cup C(7) = \{3, 6, 12, 10, 8, 15\} \cup \{4, 13, 5, 7, 11, 14\} = \Omega_p^*$. Hence $\{0, 1, 10; 3\}$ and $\{0, 1, 7; 5\}$ can be chosen as Type II base blocks of an $\text{AsSQS}^B(34)$.

We have verified the following results on rainbow 1-factors by using computers:

Theorem 2.2.23. *An $AsSQS^B(2p)$ having no Type III quadruples exists if $p \equiv 1, 5 \pmod{12}$ is prime and $17 \leq p < 1000$.*

Actually, the Construction 2.2.20 can be naturally generalized to "affine-invariant" SQSs over $\mathbb{F}_q \oplus \mathbb{F}_2$ with a non-prime q. We give an example for $q = 7^2$. This provides a 2-chromatic SQS(98) whose existence is previously unknown (see Ji [59]).

Example 2.2.24. Let α be a primitive element with $\alpha^2 + 1 = 0$ in $\mathbb{F}_{49}$. Let

$$
\begin{aligned}
& B_I = \{0, 1; 3\alpha + 4, 4\alpha + 4\}, \\
& B_0 = \{0, 1, 6; 0\}, B_\xi = \{0, 1, 3; 6\}, \text{ and } B_i = \{0, 1, a_i; b_i\},
\end{aligned}
$$

where

$$(a_1, a_2, \ldots, a_7) = (6\alpha+1, \alpha+4, 2\alpha+2, 5\alpha+3, 6\alpha+6, \alpha+1, 5) \text{ and}$$
$$(b_1, b_2, \ldots, b_7) = (2\alpha+3, 5\alpha+5, 5\alpha+2, 3\alpha+6, 2\alpha+1, 4\alpha+5, 3\alpha+1).$$

Let $\mathcal{B} = \{mB + c \mid B \in \{B_I, B_\xi, B_0, B_1, \ldots, B_7\}, m \in \mathbb{F}_{49}^\times, c \in \mathbb{F}_{49}\}$, where $|\mathcal{O}_A(B_I)| = 12 \times 98$, $|\mathcal{O}_A(B_0)| = 24 \times 98$, $|\mathcal{O}_A(B_\xi)| = 16 \times 98$, and $|\mathcal{O}_A(B_i)| = 48 \times 98$ for $1 \le i \le 7$. Then, $(\mathbb{F}_{49} \oplus \mathbb{F}_2, \mathcal{B})$ is a 2-chromatic SQS(98).

Note that, this SQS(98) is not cyclic, hence it is not an AsSQS(98). We will show the non-existence of an AsSQS(98) in Section 2.4.

2.3 Affine-invariant strictly cyclic Steiner quadruple systems over $\mathbb{Z}_{2p^m}$

2.3.1 Preliminaries

For the recursive constructions, we still suppose $p \equiv 1, 5 \pmod{12}$ is a prime. Let m be a positive integer. We aim to construct an AsSQS($2p^m$) based on an AsSQS$^A(2p)$ or an AsSQS$^B(2p)$ proposed in Sections 2.2.2 and 2.2.3.

Let χ_m denote a root of $2\chi_m^2 - 2\chi_m + 1 = 0$ over $\mathbb{Z}_{p^m}$. For $p \equiv 1 \pmod{12}$, let ξ_m denote a root of $\xi_m^2 - \xi_m + 1 = 0$ over $\mathbb{Z}_{p^m}$. It is easily seen that $\chi_m \equiv \chi_1 \pmod{p}$ and $\xi_m \equiv \xi_1 \pmod{p}$ hold for any positive integer m.

Note that the multiplicative group $\mathbb{Z}_{2p^m}^\times \cong \mathbb{Z}_{p^m}^\times \times \mathbb{Z}_2^\times \cong \mathbb{Z}_{p^m}^\times$ is of order $\varphi(p^m) = p(p^{m-1} - 1)$, where $\mathbb{Z}_{p^m}^\times = \mathbb{Z}_{p^m} \setminus p\mathbb{Z}_{p^{m-1}} = (\mathbb{Z}_p \setminus \{0\}) + p\mathbb{Z}_{p^{m-1}}$ and

$$p\mathbb{Z}_{p^{m-1}} = p\mathbb{Z}/p^m\mathbb{Z} = \{p, 2p, \ldots, p(p^{m-1}-1)\} \pmod{p^m}.$$

Definition 2.3.1. For $t \in [m-1]$, let $h = \min\{t, m-t\}$. Define a group homomorphism $\psi_t : \mathbb{Z}_{p^{m-t}}^\times \to \mathbb{Z}_{p^h}^\times$ for any $x \in \mathbb{Z}_{p^{m-t}}^\times$, so that

$$\psi_t(x) \equiv x \pmod{p^h}.$$

Conversely, for any $y \in \mathbb{Z}_{p^h}^\times$, define

$$\psi_t^{-1}(y) = \{x \in \mathbb{Z}_{p^{m-t}}^\times \mid \psi_t(x) = y\}.$$

In particular, ψ_t is trivial if $m - t \le t$.

By means of the above homomorphism ψ_t, we define two specific subsets of $\mathbb{Z}_{p^{m-t}}^\times$, namely S_t and R_t, which provide important parameters in the recursive constructions below. In the rest of this subsection, we sum up a series of properties of S_t and R_t which allow us to get some partitions related to the multiplicative group $\mathbb{Z}_{p^{m-t}}^\times$.

Proposition 2.3.2. Let g be a generator of $\mathbb{Z}_{p^h}^{\times}$, where $h = \min\{t, m-t\}$. Let

$$S_t = \bigcup_{k=0}^{\frac{\varphi(p^h)}{2}-1} \psi_t^{-1}(g^k) \subset \mathbb{Z}_{p^{m-t}}^{\times}, \tag{2.23}$$

where ψ_t is defined as in Definition 2.3.1. Then,

(i) $|S_t| = \frac{\varphi(p^{m-t})}{2}$.

(ii) $S_t + p^t \equiv S_t \pmod{p^{m-t}}$.

(iii) $S_t \uplus (-S_t) = \mathbb{Z}_{p^{m-t}}^{\times}$.

Proof. First, we suppose $m - t \leq t$.

(i) This is straightforward by the definition.

(ii) This follows from $p^t \equiv 0 \pmod{p^{m-t}}$ under the assumption $t \geq m-t$.

(iii) Note that $-S_t = \{g_t^{k+\frac{\varphi(p^{m-t})}{2}} \mid k \in [0, \frac{\varphi(p^{m-t})}{2} - 1]\} = \{g_t^k \mid k \in [\frac{\varphi(p^{m-t})}{2}, \varphi(p^{m-t}) - 1]\}$. Hence $S_t \cap (-S_t) = \emptyset$. By combining with (i), the conclusion is straightforward.

Next, we suppose $m - t > t$.

(i) Note that ψ_t is a group homomorphism, hence $\left|\psi_t^{-1}(y)\right| = p^{m-2t}$. A direct calculation gives that $|S_t| = \frac{\varphi(p^t)}{2} p^{m-2t} = \frac{\varphi(p^{m-t})}{2}$.

(ii) This follows from $\psi_t^{-1}(y) + p^t = \psi_t^{-1}(y)$ for any $y \in \mathbb{Z}_{p^t}^{\times}$.

(iii) Since ψ_t is a group homomorphism, we have

$$-S_t = \biguplus_{k=0}^{\frac{\varphi(p^t)}{2}-1} \psi_t^{-1}(-g_{m-t}^k) = \biguplus_{k=\frac{\varphi(p^t)}{2}}^{\varphi(p^t)-1} \psi_t^{-1}(g_{m-t}^k)$$

which implies $S_t \uplus (-S_t) = \psi_t^{-1}(\mathbb{Z}_{p^t}^{\times}) = \mathbb{Z}_{p^{m-t}}^{\times}$. $\square$

Example 2.3.3. Let $p = 5$, $m = 3$, and $t = 1$. Then $S_1 = \psi^{-1}(1) \cup \psi^{-1}(2) = \{1, 6, 11, 16, 21\} \cup \{2, 7, 12, 17, 22\} \subset \mathbb{Z}_{5^2}^{\times}$.

Next, we introduce a function on $\mathbb{Z}_{p^{m-t}}^{\times}$ for our constructions (see Lemma 2.3.19 of Type IV base blocks).

Proposition 2.3.4. For $s \in \mathbb{Z}_{p^{m-t}}^{\times}$, let $\zeta(s) = s + c(2s - p^t)^{-1}sp^t$, where c is a constant in $\mathbb{Z}_{p^{m-t}}^{\times}$. Then $\{\zeta(s) \mid s \in S_t\} = S_t$.

Proof. If $m - t \leq t$, then $(2s - p^t)^{-1} \equiv (2s)^{-1} \pmod{p^{m-t}}$. Thus $\zeta(s) = s + 2^{-1}cp^t$. It follows from Proposition 2.3.2 (ii) that $\{\zeta(s) \mid s \in S_t\} = S_t + 2^{-1}cp^t = S_t$.

If $m - t > t$, then $\psi(\zeta(s)) = \psi(s)$ holds for every $s \in \mathbb{Z}^{\times}_{p^{m-t}}$. In words, $\zeta(s) \in \psi^{-1}(\psi(s)) \subseteq S_t$ holds for every $s \in S_t$, which implies $\{\zeta(s) \mid s \in S_t\} \subseteq S_t$. Then it suffices to show that $\zeta(s_1) \not\equiv \zeta(s_2)$ for any distinct $s_1, s_2 \in S_t$.

(a) If $s_1 \not\equiv s_2 \pmod{p^t}$, since $\zeta(s) \equiv s \pmod{p^t}$, we have $\zeta(s_1) \not\equiv \zeta(s_2) \pmod{p^t}$. More precisely, $\zeta(s_1) \not\equiv \zeta(s_2) \pmod{p^{m-t}}$.

(b) If $s_1 \equiv s_2 \pmod{p^t}$, then $s_1 = s_2 + \ell p^t$ for some $\ell \in [p^{m-2t} - 1]$. Assuming $\zeta(s_1) = \zeta(s_2)$, we have $\ell p^t + c(2s_1 - p^t)^{-1}s_1p^t \equiv c(2s_2 - p^t)^{-1}s_2p^t \pmod{p^{m-t}}$. Thus, $\ell + c(2 - s_1^{-1}p^t)^{-1} \equiv c(2 - s_2^{-1}p^t)^{-1} \pmod{p^{m-2t}}$, i.e.,

$$\ell(2 - s_1^{-1}p^t)(2 - s_2^{-1}p^t) \equiv c(s_2^{-1} - s_1^{-1})p^t \pmod{p^{m-2t}}.$$

Moreover, note that $s_2^{-1} - s_1^{-1} = (s_1 - \ell p^t)^{-1} - s_1^{-1} = \ell \sum_{k=1}^{\infty} s_1^{-k-1}\ell^{k-1}p^{kt}$, We finally derive

$$(2 - s_1^{-1}p^t)(2 - s_2^{-1}p^t) \equiv cp^{2t} \sum_{k=0}^{\infty} s_1^{-k-2}\ell^k p^{kt} \pmod{p^{m-2t-\iota}},$$

where ι is the non-negative integer satisfying $p^{\iota} = \gcd(\ell, p^{m-2t})$. It is clear that the left-hand side is invertible but the right-hand side is not, which leads to a contradiction. Therefore, $\zeta(s_1) \not\equiv \zeta(s_2) \pmod{p^{m-t}}$. $\square$

Let $H_0^{(t)}$ denote the multiplicative subgroup of $\mathbb{Z}^{\times}_{p^m}$ generated by $g_0^{\varphi(p^{m-t})}$. Then, we denote the cosets of $H_0^{(t)}$ by

$$H_a^{(t)} = g_0^a H_0^{(t)} = \left\{ g_0^{a+k\varphi(p^{m-t})} \,\middle|\, k \in [0, p^t - 1] \right\}. \tag{2.24}$$

Proposition 2.3.5. For any $x, y \in H_0^{(t)}$ and any $z \in H^{(t)}_{\frac{\varphi(p^{m-t})}{2}}$, the following hold:

(i) $x - y \equiv 0 \pmod{p^{m-t}}$.

(ii) $x + z \equiv 0 \pmod{p^{m-t}}$.

Proof. Suppose $x = g_0^{k_1\varphi(p^{m-t})}$, $y = g_0^{k_2\varphi(p^{m-t})}$, and $z = g_0^{k_3\varphi(p^{m-t}) + \frac{\varphi(p^{m-t})}{2}}$. Since $g_0^{\varphi(p^{m-t})} \equiv 1 \pmod{p^{m-t}}$, we have

$$g_0^{\varphi(p^{m-t})}p^t \equiv p^t \pmod{p^m} \quad \text{and} \quad g_0^{\frac{\varphi(p^{m-t})}{2}}p^t \equiv -p^t \pmod{p^m}.$$

Then,

(i) $xp^t - yp^t \equiv p^t - p^t \equiv 0 \pmod{p^m}$, which implies $x - y \equiv 0 \pmod{p^{m-t}}$;

(ii) $xp^t + zp^t \equiv p^t - p^t \equiv 0 \pmod{p^m}$, which implies $x + z \equiv 0 \pmod{p^{m-t}}$.

$\square$

Proposition 2.3.6. The following holds:

$$\left(\bigcup_{s\in S_t} sH_0^{(t)}\right)\bigcup\left(\bigcup_{s\in S_t} sH^{(t)}_{\frac{\varphi(p^{m-t})}{2}}\right) = \mathbb{Z}^{\times}_{p^m}.$$

Proof. Note that the left-hand side is a union of cosets, in which the number of cosets is $2\,|S_t| = \varphi(p^{m-t})$ and each coset is of size p^t. Hence it suffices to show those cosets are mutually disjoint. Clearly, for some given $s \in S_t$, $sH_0^{(t)}$ and $sH^{(t)}_{\frac{\varphi(p^{m-t})}{2}}$ never coincide. Now we give the proofs for the remaining cases by contradiction.

(a) For distinct $s_1, s_2 \in S_t$, assume $s_1H_0^{(t)} = s_2H_0^{(t)}$. There must exist $x, y \in H_0^{(t)}$, such that $s_1x \equiv s_2y \pmod{p^m}$. It is known by Proposition 2.3.5 (i) that there exists $r \neq 0$, such that $y = x + rp^{m-t}$. Hence, we have $s_1x \equiv s_2(x + rp^{m-t}) \pmod{p^m}$, i.e., $(s_1 - s_2)x \equiv s_2rp^{m-t} \pmod{p^m}$. Since x is invertible, there must be $s_1 - s_2 \equiv 0 \pmod{p^{m-t}}$. This is known to be impossible because s_1, s_2 are distinct in $\mathbb{Z}^{\times}_{p^{m-t}}$. In the same manner, it can be easily shown that $s_1H_a^{(t)} \neq s_2H_a^{(t)}$ for any given a and distinct $s_1, s_2 \in S_t$.

(b) For distinct $s_1, s_2 \in S_t$, assume $s_1H_0^{(t)} = s_2H^{(t)}_{\frac{\varphi(p^{m-t})}{2}}$. Then there exist $x \in H_0^{(t)}$ and $z \in H^{(t)}_{\frac{\varphi(p^{m-t})}{2}}$ so that $s_1x \equiv s_2z \pmod{p^m}$. By Proposition 2.3.5 (ii), we can suppose $z = rp^{m-t} - x$ for some r. Then we have $(s_1+s_2)x \equiv s_2rp^{m-t} \pmod{p^m}$ which implies $s_1+s_2 \equiv 0 \pmod{p^{m-t}}$. On one hand, $s_1 \in S_t$ requires $s_2 = -s_1 \in -S_t$, but on the other hand, $s_2 \in S_t$. It is known by Proposition 2.3.2 that $S_t \cap (-S_t) = \emptyset$, hence $s_1 + s_2 \equiv 0 \pmod{p^{m-t}}$ cannot hold for any distinct $s_1, s_2 \in S_t$. $\square$

For $p \equiv 1 \pmod{12}$, we introduce another subset of $\mathbb{Z}^{\times}_{p^{m-t}}$, which consists of one third of the elements of $\mathbb{Z}^{\times}_{p^{m-t}}$.

Proposition 2.3.7. Let g be a generator of $\mathbb{Z}^{\times}_{p^h}$, where $h = \min\{t, m-t\}$. Let

$$R_t = \left(\bigcup_{k=0}^{\frac{\varphi(p^h)}{6}-1} \psi_t^{-1}(g^k)\right)\bigcup\left(\bigcup_{k=\frac{\varphi(p^h)}{2}}^{\frac{2\varphi(p^h)}{3}-1} \psi_t^{-1}(g^k)\right) \subset \mathbb{Z}^{\times}_{p^{m-t}}, \tag{2.25}$$

where ψ_t is defined as in Definition 2.3.1. Then,

(i) $|R_t| = \frac{\varphi(p^{m-t})}{3}$.

(ii) $R_t + p^t \equiv R_t \pmod{p^{m-t}}$.

(iii) $R_t \cupdot \xi_m^2 R_t \cupdot \xi_m^4 R_t = \mathbb{Z}_{p^{m-t}}^\times$.

Proof. We omit the proofs of (i) and (ii), because they are the same as the proofs of Proposition 2.3.2. By recalling that $\xi_m^2 \equiv g_t^{\frac{\varphi(p^{m-t})}{3}} \pmod{p^{m-t}}$ and $\xi_m^2 \equiv g_{m-t}^{\frac{\varphi(p^t)}{3}} \pmod{p^t}$, we prove (iii) in the following two cases:

For the first case, suppose $m - t \leq t$. Let

$$I = [0, \tfrac{\varphi(p^{m-t})}{6} - 1] \cup [\tfrac{\varphi(p^{m-t})}{2}, \tfrac{2\varphi(p^{m-t})}{3} - 1]$$

denote a subset of $\mathbb{Z}_{\varphi(p^{m-t})}$, then $I \cup (I + \frac{\varphi(p^{m-t})}{3}) \cup (I + \frac{2\varphi(p^{m-t})}{3}) = \mathbb{Z}_{\varphi(p^{m-t})}$, which implies $R_t \cup \xi_m^2 R_t \cup \xi_m^4 R_t = \{g_t^k \mid k \in \mathbb{Z}_{\varphi(p^{m-t})}\} = \mathbb{Z}_{p^{m-t}}^\times$.

For the second case, suppose $m - t > t$. Let

$$T = \left\{ g_{m-t}^k \,\middle|\, k \in [0, \tfrac{\varphi(p^t)}{6} - 1] \cup [\tfrac{\varphi(p^t)}{2}, \tfrac{2\varphi(p^t)}{3} - 1] \right\}.$$

In the same manner as the first case, we have $T \cup \xi_m^2 T \cup \xi_m^4 T = \mathbb{Z}_{p^t}^\times$. Moreover, since ψ is a group homomorphism, we obtain $R_t \cup \xi_m^2 R_t \cup \xi_m^4 R_t = \psi^{-1}(\mathbb{Z}_{p^t}^\times) = \mathbb{Z}_{p^{m-t}}^\times$. By combining with (i), it is easy to see they are mutually disjoint. □

Next, we define a function on $\mathbb{Z}_{p^{m-t}}^\times$ for our constructions when $p \equiv 1 \pmod{12}$ (see Lemma 2.3.20 for Type III$^\xi$ base blocks and Lemma 2.3.24 for Type II$^\xi$ base blocks). The coefficient $\sqrt{-3}$ is considered as an element in $\mathbb{Z}_{p^{m-t}}^\times$ whose square is -3. Note that there are two elements satisfying the above condition, hence we should choose $\sqrt{-3}$ as in $\xi_m = \frac{1+\sqrt{-3}}{2}$. Without loss of generality, here we set $\sqrt{-3} = 2\xi_m - 1$.

Proposition 2.3.8. Let $\vartheta(s) = (3 - \sqrt{-3}sp^t)^{-1}s$. Then

$$\bigcupdot_{s \in R_t} \left\{\vartheta(s), \xi_m^2 \vartheta(s), \xi_m^4 \vartheta(s)\right\} = \mathbb{Z}_{p^{m-t}}^\times.$$

Proof. Let $R_t^* = \bigcup_{s \in R_t} \{s^{-1}\}$. It is easy to see that $R_t^* = \xi_m^2 R_t$. By Proposition 2.3.7 (ii), we have $R_t^* + p^t = R_t^*$. Then,

$$\bigcup_{s \in R_t} \{3\vartheta(s)\} = \bigcup_{s^* \in R_t^*} \left\{ \left(s^* - \tfrac{\sqrt{-3}}{3} p^t\right)^{-1} \right\} = \bigcup_{s^{**} \in R_t^*} \left\{ (s^{**})^{-1} \right\} = R_t.$$

Furthermore, it follows from Proposition 2.3.7 (iii) that

$$\bigcup_{s \in R_t} \left\{\vartheta(s), \xi_m^2 \vartheta(s), \xi_m^4 \vartheta(s)\right\} = 3^{-1}(R_t \cup \xi_m^2 R_t \cup \xi_m^4 R_t) = \mathbb{Z}_{p^{m-t}}^\times.$$

□

Proposition 2.3.9. For any $t \in [m-1]$,

$$\bigcupdot_{s \in R_t} C(\xi_m + sp^t) = \{\xi_m, 1-\xi_m\} + p^t \mathbb{Z}_{p^{m-t}}^{\times}.$$

Proof. For any $s \in \mathbb{Z}_{p^{m-t}}^{\times}$, there are three elements in $C(\xi_m + sp^t)$ which are congruent to ξ_m modulo p^t, namely, $\xi_m + sp^t$, $1-(\xi_m+sp^t)^{-1}$, and $(1-\xi_m - sp^t)^{-1}$. Let

$$\begin{aligned}
W_1 &= \bigcup_{s \in R_t} \{\xi_m + sp^t\}, \\
W_2 &= \bigcup_{s \in R_t} \{1-(\xi_m + sp^t)^{-1}\}, \text{ and} \\
W_3 &= \bigcup_{s \in R_t} \{(1-\xi_m - sp^t)^{-1}\}
\end{aligned}$$

be three subsets of $\xi_m + p^t\mathbb{Z}_{p^{m-t}}^{\times}$ with the same size $\frac{\varphi(p^{m-t})}{3}$. Now we proof their disjointness by contradiction. Assume there exist $s_1, s_2, s_3 \in R_t$, such that at least one of the following holds:

$$\begin{aligned}
&\xi_m + s_1p^t = 1-(\xi_m + s_2p^t)^{-1}, \\
&1-(\xi_m + s_2p^t)^{-1} = (1-\xi_m - s_3p^t)^{-1}, \\
&(1-\xi_m - s_3p^t)^{-1} = \xi_m + s_1p^t,
\end{aligned}$$

which are equivalent to

$$s_1 \equiv \xi_m^4 s_2 + \xi_m^2 s_1 s_2 p^t \pmod{p^{m-t}}, \tag{2.26}$$
$$s_2 \equiv \xi_m^4 s_3 + \xi_m^2 s_2 s_3 p^t \pmod{p^{m-t}}, \tag{2.27}$$
$$s_3 \equiv \xi_m^4 s_1 + \xi_m^2 s_3 s_1 p^t \pmod{p^{m-t}}. \tag{2.28}$$

Without loss of generality, we assume (2.26) holds. Then we have

$$\psi_t(s_1) \equiv \psi_t(\xi_m^4)\psi_t(s_2) \pmod{p^h}, \tag{2.29}$$

where $h = \min\{t, m-t\}$. Here $\psi_t(\xi_m^4)$ can be regarded as the $\frac{2\varphi(p^h)}{3}$-th power of the generator of $\mathbb{Z}_{p^h}^{\times}$. However, for $I = [0, \frac{\varphi(p^h)}{6} - 1] \cup [\frac{\varphi(p^h)}{2}, \frac{2\varphi(p^h)}{3} - 1] \subset \mathbb{Z}_{\varphi(p^h)}$, $I \cap (I + \frac{2\varphi(p^h)}{3}) = \emptyset$ must hold. Therefore, the congruence (2.29) cannot hold. This proves the disjointness of W_1 and W_2. In the same manner, it can be shown that W_1, W_2, and W_3 are mutually disjoint. Hence, $\{W_1, W_2, W_3\}$ forms a partition of $\xi_m + p^t\mathbb{Z}_{p^{m-t}}^{\times}$. As a direct consequence, $\{1-W_1, 1-W_2, 1-W_3\}$

forms a partition of $1-\xi_m-p^t\mathbb{Z}^\times_{p^{m-t}}=(1-\xi_m)+p^t\mathbb{Z}^\times_{p^{m-t}}$, where

$$1-W_1=\bigcup_{s\in R_t}\{1-\xi_m-sp^t\},$$
$$1-W_2=\bigcup_{s\in R_t}\{(\xi_m+sp^t)^{-1}\},$$
$$1-W_3=\bigcup_{s\in R_t}\{1-(1-\xi_m-sp^t)^{-1}\},$$

which are also subsets of $\bigcup_{s\in R_t}C(\xi_m+sp^t)$. □

2.3.2 Recursive construction A

In this subsection, we provide a recursive construction for an AsSQS$(2p^m)$ based on AsSQS$^A(2p)$. We denote the resulting sSQS by AsSQS$^A(2p^m)$.

Construction 2.3.10. Assume that both an AsSQS$^A(2p)$ and an AsSQS$^A(2p^{m-1})$ have been constructed, then the base blocks of an AsSQS$^A(2p^m)$ can be obtained as follows:

(i) For the cases of prime $p\equiv 1$ or $5 \pmod{12}$, we have the base blocks as follows:

Type I′: $\{0,1;\chi_m,1-\chi_m\}$;

Type I: $\{0,1;b_i+sp^{m-1},1-(b_i+sp^{m-1})\}$ for $i\in[\frac{p-5}{4}]$ and $s\in[0,p-1]$;

Type II′: $\{0,1,-1+sp^{m-1};sp^{m-1}\}$ for $s\in[0,\frac{p-1}{2}]$;

Type IV: $\{0,p^t,s_t;\chi_m s_t+(2s_t-p^t)^{-1}(1-\chi_m)p^t s_t\}$ for $t\in[m-1]$ and $s_t\in S_t$, where S_t is defined by (2.23);

Type V: $pB \pmod{p^m}$ for every base block B of an AsSQS$(2p^{m-1})$.

(ii) If $p\equiv 5 \pmod{12}$, we additionally have

Type III: $\{0,1,a_i+sp^{m-1},1-(a_i+sp^{m-1})\}$ for $i\in[\frac{p-5}{12}]$ and $s\in[0,p-1]$;

(iii) If $p\equiv 1 \pmod{12}$, we additionally have

Type III: $\{0,1,a_i+sp^{m-1},1-(a_i+sp^{m-1})\}$ for $i\in[\frac{p-13}{12}]$ and $s\in[0,p-1]$;

Type III$^\xi$: $\{0,1,\xi_m,\overline{\xi_m}\}$ and $\{0,1,\xi_m+s_tp^t,\overline{\xi_m}+(3-\sqrt{-3}s_tp^t)^{-1}s_tp^t\}$ for $s_t\in R_t$, where R_t is defined by (2.25).

Example 2.3.11. Let $p=5$ and $m=2$. Take $\chi_m=4$. The base blocks are given as follows:

Type I′: $\{0,1;4,22\}$,

Type II′: $\{0,1,24;0\}$, $\{0,1,4;5\}$, $\{0,1,9;10\}$, Type IV: $\{0,5,1;9\}$, $\{0,5,2;13\}$,

Type V: $\{0,5;10,20\}$, $\{0,5,20;0\}$.

Example 2.3.12. Let $p = 5$ and $m = 3$. Take $\chi_m = 29$. The base blocks are given as follows:

Type I$'$: $\{0,1;29,97\}$,

Type II$'$: $\{0,1,124;0\}$, $\{0,1,24;25\}$, $\{0,1,49;50\}$,

Type IV: $\{0,5,1;34\}$, $\{0,5,6;54\}$, $\{0,5,11;74\}$, $\{0,5,16;94\}$, $\{0,5,21;114\}$, $\{0,5,2;88\}$, $\{0,5,7;108\}$, $\{0,5,12;3\}$, $\{0,5,17;23\}$, $\{0,5,22;43\}$, $\{0,25,1;54\}$, $\{0,25,2;83\}$,

Type V: $5B \pmod{125}$ for every $B \in \mathcal{B}$, where $\mathcal{B}$ consists of all base blocks listed in Example 2.3.11.

It is clear that every pure triple is a member of $\mathcal{O}_A(\{0,1,a\})$ for some a, and every mixed triple is a member of $\mathcal{O}_A(\{0,1;b\})$ for some b. Now we begin to prove that every pure or mixed triple can be covered exactly once in $\mathcal{O}_A(B)$ for some base block B in Construction 2.3.10.

Lemma 2.3.13 (Type I$'$)**.** *There are exactly two mixed triples containing* $\{0,1\}$ *covered by* $\mathcal{O}_A(\{0,1;\chi_m,1-\chi_m\})$*, namely,* $\{0,1;\chi_m\}$ *and* $\{0,1;1-\chi_m\}$*.*

Proof. Note that χ_m is a root of $2\chi_m^2 - 2\chi_m + 1 = 0$ over $\mathbb{Z}_{p^m}$, hence $\overline{\chi_m} = \chi_m$. Therefore, $\mathrm{orb}_{\boldsymbol{AC}}(\chi_m) = \{\chi_m, 1-\chi_m\}$ and $\mathcal{O}_A(\{0,1;\chi_m,1-\chi_m\})$ covers only two mixed triples containing $\{0,1\}$. $\square$

Lemma 2.3.14 (Type I)**.** *Let* $B_1(b_i,s) = \{0,1;b_i+sp^{m-1},1-(b_i+sp^{m-1})\}$*. Then,* $\bigcup_{i=1}^{\frac{p-5}{4}} \bigcup_{s=0}^{p-1} \mathcal{O}_A(B_1(b_i,s))$ *covers each mixed triple in*

$$\left\{\{0,1;y\} \,\middle|\, y \in (\mathbb{Z}_p \setminus \{0,1,2^{-1},\chi_m,1-\chi_m\}) + p\mathbb{Z}_{p^{m-1}}\right\}$$

exactly once.

Proof. Given b_i and s, $\mathcal{O}_A(B_1(b_i,s))$ covers four mixed triples containing $\{0,1\}$ exactly once, that is, $\left\{\{0,1;y\} \,\middle|\, y \in \mathrm{orb}_{\boldsymbol{AC}}(b_i+sp^{m-1})\right\}$. Thus, it suffices to prove the disjointness of $\mathrm{orb}_{\boldsymbol{AC}}(b_{i_1}+s_1p^{m-1})$ and $\mathrm{orb}_{\boldsymbol{AC}}(b_{i_2}+s_2p^{m-1})$ for any distinct pairs (i_1,s_1) and (i_2,s_2). First, when $i_1 \neq i_2$, assume $\mathrm{orb}_{\boldsymbol{AC}}(b_{i_1}+sp^{m-1})$ and $\mathrm{orb}_{\boldsymbol{AC}}(b_{i_2}+sp^{m-1})$ coincide, then $\mathrm{orb}_{\boldsymbol{AC}}(b_{i_1}+sp^{m-1}) \equiv \mathrm{orb}_{\boldsymbol{AC}}(b_{i_2}+sp^{m-1}) \pmod{p}$, i.e., $\mathrm{orb}_{\boldsymbol{AC}}(b_{i_1}) \equiv \mathrm{orb}_{\boldsymbol{AC}}(b_{i_2}) \pmod{p}$, which contradicts Lemma 2.2.2. Next, when $s_1 \neq s_2$, assume $\mathrm{orb}_{\boldsymbol{AC}}(b_i+s_1p^{m-1})$ and $\mathrm{orb}_{\boldsymbol{AC}}(b_i+s_2p^{m-1})$ coincide, then one of the following must hold:

(a) $b_i + s_1p^{m-1} = 1-(b_i+s_2p^{m-1})$,

(b) $b_i + s_1p^{m-1} = -(b_i+s_2p^{m-1})(1-2(b_i+s_2p^{m-1}))^{-1}$,

(c) $b_i + s_1p^{m-1} = (1-(b_i+s_2p^{m-1}))(1-2(b_i+s_2p^{m-1}))^{-1}$, which implies $b_i \equiv 2^{-1}$, $b_i \equiv 0$ or 1, and $b_i \equiv \chi_1$ or $1-\chi_1 \pmod p$, respectively. This again contradicts Lemma 2.2.2. $\square$

Lemma 2.3.15 (Type II$'$). *Let $B_2(s) = \{0, 1, -1 + sp^{m-1}; sp^{m-1}\}$ for $s \in [0, \frac{p-1}{2}]$. Then, $\bigcup_{s=0}^{\frac{p-1}{2}} \mathcal{O}_A(B_2(s))$ covers the pure triple $\{0, 1, x\}$ for every $x \in \{-1, 2, 2^{-1}\} + p\mathbb{Z}_{p^{m-1}}$ and the mixed triple $\{0, 1; y\}$ for every $y \in \{0, 1, 2^{-1}\} + p\mathbb{Z}_{p^{m-1}}$ exactly once.*

Proof. By acting proper affine transformations on $B_2(s)$, we obtain all quadruples containing $\{0, 1\}$ in $\mathcal{O}_A(B_2(s))$ as follows:

$$\begin{aligned}
&\{0, 1, -1 + sp^{m-1}; sp^{m-1}\}, \{0, -1 - sp^{m-1}, 1; -sp^{m-1}\},\\
&\{1, 0, 2 - sp^{m-1}; 1 - sp^{m-1}\}, \{1, 2 + sp^{m-1}, 0; 1 + sp^{m-1}\},\\
&\{\tfrac{1}{2} - \tfrac{1}{4}sp^{m-1}, 1, 0; \tfrac{1}{2} + \tfrac{1}{4}sp^{m-1}\}, \{\tfrac{1}{2} + \tfrac{1}{4}sp^{m-1}, 0, 1; \tfrac{1}{2} - \tfrac{1}{4}sp^{m-1}\}.
\end{aligned}$$

It is readily checked that the pure triples arising from these base blocks cover $\big\{\{0, 1, x\} \,\big|\, x \in \{-1, 2, 2^{-1}\} + p\mathbb{Z}_{p^{m-1}}\big\}$ exactly once, and the mixed triples cover $\big\{\{0, 1; y\} \,\big|\, y \in \{0, 1, 2^{-1}\} + p\mathbb{Z}_{p^{m-1}}\big\}$ exactly once. $\square$

Lemma 2.3.16. *Let $(x_1, s_1), (x_2, s_2)$ be distinct pairs in $\mathbb{Z}_p \times [0, p-1]$. Assume $C(x_1), C(x_2) \notin \{C(0), C(-1), C(\xi_1)\}$. Moreover, assume $\overline{C}(x_1)$ and $\overline{C}(x_2)$ are disjoint if $x_1 \neq x_2$. Then, $\overline{C}(x_1 + s_1p^{m-1})$ and $\overline{C}(x_2 + s_2p^{m-1})$ are disjoint.*

Proof. Firstly, suppose $x_1 \neq x_2$. If $\overline{C}(x_1+s_1p^{m-1})$ and $\overline{C}(x_2+s_2p^{m-1})$ intersect, then $\overline{C}(x_1+s_1p^{m-1})$ and $\overline{C}(x_2+s_2p^{m-1}) \pmod p$ must intersect, which implies $\overline{C}(x_1) \cap \overline{C}(x_2) \neq \emptyset$ and contradicts the assumption. Secondly, suppose $x_1 = x_2 = x$ and $s_1 \neq s_2$. Assume $\overline{C}(x + s_1p^{m-1})$ and $\overline{C}(x + s_2p^{m-1})$ intersect. Without loss of generality, assume $C(x + s_1p^{m-1}) = C(x + s_2p^{m-1})$. Then we can derive that x must be in $\{\infty, 2^{-1}, 1, -1, \xi_1, 1 - \xi_1, 0, 2\}$ which is contrary to the assumption. To sum up, $\overline{C}(x_1 + s_1p^{m-1})$ and $\overline{C}(x_2 + s_2p^{m-1})$ must be disjoint. $\square$

Lemma 2.3.17 (Type III). *Let $B_3(a_i, s) = \{0, 1, a_i + sp^{m-1}, 1 - (a_i + sp^{m-1})\}$ for $s \in [0, p-1]$. Then, $\bigcup_{i=1}^{\ell_p} \bigcup_{s=0}^{p-1} \mathcal{O}_A(B_3(a_i, s))$ covers every pure triple in*

$$\big\{\{0, 1, x\} \,\big|\, x \in (\mathbb{Z}_p \setminus \Theta) + p\mathbb{Z}_{p^{m-1}}\big\}$$

exactly once, where

$$\ell_p := \begin{cases} \frac{p-5}{12}, & \text{if } p \equiv 5 \pmod{12}, \\ \frac{p-13}{12}, & \text{if } p \equiv 1 \pmod{12}, \end{cases} \quad \text{and}$$

$$\Theta := \begin{cases} \{0, 1, -1, 2, 2^{-1}\}, & \text{if } p \equiv 5 \pmod{12}, \\ \{0, 1, -1, 2, 2^{-1}\} \cup \overline{C}(\xi_m), & \text{if } p \equiv 1 \pmod{12}. \end{cases}$$

Proof. It is known that $\mathcal{O}_A(B_3(a_i,s))$ covers the pure triple $\{0,1,x\}$ for every $x \in \overline{C}(a_i+sp^{m-1})$. First, $C(a_i+sp^{m-1})$ and $C(\overline{a_i+sp^{m-1}})$ must be disjoint by Lemma 2.2.4. Moreover, note that a_i's satisfy the assumptions in Lemma 2.3.16 by Lemma 2.2.4. Thus, we can conclude the disjointness of $\overline{C}(a_{i_1}+s_1p^{m-1})$ and $\overline{C}(a_{i_2}+s_2p^{m-1})$ for any distinct pairs $\{i_1,s_1\}$ and $\{i_2,s_2\}$. Therefore, we have

$$\bigcupdot_{s=0}^{p-1}\bigcupdot_{i=1}^{\ell}\overline{C}(a_i+sp^{m-1}) \subseteq (\mathbb{Z}_p\setminus\Theta)+p\mathbb{Z}_{p^{m-1}}. \tag{2.30}$$

Furthermore, both the left-hand side and the right-hand side of (2.30) have cardinalities $12\ell p^{m-1}$, which completes the proof. □

Lemma 2.3.18 (Type IV)**.** *Let S_t be the subset defined in* (2.23)*. Denote $\alpha=\chi_m$, $\beta=1-\chi_m$, and $B_2^{(t)}(s_t)=\{0,p^t,s_t;\alpha s_t+(2s_t-p^t)^{-1}\beta p^t s_t\}$ for $t\in[m-1]$ and $s_t\in S_t$. Then, $\bigcup_{t=1}^{m-1}\bigcup_{s_t\in S_t}\mathcal{O}_A(B_2^{(t)}(s_t))$ covers the pure triple $\{0,1,x\}$ for every $x\in\big(\{0,1\}+p\mathbb{Z}_{p^{m-1}}\}\big)\setminus\{0,1\}$, and the mixed triple $\{0,1;y\}$ for every $y\in\big(\{\alpha,\beta\}+p\mathbb{Z}_{p^{m-1}}\}\big)\setminus\{\alpha,\beta\}$ exactly once.*

Proof. We exhaustively list all the quadruples containing $\{0,1\}$ in $\mathcal{O}_A(B_2^{(t)}(s_t))$ as follows:

$$B_2^{(t)}(s_t)\times s_t^{-1}=\{0,s_t^{-1}p^t,1;\alpha+(2s_t-p^t)^{-1}\beta p^t\},$$
$$(B_2^{(t)}(s_t))-p^t)\times(s_t-p^t)^{-1}=\{-(s_t-p^t)^{-1}p^t,0,1;\alpha-(2s_t-p^t)^{-1}\beta p^t\},$$
$$B_2^{(t)}(s_t)\times(-s_t^{-1})+1=\{1,1-s_t^{-1}p^t,0;\beta-(2s_t-p^t)^{-1}\beta p^t\},$$
$$(p^t-B_2^{(t)}(s_t))\times(s_t-p^t)^{-1}+1=\{1+(s_t-p^t)^{-1}p^t,1,0;\beta+(2s_t-p^t)^{-1}\beta p^t\}.$$

Each pure triple in

$$\big\{\{0,1,x\}\,\big|\,x\in\{s_t^{-1}p^t,-(s_t-p^t)^{-1}p^t,1-s_t^{-1}p^t,1+(s_t-p^t)^{-1}p^t\}\big\}$$

is covered exactly once in $\mathcal{O}_A(B_2^{(t)}(s_t))$. By Proposition 2.3.2,

$$\{s_t^{-1},-(s_t-p^t)^{-1}\pmod{p^{m-t}}\mid s_t\in S_t\}=S_t\cup(-S_t)=\mathbb{Z}_{p^{m-t}}^{\times}.$$

Therefore, for each $t\in[m-1]$ and each $s_t\in S_t$, the pure triple $\{0,1,x\}$ is covered exactly once for every

$$x\in\bigcup_{t=1}^{m-1}\Big(\{0,1\}+p^t\mathbb{Z}_{p^{m-t}}^{\times}\Big)=\big(\{0,1\}+p\mathbb{Z}_{p^{m-1}}\}\big)\setminus\{0,1\}.$$

Each mixed triple in

$$\big\{\{0,1;y\}\,\big|\,y\in\{\alpha\pm(2s_t-p^t)^{-1}\beta p^t,\beta\pm(2s_t-p^t)^{-1}\beta p^t\}\big\}$$

is covered exactly once in $\mathcal{O}_A(B_2^{(t)}(s_t))$. By Proposition 2.3.2,

$$\{\pm(2s_t-p^t)^{-1}\pmod{p^{m-t}}\mid s_t\in S_t\}=\mathbb{Z}_{p^{m-t}}^{\times}.$$

Therefore, for each $t \in [m-1]$ and each $s_t \in S_t$, the mixed triple $\{0, 1; y\}$ is covered exactly once for every

$$y \in \bigcup_{t=1}^{m-1} \left(\{\alpha, \beta\} + p^t \mathbb{Z}_{p^{m-t}}^{\times} \right) = \left(\{\alpha, \beta\} + p\mathbb{Z}_{p^{m-1}} \} \right) \setminus \{\alpha, \beta\}.$$

□

Lemma 2.3.19 (Type IV)**.** *For a given $t \in [m-1]$, $\bigcup_{s_t \in S_t} \mathcal{O}_A(B_2^{(t)}(s_t))$ covers the pure triple $\{0, p^t, x_t\}$ for every $x_t \in \mathbb{Z}_{p^m}^{\times}$, and the mixed triple $\{0, p^t; y_t\}$ for every $y_t \in \mathbb{Z}_{p^m}^{\times}$ exactly once.*

Proof. Let g_0 be a generator of $\mathbb{Z}_{p^m}^{\times}$. We denote $q = p^{m-t}$. Let

$$\begin{aligned} Q_1(s, u) =& B_2^{(t)}(s) \times g_0^{u\varphi(q)}, \\ =& \left\{ 0, p^t, g_0^{u\varphi(q)} s; g_0^{u\varphi(q)} \left(\alpha s + \beta (2s - p^t)^{-1} s p^t \right) \right\}, \\ Q_2(s, u) =& (B_2^{(t)}(s) - p^t) \times g_0^{u\varphi(q) + \frac{\varphi(q)}{2}}, \\ =& \left\{ p^t, 0, g_0^{\frac{\varphi(q)}{2} + u\varphi(q)} (s - p^t); g_0^{\frac{\varphi(q)}{2} + u\varphi(q)} \left(\alpha s + \beta (2s - p^t)^{-1} s p^t - p^t \right) \right\} \end{aligned}$$

for $u \in [0, p^t - 1]$ and $s \in S_t$, where the second equalities of $Q_1(s, u)$ and $Q_2(s, u)$ follow from $p^t g_0^{\varphi(q)} \equiv p^t \pmod{p^m}$ and $p^t g_0^{\frac{\varphi(q)}{2}} \equiv -p^t \pmod{p^m}$, respectively.

Let $H_0^{(t)}$ denote the multiplicative subgroup of $\mathbb{Z}_{p^m}^{\times}$ generated by $g_0^{\varphi(q)}$ and denote the cosets of $H_0^{(t)}$ by $H_a^{(t)} = g_0^a H_0^{(t)}$.

First, consider the pure triples containing $\{0, p^t\}$ in $Q_1(s, u)$ and $Q_2(s, u)$. Let

$$U_1 = \bigcup_{s \in S_t} \bigcup_{u=0}^{p^t - 1} \left\{ g_0^{u\varphi(q)} s \right\} = \bigcup_{s \in S_t} s H_0^{(t)}, \tag{2.31}$$

$$U_2 = \bigcup_{s \in S_t} \bigcup_{u=0}^{p^t - 1} \left\{ g_0^{\frac{\varphi(q)}{2} + u\varphi(q)} (s - p^t) \right\} = \bigcup_{s \in S_t} (s - p^t) H_{\frac{\varphi(q)}{2}}^{(t)}. \tag{2.32}$$

Furthermore, it follows from Proposition 2.3.2 (ii) that,

$$U_2 = \bigcup_{s \in S_t} (s - p^t) H_{\frac{\varphi(q)}{2}}^{(t)} = \bigcup_{s' \in S_t} s' H_{\frac{\varphi(q)}{2}}^{(t)}. \tag{2.33}$$

Then it follows from Proposition 2.3.6 that $U_1 \cup U_2 = \mathbb{Z}_{p^m}^{\times}$. Therefore, the pure triple $\{0, p^t, x_t\}$ for every $x_t \in \mathbb{Z}_{p^m}^{\times}$ is covered in $\bigcup_{s_t \in S_t} \mathcal{O}_A(B_2^{(t)}(s_t))$.

Then, consider the mixed triples containing $\{0, p^t\}$ in $Q_1(s,u)$ and $Q_2(s,u)$. Let $\zeta(s) = s + \alpha^{-1}\beta(2s - p^t)^{-1}sp^t$. Since $\zeta(s)$ is independent from u, we denote

$$\begin{aligned} U_1(s) =& \alpha\zeta(s) \bigcup_{u=0}^{p^t-1} \left\{ g_0^{u\varphi(q)} \right\} = \alpha\zeta(s) H^0_{(t)}, \\ U_2(s) =& (\alpha\zeta(s) - p^t) \bigcup_{u=0}^{p^t-1} \left\{ g_0^{\frac{\varphi(q)}{2} + u\varphi(q)} \right\} = (\alpha\zeta(s) - p^t) H_{(t)}^{\frac{\varphi(q)}{2}}. \end{aligned}$$

Furthermore, by Proposition 2.3.4, we have

$$\begin{aligned} U_1 &= \bigcup_{s \in S_t} U_1(s) = \bigcup_{s' \in S_t} \alpha s' H^0_{(t)}, \\ U_2 &= \bigcup_{s \in S_t} U_2(s) = \bigcup_{s'' \in S_t} \alpha s'' H_{(t)}^{\frac{\varphi(q)}{2}} \end{aligned}$$

It follows from Proposition 2.3.6 again that $\bigcup_{s_t \in S_t} \mathcal{O}_A(B_2^{(t)}(s_t))$ covers the mixed triple $\{0, p^t; y_t\}$ for every $y_t \in U_1 \cup U_2 = \alpha\mathbb{Z}^\times_{p^m} = \mathbb{Z}^\times_{p^m}$. In addition, since all the unions in this proof are between cosets, each pure or mixed triple we considered is covered exactly once. □

Lemma 2.3.20 (Type III$^\xi$)**.** *For $p \equiv 1 \pmod{12}$, let $B^{(t)}(s_t) = \{0, 1, \xi_m + s_t p^t, \overline{\xi_m} + (3 - \sqrt{-3} s_t p^t)^{-1} s_t p^t\}$. Then, $\bigcup_{t=1}^{m-1} \bigcup_{s_t \in S_t} \mathcal{O}_A(B^{(t)}(s_t))$ covers each pure triple of the form $\{0, 1, x\}$ for $x \in \left(\overline{C}(\xi_m) + p\mathbb{Z}_{p^{m-1}}\right) \setminus \overline{C}(\xi_m)$ exactly once.*

Proof. For a given s, denote

$$x(s) = \xi_m + sp^t \quad \text{and} \quad y(s) = \overline{\xi_m} + \vartheta(s)p^t,$$

where $\vartheta(s) = (3 - \sqrt{-3}sp^t)^{-1}s$. It can be verified that all pure triples containing $\{0, 1\}$ covered by $\mathcal{O}_A(B^{(t)}(s))$ are

$$\left\{ \{0, 1, a\} \,\middle|\, a \in C(x(s)) \cup C(y(s)) \cup C\left(\frac{1 - y(s)}{1 - x(s)}\right) \cup C\left(\frac{x(s) - y(s)}{x(s)}\right) \right\}.$$

On the one hand, it is shown in Proposition 2.3.9 that

$$\bigcup_{s \in R_t} C(x(s)) = C(\xi_m) + p^t \mathbb{Z}^\times_{p^{m-t}}.$$

On the other hand, we observe that

$$\left\{ y(s), \frac{1 - y(s)}{1 - x(s)}, \frac{x(s) - y(s)}{x(s)} \right\} = \overline{\xi_m} + \left\{ \vartheta(s)p^t, \xi_m^2 \vartheta(s)p^t, \xi_m^4 \vartheta(s)p^t \right\}. \quad (2.34)$$

For some $C(v)$ satisfying $C(v) \equiv C(\overline{\xi_m}) \pmod{p^t}$, each of the six elements of $C(v)$ are distinct by modulo p^t. Hence, for distinct $v_1, v_2 \in \mathbb{Z}_{p^m}$, if $v_1 \equiv v_2 \equiv \overline{\xi_m}$

(mod p^t), then $C(v_1) \equiv C(v_2) \equiv C(\overline{\xi_m}) \pmod{p^t}$ must hold, and $C(v_1)$ must be disjoint from $C(v_2)$. In particular, there is only one element w in $C(v)$ such that $w \equiv \overline{\xi_m} \pmod{p^t}$. Now, we choose $y(s)$, $\frac{1-y(s)}{1-x(s)}$ and $\frac{x(s)-y(s)}{x(s)}$ as representatives of their cross-ratio classes, and then show that

$$\bigcup_{s \in R_t} \left\{ y(s), \frac{1-y(s)}{1-x(s)}, \frac{x(s)-y(s)}{x(s)} \right\} = \overline{\xi_m} + p^t \mathbb{Z}^\times_{p^{m-t}}, \tag{2.35}$$

which implies that

$$\bigcup_{s \in R_t} \left(C(y(s)) \cup C\left(\frac{1-y(s)}{1-x(s)}\right) \cup C\left(\frac{x(s)-y(s)}{x(s)}\right)\right) = C(\overline{\xi_m}) + p^t \mathbb{Z}^\times_{p^{m-t}}.$$

(2.35) can be easily shown by replacing the left-hand side with (2.34) and then applying Proposition 2.3.8. In addition, since $3\,|R_t| = \left|\mathbb{Z}'_{p^{m-t}}\right|$, the number of appearances in $\mathcal{O}_A(B^{(t)}(s))$ of every such pure triple is exactly one. □

It remains to consider the pure and mixed triples containing $\{0, p^t\}$ for every $t \in [m-1]$. We complete this case by the following lemma without proof, since it is straightforward by the definition of an AsSQS.

Lemma 2.3.21 (Type V). *Let $(\mathbb{Z}_{p^{m-1}} \times \mathbb{Z}_2, \mathcal{B})$ be an AsSQS. For each $t \in [m-1]$, $\{pB \pmod{p^m} \mid B \in \mathcal{B}\}$ covers the pure triple $\{0, p^t, x_t\}$ for every $x_t \in p\mathbb{Z}_{p^{m-1}} \setminus \{0, p^t\}$ and the mixed triple $\{0, p^t; y_t\}$ for every $y_t \in p\mathbb{Z}_{p^{m-1}}$.*

We summarize the above lemmas of AsSQS$^A(2p^m)$ in Table 2.6, Table 2.7 and Table 2.8. In conclusion, if an AsSQS$(2p)$ exists, we can sequentially construct an AsSQS$(2p^2)$, an AsSQS$(2p^3)$, ..., an AsSQS$(2p^m)$ for any positive integer m.

Table 2.6: Triples containing $\{0, 1\}$ in an AsSQS$^A(2p^m)$ for $p \equiv 5 \pmod{12}$

Type	Pure triples $\{0, 1, x\}$, for all x in the following set	Mixed triples $\{0, 1; y\}$, for all y in the following set	Lemmas
I′		$\{\alpha, \beta\}$	2.3.13
I		$\mathbb{Z}_p \backslash \{0, 1, 2^{-1}, \chi, 1-\chi\} + p\mathbb{Z}_{p^{m-1}}$	2.3.14
II′	$\{-1, 2, 2^{-1}\} + p\mathbb{Z}_{p^{m-1}}$	$\{0, 1, 2^{-1}\} + p\mathbb{Z}_{p^{m-1}}$	2.3.15
III	$\mathbb{Z}_p \backslash \{0, 1, -1, 2, 2^{-1}\} + p\mathbb{Z}_{p^{m-1}}$		2.3.17
IV	$(\{0, 1\} + p\mathbb{Z}_{p^{m-1}}) \setminus \{0, 1\}$	$(\{\alpha, \beta\} + p\mathbb{Z}_{p^{m-1}}) \setminus \{\alpha, \beta\}$	2.3.18
Union	$\mathbb{Z}_{p^m} \setminus \{0, 1\}$	$\mathbb{Z}_{p^m}$	

2.3.3 Recursive construction B

In this subsection, we introduce a recursive construction for an AsSQS$(2p^m)$ based on an AsSQS$^B(2p)$, denoted by AsSQS$^B(2p^m)$. It is remarkable that any

Table 2.7: Triples containing $\{0,1\}$ in an $\mathrm{AsSQS}^A(2p^m)$ for $p \equiv 1 \pmod{12}$

Type	Pure triples $\{0,1,x\}$, for all x in the following set	Mixed triples $\{0,1;y\}$, for all y in the following set	Lemmas
I′		$\{\alpha,\beta\}$	2.3.13
I		$\mathbb{Z}_p \backslash \{0,1,2^{-1},\chi,1-\chi\} + p\mathbb{Z}_{p^{m-1}}$	2.3.14
II′	$\{-1,2,2^{-1}\} + p\mathbb{Z}_{p^{m-1}}$	$\{0,1,2^{-1}\} + p\mathbb{Z}_{p^{m-1}}$	2.3.15
III	$\mathbb{Z}_p \backslash (\{0,1,-1,2,2^{-1}\} \cup \overline{C}(\xi_m)) + p\mathbb{Z}_{p^{m-1}}$		2.3.17
III^{ξ}	$\overline{C}(\xi_m) + p\mathbb{Z}_{p^{m-1}}$		2.3.20
IV	$(\{0,1\} + p\mathbb{Z}_{p^{m-1}}) \setminus \{0,1\}$	$(\{\alpha,\beta\} + p\mathbb{Z}_{p^{m-1}}) \setminus \{\alpha,\beta\}$	2.3.18
Union	$\mathbb{Z}_{p^m} \setminus \{0,1\}$	$\mathbb{Z}_{p^m}$	

Table 2.8: Triples containing $\{0,p^t\}$ in an $\mathrm{AsSQS}^A(2p^m)$

Type	Pure triples $\{0,p^t,x_t\}$, for $t \in [m-1]$	Mixed triples $\{0,p^t;y_t\}$, for $t \in [m-1]$	Lemmas
IV	$x_t \in \mathbb{Z}_{p^m}^{\times}$	$y_t \in \mathbb{Z}_{p^m}^{\times}$	2.3.19
V	$x_t \in p\mathbb{Z}_{p^{m-1}} \setminus \{0,p^t\}$	$y_t \in p\mathbb{Z}_{p^{m-1}}$	2.3.21
Union	$x_t \in \mathbb{Z}_{p^m} \setminus \{0,p^t\}$	$y_t \in \mathbb{Z}_{p^m}$	

$\mathrm{AsSQS}^B(2p)$ is 2-chromatic, accordingly, an $\mathrm{AsSQS}^B(2p^m)$ is also 2-chromatic if all Type V base blocks in Construction 2.3.22 come from an $\mathrm{AsSQS}^B(2p^{m-1})$.

Construction 2.3.22. Assume both an $\mathrm{AsSQS}^B(2p)$ and an $\mathrm{AsSQS}^B(2p^{m-1})$ have been constructed, the base blocks of an $\mathrm{AsSQS}^B(2p^m)$ can be obtained as follows:

(i) For the cases of prime $p \equiv 1$ or $5 \pmod{12}$, we have the base blocks as follows:

Type I′: $\{0,1;\chi_m,1-\chi_m\}$,

Type II′: $\{0,1,-1+sp^{m-1};sp^{m-1}\}$ for $s \in [0,\frac{p-1}{2}]$,

Type IV: $\{0,p^t,s_t;\chi_m s_t + (2s_t-p^t)^{-1}(1-\chi_m)p^t s_t\}$ for $t \in [m-1]$ and $s_t \in S_t$, where S_t is defined by (2.23),

Type V: $pB \pmod{p^m}$ for every base block B of an $\mathrm{AsSQS}(2p^{m-1})$;

(ii) If $p \equiv 5 \pmod{12}$, we additionally have

Type II: $\{0,1,a_i+sp^{m-1};b_i+sp^{m-1}\}$ for $s \in [0,p-1]$ and $i \in [\frac{p-5}{6}]$;

(iii) If $p \equiv 1 \pmod{12}$, we additionally have

Type II^{ξ}: $\{0,1,\xi_m;\overline{\xi_m}\}$ and $\{0,1,\xi_m+s_tp^t;\overline{\xi_m}+(3-\sqrt{-3}s_tp^t)^{-1}s_tp^t\}$ for $t \in [m-1]$ and $s_t \in R_t$, where R_t is defined by (2.25),

Table 2.9: Triples containing $\{0,1\}$ in an $\mathrm{AsSQS}^B(2p^m)$ for $p \equiv 5 \pmod{12}$

Type	Pure triples $\{0,1,x\}$, for all x in the following set	Mixed triples $\{0,1;y\}$, for all y in the following set	Lemmas
I′		$\{\alpha,\beta\}$	2.3.13
II′	$\{-1,2,2^{-1}\}+p\mathbb{Z}_{p^{m-1}}$	$\{0,1,2^{-1}\}+p\mathbb{Z}_{p^{m-1}}$	2.3.15
II	$\mathbb{Z}_p\backslash\{0,1,-1,2,2^{-1}\}+p\mathbb{Z}_{p^{m-1}}$	$\mathbb{Z}_p\backslash\{0,1,2^{-1},\chi,1-\chi\}+p\mathbb{Z}_{p^{m-1}}$	2.3.23 (i)
IV	$(\{0,1\}+p\mathbb{Z}_{p^{m-1}})\setminus\{0,1\}$	$(\{\alpha,\beta\}+p\mathbb{Z}_{p^{m-1}})\setminus\{\alpha,\beta\}$	2.3.18
Union	$\mathbb{Z}_{p^m}\setminus\{0,1\}$	$\mathbb{Z}_{p^m}$	

Type II: $\{0,1,a_i+sp^{m-1};b_i+sp^{m-1}\}$ for $s\in[0,p-1]$ and $i\in[\frac{p-7}{6}]$.

Types I′, II′, IV, and V are exactly the same as those in Construction 2.3.10, hence we omit the proofs. For Type II base blocks, by a direct calculation which is analogous to the proof of Lemmas 2.3.14 and 2.3.17, we state the following:

Lemma 2.3.23 (Type II). *Let $B_2^s(a_i,b_i)=\{0,1,a_i+sp^{m-1};b_i+sp^{m-1}\}$.*

(i) For $p \equiv 5 \pmod{12}$, $\bigcup_{i=1}^{\frac{p-5}{6}}\bigcup_{s=0}^{p-1}\mathcal{O}_A(B_2^s(a_i,b_i))$ covers the pure triple $\{0,1,x\}$ for every

$$x\in\big(\mathbb{Z}_p\setminus\{0,1,-1,2,2^{-1}\}\big)+p\mathbb{Z}_{p^{m-1}},$$

and the mixed triple $\{0,1;y\}$ for every

$$y\in\big(\mathbb{Z}_p\setminus\{0,1,2^{-1},\chi_m,1-\chi_m\}\big)+p\mathbb{Z}_{p^{m-1}}.$$

(ii) For $p \equiv 1 \pmod{12}$, $\bigcup_{i=1}^{\frac{p-7}{6}}\bigcup_{s=0}^{p-1}\mathcal{O}_A(B_2^s(a_i,b_i))$ covers the pure triple $\{0,1,x\}$ for every

$$x\in\big(\mathbb{Z}_p\setminus\{0,1,-1,2,2^{-1},\xi_m,1-\xi_m\}\big)+p\mathbb{Z}_{p^{m-1}},$$

and the mixed triple $\{0,1;y\}$ for every

$$y\in\big(\mathbb{Z}_p\setminus\{0,1,2^{-1},\chi_m,1-\chi_m,\overline{\xi_m},1-\overline{\xi_m}\}\big)+p\mathbb{Z}_{p^{m-1}}.$$

In summary, for $p \equiv 5 \pmod{12}$, Table 2.9 lists all types of base blocks whose orbits cover the triples of the form $\{0,1,x\}$ and $\{0,1;y\}$. The triples of the form $\{0,p^t,x_t\}$ and $\{0,p^t;y_t\}$ are shown in Table 2.8.

Moreover, for $p \equiv 1 \pmod{12}$, $\mathcal{O}_A(\{0,1,\xi_m;\overline{\xi_m}\})$ covers pure triples $\{0,1,\xi_m\}$, $\{0,1,1-\xi_m\}$ and mixed triples $\{0,1;\overline{\xi_m}\}$, $\{0,1;1-\overline{\xi_m}\}$.

Lemma 2.3.24 (Type II$^\xi$). *Let $B^{(t)}(s_t)=\{0,1,\xi_m+s_tp^t;\overline{\xi_m}+(3-\sqrt{-3}s_tp^t)^{-1}s_tp^t\}$ for each $s_t\in R_t$, where R_t is defined as in (2.25). Then, $\bigcup_{t=1}^{m-1}\bigcup_{s_t\in S_t}\mathcal{O}_A(B^{(t)}(s_t))$ covers the pure triple $\{0,1,x\}$ for every*

$$x\in\{\xi_m,1-\xi_m\}+p\mathbb{Z}_{p^{m-1}}\setminus\{\xi_m,1-\xi_m\}$$

and the mixed triple $\{0,1;y\}$ *for every*

$$y \in \{\overline{\xi_m}, 1-\overline{\xi_m}\} + p\mathbb{Z}_{p^{m-1}} \setminus \{\overline{\xi_m}, 1-\overline{\xi_m}\}$$

exactly once.

Proof. Note that $\bigcup_{t=1}^{m-1} p^t\mathbb{Z}_{p^{m-t}}^{\times} = p\mathbb{Z}_{p^{m-1}} \setminus \{0\}$. Thus, it suffices to prove, for each $t \in [m-1]$, $\bigcup_{s_t\in R_t} \mathcal{O}_A(B^{(t)}(s_t))$ covers every triple in

$$\left\{\{0,1;y\} \,\middle|\, y \in \{\overline{\xi_m}, 1-\overline{\xi_m}\} + p^t\mathbb{Z}_{p^{m-t}}^{\times}\right\} \cup$$
$$\left\{\{0,1,x\} \,\middle|\, x \in \{\xi_m, 1-\xi_m\} + p^t\mathbb{Z}_{p^{m-t}}^{\times}\right\}$$

exactly once. Denote $\vartheta(s_t) = (3-\sqrt{-3}s_tp^t)^{-1}s_t$ for $s_t \in R_t$. By tedious calculations we yield all the six quadruples containing $\{0,1\}$ in $\mathcal{O}_A(B^{(t)}(s_t))$, namely,

$$\{0,1,\xi_m+s_tp^t;\overline{\xi_m}+\vartheta(s_t)p^t\}, \tag{2.36}$$
$$\{0,(\xi_m+s_tp^t)^{-1},1;1-\overline{\xi_m}-\xi_m^4\vartheta(s_t)p^t\}, \tag{2.37}$$
$$\{1,1-(\xi_m+s_tp^t)^{-1},0;\overline{\xi_m}+\xi_m^4\vartheta(s_t)p^t\}, \tag{2.38}$$
$$\{1,0,1-\xi_m-s_tp^t;1-\overline{\xi_m}-\vartheta(s_t)p^t\}, \tag{2.39}$$
$$\{(1-\xi_m-s_tp^t)^{-1},0,1;\overline{\xi_m}+\xi_m^2\vartheta(s_t)p^t\}, \tag{2.40}$$
$$\{1-(1-\xi_m-s_tp^t)^{-1},1,0;1-\overline{\xi_m}-\xi_m^2\vartheta(s_t)p^t\}. \tag{2.41}$$

We first consider the mixed triples. For a fixed s_t, we can collect all the mixed triples contained in the quadruples (2.36)-(2.41), given by

$$\left\{\{0,1;y\} \,\middle|\, y \in (\overline{\xi_m}+U(s_t)) \cup (1-\overline{\xi_m}-U(s_t))\right\},$$

where $U(s_t) = \{\vartheta(s_t), \xi_m^2\vartheta(s_t), \xi_m^4\vartheta(s_t)\}$. It follows from Proposition 2.3.8 that $\bigcup_{s_t\in R_t}(-U(s_t)) = \bigcup_{s_t\in R_t} U(s_t) = \mathbb{Z}_{p^{m-t}}^{\times}$. Therefore, for a certain $t \in [m-1]$, $\bigcup_{s_t\in S_t} \mathcal{O}_A(B_{s_t}^{(t)})$ covers the mixed triple $\{0,1;y\}$ for every $y \in \{\overline{\xi_m}, 1-\overline{\xi_m}\} + p^t\mathbb{Z}_{p^{m-t}}^{\times}$.

Next, all pure triples contained in the quadruples (2.36)-(2.41) are given by

$$\left\{\{0,1,x\} \,\middle|\, x \in C(\xi_m+s_tp^t)\right\}.$$

It follows from Proposition 2.3.9 that

$$\bigcup_{s_t\in R_t} C(\xi_m+s_tp^t) = \{\xi_m, 1-\xi_m\} + p^t\mathbb{Z}_{p^{m-t}}^{\times}.$$

Therefore, for a certain t, $\bigcup_{s_t\in S_t} \mathcal{O}_A(B^{(t)}(s_t))$ covers the pure triple $\{0,1,x\}$ for every $x \in \{\xi_m, 1-\xi_m\} + p^t\mathbb{Z}_{p^{m-t}}^{\times}$. $\square$

In summary, for $p \equiv 1 \pmod{12}$, Table 2.10 lists all types of base blocks whose orbits cover the triples of the form $\{0,1,x\}$ and $\{0,1;y\}$.

Table 2.10: Triples containing $\{0,1\}$ in an $\mathrm{AsSQS}^B(2p^m)$ for $p \equiv 1 \pmod{12}$

Type	Pure triples $\{0,1,x\}$, for all x in the following set	Mixed triples $\{0,1;y\}$, for all y in the following set	Lemmas
I′		$\{\alpha,\beta\}$	2.3.13
II′	$\{-1,2,2^{-1}\}+p\mathbb{Z}_{p^{m-1}}$	$\{0,1,2^{-1}\}+p\mathbb{Z}_{p^{m-1}}$	2.3.15
II^{ξ}	$\{\xi_m,1-\xi_m\}+p\mathbb{Z}_{p^{m-1}}$	$\{\overline{\xi_m},1-\overline{\xi_m}\}+p\mathbb{Z}_{p^{m-1}}$	2.3.24
II	$\mathbb{Z}_p\backslash\{0,1,-1,2,2^{-1},\xi_m,1-\xi_m\}$ $+p\mathbb{Z}_{p^{m-1}}$	$\mathbb{Z}_p\backslash\{0,1,2^{-1},\chi_m,1-\chi_m,\overline{\xi_m},1-\overline{\xi_m}\}$ $+p\mathbb{Z}_{p^{m-1}}$	2.3.23 (b)
IV	$(\{0,1\}+p\mathbb{Z}_{p^{m-1}})\setminus\{0,1\}$	$(\{\chi,1-\chi\}+p\mathbb{Z}_{p^{m-1}})\setminus\{\alpha,\beta\}$	2.3.18
Union	$\mathbb{Z}_{p^m}\setminus\{0,1\}$	$\mathbb{Z}_{p^m}$	

2.4 A necessary condition for the existence of affine-invariant strictly cyclic Steiner quadruple systems

Recall that $n \equiv 1,5 \pmod{12}$ is necessary for the existence of an sSQS($2n$). A natural question arises: Is there any further requirement for an AsSQS($2n$)? For example, it is known that an sSQS(98) exists (see [44] Example 7.7). Also, Example 2.2.24 gives an "affine-invariant" SQS(98) over $\mathbb{F}_{49} \oplus \mathbb{F}_2$, which is not cyclic. Although we cannot construct an AsSQS(98) by our constructions, it would be interesting if it did exist. Now, we give a negative answer as follows:

Theorem 2.4.1. *If there exists an AsSQS*$(2n)$*, then every prime factor p of n must satisfy* $p \equiv 1,5 \pmod{12}$.

Proof. The necessary condition $n \equiv 1,5 \pmod{12}$ implies that all the prime factors of n are congruent to $1,5,7,11$ modulo 12. Thus it suffices to prove that n does not have a prime factor p with $p \equiv 7,11 \pmod{12}$.

Assume $n = p^\alpha q$, where $\alpha \geq 1$ and q is coprime with p. We consider the quadruple containing $\{0,p,kp\}$ with $k \not\equiv 0,1 \pmod{p^{\alpha-1}q}$. First, we suppose $B = \{0,p,kp,s\}$, where $s \not\equiv 0 \pmod{p}$. Then, we can denote $s = a + bp$, for some $a \in \mathbb{Z}_p^\times$ and $b \in \mathbb{Z}_{p^{\alpha-1}q}$. Let $\lambda = 1 + cp^{\alpha-1}q$ be an element in $\mathbb{Z}_n^\times$ for some $c \in \mathbb{Z}_p^\times$. Then $\lambda p \equiv p \pmod{n}$ holds. Moreover, $\lambda s - s = (\lambda-1)s = cp^{\alpha-1}q(a+bp) \equiv acp^{\alpha-1}q \not\equiv 0 \pmod{n}$ holds. Therefore, B and λB are distinct and both of them contain the triple $\{0,p^\alpha,ap^\alpha\}$. Hence it suffices to consider the case when $B = \{0,p,kp,lp\}$, where $l \not\equiv 0,1,k \pmod{p^{\alpha-1}q}$. This is equivalent to saying $\{0,1,k,l\}$ is a base block of an AsSQS($2p^{\alpha-1}q$). By repeatedly applying this strategy, we can see that the existence of an AsSQS($2n$) requires that an AsSQS($2p$) exists for every prime divisor p of n. □

As an open problem and for future work, we are also interested in the existence of an affine-invariant SQS($2^{\alpha_0}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}$) which is not necessarily strictly cyclic, where $p_i \equiv 1,5 \pmod{12}$ is prime for every $i \in [r]$. It is also a challenge to consider packing designs and covering designs in the same manner for applications.

2.5 Affine-invariant two-fold quadruple systems over $\mathbb{Z}_p$

This section is devoted to providing a direct construction of an affine-invariant TQS (two-fold quadruple system) via the graphs $\mathrm{CG}(\Omega_p)$. Roughly speaking, by removing a 1-factor from $\mathrm{CG}(\Omega_p)$, the resulting graph leads to the base blocks of an affine-invariant $\mathrm{TQS}(p)$.

Construction 2.5.1. For prime $p \equiv 5 \pmod{12}$, suppose $\mathrm{CG}(\Omega_p)$ has a 1-factor, say F. Let $\ell = \frac{p-5}{6}$ and let $a_1, a_2, \dots, a_\ell$ be elements in Ω_q such that

$$\big\{\{C(a_1), C(\overline{a_1})\}, \{C(a_2), C(\overline{a_2})\}, \dots, \{C(a_\ell), C(\overline{a_\ell})\}\big\} = E(\mathrm{CG}(\Omega_q)) \setminus E(F),$$

where $E(\mathrm{CG}(\Omega_q))$ and $E(F)$ denote the edge set of $\mathrm{CG}(\Omega_q)$ and F, respectively. Then

$$\mathcal{B} = \big\{B_{a_i} = \{0, 1, a_i, 1 - a_i\} \mid i \in [\ell]\big\} \cup \{B_{-1}\}.$$

is the set of base blocks of an affine-invariant $\mathrm{TQS}(p)$.

Theorem 2.5.2. *An affine-invariant* $\mathrm{TQS}(p)$ *exists if the graph* $\mathrm{CG}(\Omega_p)$ *has a 1-factor.*

Proof. As shown in the proof of Lemma 2.2.4 for Type III base blocks of $\mathrm{AsSQS}^A(2p)$, $\mathcal{O}_A(B_{a_i})$ covers all triples of the form $\{0, 1, x\}$ for $x \in C(a_i) \cup C(\overline{a_i})$ if $C(a_i) \neq C(\overline{a_i})$. It is shown in Proposition 2.1.10 (ii) that all the vertices of $\mathrm{CG}(\Omega_q)$ are of degree 3 except $C(3)$ and $C(\mu)$ for $q \equiv 5 \pmod{12}$. Hence, the multiset union of all the non-loop edges in $E(\mathrm{CG}(\Omega_q)) \setminus E(F)$ covers all the vertices of $\mathrm{CG}(\Omega_q)$ twice except $C(3)$, $C(\chi)$, and $C(\mu)$, where each of $C(3)$ and $C(\chi)$ occurs once, and $C(\mu)$ does not appear.

Moreover, by Proposition 2.1.10 (i), $C(a_i) = C(\overline{a_i})$ if and only if $C(a_i) = C(\chi)$ or $C(\mu)$, where $\chi = \frac{1+\sqrt{-1}}{2}$ satisfies $\chi = \chi^{\sigma_C}$ and $\mu = \frac{3+\sqrt{5}}{2}$ satisfies $\mu^{\sigma_B} = \mu^{\sigma_C}$ (cf. Table 2.1). In these cases, we can explicitly derive all the blocks containing $\{0, 1\}$ in $\mathcal{O}_A(B_\chi)$ and $\mathcal{O}_A(B_\mu)$, namely,

$$\begin{aligned}
&\{0, 1, \chi, 1-\chi\}, \left\{0, \tfrac{1}{\chi}, 1, \tfrac{\chi}{\chi-1}\right\}, \left\{1, \tfrac{\chi-1}{\chi}, 0, \tfrac{1}{1-\chi}\right\}, \text{ and} \\
&\{0, 1, \mu, 1-\mu\}, \left\{0, \tfrac{1}{\mu}, 1, \tfrac{1}{1-\mu}\right\}, \left\{1, \tfrac{\mu-1}{\mu}, 0, \tfrac{\mu}{\mu-1}\right\}, \\
&\left\{0, \tfrac{1}{1-\mu}, 1-\mu, 1\right\}, \left\{1, \tfrac{\mu}{\mu-1}, \mu, 0\right\}, \left\{\tfrac{1}{\mu}, \tfrac{\mu-1}{\mu}, 1, 0\right\},
\end{aligned}$$

in which every element of $C(\chi)$ occurs once and every element of $C(\mu)$ occurs twice.

Last, all the blocks containing $\{0, 1\}$ in $\mathcal{O}_A(B_{-1})$ are

$$\{0, 1, -1, 2\}, \{0, -1, 1, -2\}, \{0, \tfrac{1}{2}, -\tfrac{1}{2}, 1\}, \{1, 2^{-1}, \tfrac{3}{2}, 0\}, \{2, 1, 3, 0\}, \{\tfrac{2}{3}, \tfrac{1}{3}, 1, 0\},$$

where each element of $C(2)$ occurs twice and each element of $C(3)$ occurs once.

Summing up the elements being covered in the above three cases, we observe that every element of $\Omega_q \cup C(2)$, that is $\mathbb{F}_q \setminus \{0,1\}$, appears twice. Therefore, $\bigcup_{B \in \mathcal{B}} \mathcal{O}_A(B)$ covers all triples of the form $\{0,1,x\}$ twice for every $x \in \mathbb{F}_q \setminus \{0,1\}$. □

Example 2.5.3. Let $p = 29$. Then B_{-1}, B_{14}, B_4, B_{25}, B_9 are the base blocks of an affine-invariant TQS(p), where the last four blocks respectively correspond to the edges $\{C(3), C(4)\}$, $\{C(4), C(9)\}$, $\{C(5)\}$ (a self-loop), $\{C(9)\}$ (a self-loop) of CG(Ω_{29}) illustrated in Figure 2.5 (cf. Figure 2.2).

2.6 Affine-invariant two-fold quadruple systems over $\mathbb{Z}_{p^m}$

In this section, we construct an affine-invariant TQS(p^m) via the affine-invariant TQS(p) obtained from Construction 2.5.1.

Let χ_t denote a root of $2\chi_t^2 - 2\chi_t + 1 = 0$ over $\mathbb{Z}_{p^t}$ for $t \in [1, m]$. Let μ_t denote a root of $\mu_t^2 - 3\mu_t + 1 = 0$ over $\mathbb{Z}_{p^t}$ for $t \in [1, m]$. Let $B_s(a) = \{0, 1, a + sp^{m-1}, 1 - (a + sp^{m-1})\}$.

Construction 2.6.1. Suppose $p \equiv 5 \pmod{12}$ is prime. We use the same notation with Construction 2.5.1. Assume that both an affine-invariant TQS(p) and an affine-invariant TQS(p^{m-1}) have been constructed, then the base blocks of an affine-invariant TQS(p^m) can be obtained as follows:

Type I: $B_s(a_i)$ for $i \in [\frac{p-5}{6}]$ and $s \in [0, p-1]$;

Type II: $B_s(-1)$ for $s \in [0, p-1]$;

Type III: $B_s(\chi_m)$ for $s \in [0, \frac{p-1}{2}]$;

Type IV: $B_s(\mu_m)$ for $s \in [0, p-1]$, if $p \equiv 29, 41 \pmod{60}$;

Type V: $\{0, p^t, s_t, s_t + p^t\}$, for $t \in [m-1]$ and $s_t \in S_t$, where S_t is defined by (2.23);

Type VI: $pB \pmod{p^m}$, for all base blocks B of the affine-invariant TQS(p^{m-1}).

Lemma 2.6.2. *For a fixed $a \in \Omega_p \setminus (C(\chi_1) \cup C(\mu_1))$, $\bigcup_{s=0}^{p-1} \mathcal{O}_A(B_s(a))$ covers $\{0,1,x\}$ exactly once for every $x \in \overline{C}(a) + p\mathbb{Z}_{p^{m-1}}$.*

Proof. It suffices to show $\bigcup_{s=0}^{p-1} \overline{C}(a + sp^{m-1}) = \overline{C}(a) + p\mathbb{Z}_{p^{m-1}}$. First, $C(a + sp^{m-1})$ and $C(\overline{a + sp^{m-1}})$ are clearly disjoint. By Lemma 2.3.16, $\overline{C}(a + s_1 p^{m-1})$ and $\overline{C}(a + s_2 p^{m-1})$ are disjoint if $s_1 \neq s_2$. Therefore, we have

$$\dot{\bigcup_{s=0}^{p-1}} \overline{C}(a + sp^{m-1}) \subseteq \overline{C}(a) + p\mathbb{Z}_{p^{m-1}}.$$

Furthermore, both the left-hand side and the right-hand side have cardinalities $12p^{m-1}$, which completes the proof. □

In the same manner, we can easily obtain the following lemmas.

Lemma 2.6.3. $\bigcup_{s=0}^{p-1} \mathcal{O}_A(B_s(-1))$ *covers* $\{0,1,x\}$ *once for every* $x \in C(3) + p\mathbb{Z}_{p^{m-1}}$ *and twice for every* $x \in C(2) + p\mathbb{Z}_{p^{m-1}}$.

Proof. It is easy to check that $\mathcal{O}_A(B_s(-1))$ covers $\{0,1,x\}$ for $x \in C(-1 + sp^{m-1}) \cup C(3+sp^{m-1})$. Then we can complete the proof by noting that $C(-1+sp^{m-1}) = \{-1 \pm sp^{m-1}, 2 \pm sp^{m-1}, 2^{-1} \pm 2^{-1}sp^{m-1}\}$ and $C(3 + sp^{m-1}) = \{3+sp^{m-1}, -2-sp^{m-1}, -\frac{1}{2}+\frac{1}{4}sp^{m-1}, \frac{3}{2}-\frac{1}{4}sp^{m-1}, \frac{2}{3}+\frac{1}{9}sp^{m-1}, \frac{1}{3}-\frac{1}{9}sp^{m-1}\}$. $\square$

Lemma 2.6.4. $\bigcup_{s=0}^{\frac{p-1}{2}} \mathcal{O}_A(B_s(\chi_m))$ *covers* $\{0,1,x\}$ *once for every* $x \in C(\chi_1) + p\mathbb{Z}_{p^{m-1}}$.

Proof. Note that $\overline{\chi_m + sp^{m-1}} = \chi_m - sp^{m-1}$. Hence

$$\bigcup_{s=1}^{\frac{p-1}{2}} \{C(\chi_m + sp^{m-1}), C(\overline{\chi_m + sp^{m-1}})\} = \bigcup_{s=1}^{p-1} \{C(\chi_m + sp^{m-1})\}.$$

Therefore, $\bigcup_{s=1}^{\frac{p-1}{2}} \mathcal{O}_A(B_s(\chi_m))$ covers $\{0,1,x\}$ once for every $x \in C(\chi_m) + p(\mathbb{Z}_{p^{m-1}} \setminus \{0\})$. In addition, it is known that $\mathcal{O}_A(B_0(\chi_m))$ covers $\{0,1,x\}$ once for every $x \in C(\chi_m)$. Thus, $\bigcup_{s=0}^{\frac{p-1}{2}} \mathcal{O}_A(B_s(\chi_m))$ covers $\{0,1,x\}$ once for every $x \in C(\chi_m) + p\mathbb{Z}_{p^{m-1}} = C(\chi_1) + p\mathbb{Z}_{p^{m-1}}$. $\square$

Lemma 2.6.5. $\bigcup_{s=0}^{p-1} \mathcal{O}_A(B_s(\mu_m))$ *covers* $\{0,1,x\}$ *twice for every* $x \in C(\mu_1) + p\mathbb{Z}_{p^{m-1}}$.

Proof. Note that $C(\overline{\mu_m + sp^{m-1}}) = C(\mu_m - \mu_m^{-1}sp^{m-1})$. Moreover, $\mathcal{O}_A(B_0(\mu_m))$ covers $\{0,1,x\}$ twice for each $x \in C(\mu_m)$. Therefore, $\bigcup_{s=0}^{p-1} \mathcal{O}_A(B_s(\mu_m))$ covers $\{0,1,x\}$ twice for every $x \in C(\mu_m) + p\mathbb{Z}_{p^{m-1}} = C(\mu_1) + p\mathbb{Z}_{p^{m-1}}$. $\square$

Lemma 2.6.6 (Type I, II, III, IV)**.** *Let* $\mathcal{O}_1 = \bigcup_{i=1}^{\frac{p-5}{6}} \bigcup_{s=0}^{p-1} \mathcal{O}_A(B_s(a_i))$, $\mathcal{O}_2 = \bigcup_{s=0}^{p-1} \mathcal{O}_A(B_s(-1))$, $\mathcal{O}_3 = \bigcup_{s=0}^{\frac{p-1}{2}} \mathcal{O}_A(B_s(\chi_m))$, *and* $\mathcal{O}_4 = \bigcup_{s=0}^{p-1} \mathcal{O}_A(B_s(\mu_m))$. *Then* $\bigcup_{k=1}^{4} \mathcal{O}_k$ *covers* $\{0,1,x\}$ *twice for every* $x \in (\mathbb{Z}_p \setminus \{0,1\}) + p\mathbb{Z}_{p^{m-1}}$.

Proof. It follows from Construction 2.5.1 and Lemma 2.6.2 that $\mathcal{O}_1$ covers $\{0,1,x\}$ exactly twice for every $x \in (\mathbb{Z}_p \setminus (C(0) \cup C(2) \cup C(3) \cup C(\chi_1) \cup C(\mu_1)) + p\mathbb{Z}_{p^{m-1}}$ and exactly once for $x \in C(3) + p\mathbb{Z}_{p^{m-1}}$. It can be immediately concluded, by combining Lemmas 2.6.3, 2.6.4, and 2.6.5, that $\bigcup_{k=1}^{4} \mathcal{O}_k$ covers $\{0,1,x\}$ twice for every $x \in (\mathbb{Z}_p \setminus \{0,1\}) + p\mathbb{Z}_{p^{m-1}}$. $\square$

Lemma 2.6.7 (Type V)**.** *Let* $B_{s_t}^{(t)} = \{0, p^t, s_t, s_t + p^t\}$. *Then* $\bigcup_{s_t \in S_t} \mathcal{O}_A(B_{s_t}^{(t)})$ *covers* $\{0,1,x\}$ *exactly twice for every* $x \in \big(\{0,1\} + p\mathbb{Z}_{p^{m-1}}\}\big) \setminus \{0,1\}$.

Proof. There are four distinct blocks containing $\{0,1\}$ in $\mathcal{O}_A(B_{s_t}^{(t)})$.

$$\begin{aligned}
B' =& B_{s_t}^{(t)} \times s_t^{-1} = \{0, s_t^{-1}p^t, 1, 1+s_t^{-1}p^t\}, && (2.42)\\
\tilde{B}' =& B' \times (1+s_t^{-1}p^t)^{-1} = \{0, p^t(s_t+p^t)^{-1}, (1+s_t^{-1}p^t)^{-1}, 1\}, && (2.43)\\
B'' =& (B_{s_t}^{(t)} - p^t) \times (s_t - p^t)^{-1} = \{p^t(-s_t+p^t)^{-1}, 0, 1, (1-s_t^{-1}p^t)^{-1}\}, && (2.44)\\
\tilde{B}'' =& B'' \times (1 - s_t^{-1}p^t) = \{-s_t^{-1}p^t, 0, 1-s_t^{-1}p^t, 1\}, && (2.45)
\end{aligned}$$

where $\tilde{B}'' = 1 - B'$, $\tilde{B}' = 1 - \tilde{B}'$, and $B'' = 1 - B''$. Moreover, we have $(1 \pm s_t^{-1}p^t)^{-1} - 1 = -p^t(\pm s_t + p^t)^{-1}$. Recall Proposition 2.3.2 (ii) and (iii) that $S_t + p^t \equiv S_t \pmod{p^{m-t}}$ and $S_t \uplus (-S_t) = \mathbb{Z}_{p^{m-t}}^\times$. Hence,

$$\begin{aligned}
&\{s_t^{-1} \mid s_t \in S_t\} \cup \{-s_t^{-1} \mid s_t \in S_t\} = \mathbb{Z}_{p^{m-t}}^\times \text{ and}\\
&\{(s_t+p^t)^{-1} \mid s_t \in S_t\} \cup \{(-s_t+p^t)^{-1} \mid s_t \in S_t\} = \mathbb{Z}_{p^{m-t}}^\times.
\end{aligned}$$

Therefore, for any given $t \in [m-1]$, the union of all the triples containing $\{0,1\}$ in (2.42)-(2.45) extended over $s_t \in S_t$ covers $\left\{\{0,1,x\} \mid x \in \{0,1\} + p^t\mathbb{Z}_{p^{m-t}}^\times\right\}$ twice. Furthermore, by $\bigcup_{t=1}^{m-1}\left(\{0,1\} + p^t\mathbb{Z}_{p^{m-t}}^\times\right) = \left(\{0,1\} + p\mathbb{Z}_{p^{m-1}}\}\right) \setminus \{0,1\}$, the proof is completed. $\square$

Lemma 2.6.8 (Type V)**.** *For any fixed $t \in [m-1]$, $\bigcup_{s_t \in S_t} \mathcal{O}_A(B_{s_t}^{(t)})$ covers $\{0, p^t, x\}$ exactly twice for every $x \in \mathbb{Z}_{p^m}^\times$.*

Proof. The idea is the same as the proof of Lemma 2.3.19 for Type IV base blocks of AsSQS$^A(2p^m)$. Let g_0 be a generator of $\mathbb{Z}_{p^m}^\times$ and simply denote $q = p^{m-t}$. For a given $s \in S_t$, we can derive the blocks containing $\{0, p^t\}$ in $\mathcal{O}_A(B_s^{(t)})$ as follows: Let

$$\begin{aligned}
Q_1(s,u) =& B_2^{(t)}(s) \times g_0^{u\varphi(q)} = \left\{0, p^t, g_0^{u\varphi(q)}s, p^t + g_0^{u\varphi(q)}s\right\} \text{ and}\\
Q_2(s,u) =& (B_2^{(t)}(s) - p^t) \times g_0^{u\varphi(q)+\frac{\varphi(q)}{2}} = \left\{p^t, 0, p^t + g_0^{\frac{\varphi(q)}{2}+u\varphi(q)}s, g_0^{\frac{\varphi(q)}{2}+u\varphi(q)}s\right\}
\end{aligned}$$

for $u \in [0, p^t-1]$, which follow from $p^t g_0^{\varphi(q)} \equiv p^t \pmod{p^m}$ and $p^t g_0^{\frac{\varphi(q)}{2}} \equiv -p^t \pmod{p^m}$, respectively. We have

$$\bigcup_{s \in S_t} \bigcup_{u=0}^{p^t-1} \left\{g_0^{u\varphi(q)}s, g_0^{\frac{\varphi(q)}{2}+u\varphi(q)}s\right\} = \bigcup_{s \in S_t} s\left(H_0^{(t)} \cup H_{\frac{\varphi(q)}{2}}^{(t)}\right) = \mathbb{Z}_{p^m}^\times,$$

where the last equality follows from Proposition 2.3.6. Hence, for every $x \in \mathbb{Z}_{p^m}^\times$, the triple $\{0, p^t, x\}$ is covered twice in $\bigcup_{s_t \in S_t} \mathcal{O}_A(B_{s_t}^{(t)})$. $\square$

Let $p\mathcal{B}_p = \{pB \pmod{p^m} \mid B \in \mathcal{B}_p\}$, where $\mathcal{B}_p$ denotes the set of all base blocks of the affine-invariant TQS(p^{m-1}) obtained from Construction 2.5.1.

Lemma 2.6.9 (Type VI)**.** *For each* $t \in [m-1]$, $\bigcup_{B^* \in p\mathcal{B}_p} \mathcal{O}_A(B^*)$ *covers* $\{0, p^t, x_t\}$ *for every* $x_t \in p\mathbb{Z}_{p^{m-1}} \setminus \{0, p^t\}$ *exactly twice.*

Proof. This is obvious from Construction 2.5.1. □

We can sum up Lemmas 2.6.6, 2.6.8, 2.6.7 and 2.6.9 as follows:

(i) (Lemma 2.6.6) The affine orbits of Type I, II, III, and IV blocks cover $\{0, 1, x\}$ twice for every $x \in \mathbb{Z}_p \setminus \{0, 1\} + p\mathbb{Z}_{p^{m-1}}$.

(ii) (Lemma 2.6.7) The affine orbits of Type V blocks cover $\{0, 1, x\}$ twice for every $x \in (\{0, 1\} + p\mathbb{Z}_{p^{m-1}}) \setminus \{0, 1\}$.

(iii) (Lemma 2.6.8) The affine orbits of Type V blocks cover $\{0, p^t, x\}$ twice for each $t \in [m-1]$ and every $x \in \mathbb{Z}_{p^m}^{\times}$.

(iv) (Lemma 2.6.9) The affine orbits of Type V blocks cover $\{0, p, x\}$ twice for each $t \in [m-1]$ and every $x_t \in p\mathbb{Z}_{p^{m-1}} \setminus \{0, p^t\}$.

In summary, we have the following criterion for the existence of affine-invariant TQS.

Theorem 2.6.10. *For* $p \equiv 5 \pmod{12}$*, if the graph* $\mathrm{CG}(\Omega_p)$ *has no bridge besides its pendant edge, then an affine-invariant* $\mathrm{TQS}(p^m)$ *exists for any positive integer* m*.*

2.7 Applications

In addition to the applications to OOCs, we briefly introduce the merits of the affine-invariant property for other applications. In particular, the constructions of 3-designs are usually more complicated than 2-designs. It is necessary to consider the practical significance for applications.

2.7.1 Searching blocks

Let $(V, \mathcal{B})$ be a t-design. For a given s-subset with $s \leq t$ (for example, a pair, a triple, etc.) of the point set V, say T, it is usually required to find the blocks containing a certain T in the applications to group testing [39], filing schemes [6, 126], etc. The affine-invariant property works effectively for these kind of problems.

We recall the AsSQS(25) in Example 2.3.11 to illustrate the main idea for searching blocks. First, we index every base block as shown in Table 2.11. Then, we create a "retrieval table" for the triples containing $\{0, 1\}$ as shown in Table 2.12. For example, when the quadruple containing $\{1, 3; 5\}$, say Q, is requested, we follow these steps:

Step 1: Since $(\{1, 3; 5\} - 1) \times 2^{-1} = \{0, 1; 2\}$, then $\mathcal{O}_A(\{1, 3; 5\}) = \mathcal{O}_A(\{0, 1; 2\})$.

Table 2.11: Index of base blocks

No.	Base blocks	No.	Base blocks
1	$\{0,1;4,22\}$	5	$\{0,5,1;9\}$
2	$\{0,1,24;0\}$	6	$\{0,5,2;13\}$
3	$\{0,1,4;5\}$	7	$\{0,5;10,20\}$
4	$\{0,1,9;10\}$	8	$\{0,5,20;0\}$

Table 2.12: Retrieval table of cyclic orbits in each affine orbit

Triples	No. of base blocks	The other element
$\{0,1;0\}$	2	24
$\{0,1;1\}$	2	2
$\{0,1;2\}$	5	6
$\{0,1;3\}$	4	23
$\vdots$	$\vdots$	$\vdots$

Step 2: Find $\{0,1;2\}$ in Table 2.12 and observe $\{0,1;2\}$ is covered by the affine orbit of No. 5 base block, i.e., $\mathcal{O}_A(\{0,5,1;9\})$. Then, the desired quadruple for $\{0,1;2\}$ is $\{0,1,6;2\}$.

Step 3: Take $Q = \{0,1,6;2\} \times 2 + 1 = \{1,3,13;5\}$.

In summary, we first find the desired "affine orbits", then the "cyclic orbits", and finally the "blocks". This procedure can be regarded as a generalization of the "retrieval algorithm" in filing schemes by using cyclic 2-designs (difference families) (see [6]). Clearly, by making use of the structure of automorphism groups, it is much more efficient than searching among all blocks.

2.7.2 Generating blocks

It is usually desired to generate a certain part of blocks for the applications of authentication codes [88, 110] as fast as possible using less storage. The structure of "affine orbits – cyclic orbits – blocks" also helps us to avoid unnecessary computation. Moreover, the storage requirement of affine base blocks of an AsSQS(v) is approximately reduced by up to $O(v)$ times from that of cyclic base blocks (see Tables 2.2, 2.3, 2.4, and 2.5).

On the other hand, practical applications of authentication codes often ask for an extremal large-scale design. The procedure of generating base blocks of an AsSQS($2p$) of Construction 2.2.6 relies on a 1-factor of the graph CG(Ω_p). Clearly, if a 1-factor is known, it needs at most $O(p)$ time to generate all base blocks. Note that CG(Ω_p) is an "almost" 3-regular graph of order $O(p)$ by Proposition 2.1.10 (ii). By using an algorithm for the maximum matching problem by Micali and Vazirani (see [91, 114]), it can be completed in $O(p^{3/2})$ time to find a 1-factor of $\mathrm{CG}(\Omega_p)$. Actually, if we assume that $\mathrm{CG}(\Omega_p)$ has no bridge except its pendant edges, by using Diks and Stańczyk's algorithm [38] for a 2-connected 3-regular graph, a 1-factor can be found in $O(p \log^2 p)$ time. In summary, even if all the blocks (the whole incident matrix) are required, it can be done in $O(p^{3/2})$ time.

Chapter 3

Grid-block difference families

This chapter is devoted to the existence and construction of grid-block difference families, which can be regarded as generalizations of difference families and cyclic grid-block designs.

In order to show the existence, we first introduce an intermediate conclusion for estimating the asymptotic existence of an element satisfying certain cyclotomic conditions in a finite field.

3.1 An intermediate consequence derived from Weil's Theorem on multiplicative character sums

For many direct constructions of designs, the essential problem often comes down to choosing *a proper subset* to form an *SDR (system of distinct representatives)* of *a certain set system.* For "DF-like" structures over $\mathbb{F}_q$, the "certain set system" is usually a collection of cyclotomic cosets. In this case, Buratti and Pasotti's Theorem 1.4.8 provides a general solution when the desired "proper subset" forms a system of linear functions with respect to some $x \in \mathbb{F}_q$.

For instance, for showing the existence of a $(q, 6, 1)$-DF over $\mathbb{F}_q$, Wilson proposed a sufficient condition as follows:

Theorem 3.1.1 (Wilson [120] Theorem 11)**.** *Let $q \equiv 1 \pmod{30}$ be a prime power and let ω be a primitive cube root of unity in $\mathbb{F}_q$. If there exists an element $x \in \mathbb{F}_q$ such that $\{1, x, \frac{x-1}{\omega-1}, \frac{x-\omega}{\omega-1}, \frac{x-\omega^2}{\omega-1}\}$ forms a system of representatives for $\mathcal{C}^{(5)}$, then there exists a $(q, 6, 1)$-DF over $\mathbb{F}_q$.*

In order to meet the above criteria, one can suppose

$$x \in C_1^{(5)}, \frac{x-1}{\omega-1} \in C_2^{(5)}, \frac{x-\omega}{\omega-1} \in C_3^{(5)}, \text{ and } \frac{x-\omega^2}{\omega-1} \in C_4^{(5)}$$

and use Theorem 1.4.8 to obtain a bound on q. Actually, Chen and Zhu [28] considered a more relaxed assumption, say

$$x \in C_i^{(5)}, \tfrac{x-1}{\omega-1} \in C_{2i}^{(5)}, \tfrac{x-\omega}{\omega-1} \in C_{3i}^{(5)}, \text{ and } \tfrac{x-\omega^2}{\omega-1} \in C_{4i}^{(5)} \text{ for some } i \in \mathbb{Z}_5 \setminus \{0\},$$

where the subscripts of $C_{ij}^{(5)}$ are reduced modulo 5. Consequently, a better bound on q was obtained.

The same trick has also been used by Chen and Zhu [30] to improve the existence bound for a $(q, 7, 1)$-DF in which every base block is of the form $\{0, 1, x, x^2, x^3, x^4, x^5\}$.

In general, if a *complete SDR* of $\mathcal{C}^{(e)}$ is desired instead of an "SDR", any m in the group of units $\mathbb{Z}_e^\times$ can be used as a multiplier to the subscripts. Then, a better existence bound can be obtained from the relaxed criteria.

Note that, for instance, if $(1, 2, x_2, x_3, x_4)$ is desired to form a complete system of representatives of $\mathcal{C}^{(5)}$, this idea does not work well anymore (see, for instance, Chen, Wei, and Zhu [27] on $(q, 7, 1)$-DF). But in this case, Buratti and Pasotti's Theorem 1.4.8 can also give an answer.

In what follows, let $\mu(\cdot)$ and $\varphi(\cdot)$ denote the Möbius function and Euler's totient function, respectively. For basic properties of these number-theoretic functions, the reader can refer to [3].

Lemma 3.1.2. *Let $e > 1$ be a positive integer and $q \equiv 1 \pmod e$ be a prime power. Let χ be a multiplicative character of order e of $\mathbb{F}_q$. For any divisor w of e, let*

$$A_w(x) = 1 + \sum_{k=1}^{e-1} \chi(x^{wk}) \quad \text{and} \quad A(x) = \sum_{w \mid e} \mu(\tfrac{e}{w}) A_w(x) \tag{3.1}$$

for $x \in \mathbb{F}_q$. Then $A(x) = e$ if $x \in \bigcup_{i \in \mathbb{Z}_e^\times} C_i^{(e)}$ and $A(x) = 0$ otherwise.

Proof. First we can reformulate $A_w(x)$ in an explicit form, namely

$$A_w(x) = \begin{cases} 1, & \text{if } x = 0, \\ e, & \text{if } x \in \bigcup\limits_{\substack{0 \le i \le e-1 \\ e \mid iw}} C_i^{(e)}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.2}$$

Then the proof can be simply done by the well-known property

$$\sum_{d \mid n} \mu(d) = \sum_{d \mid n} \mu(\tfrac{n}{d}) = \begin{cases} 1, & \text{if } n = 1, \\ 0, & \text{if } n > 1. \end{cases}$$

For $x = 0$, we have $A(0) = \sum_{w \mid e} \mu(\frac{e}{w}) = 0$. For a given $x \in C_i^{(e)}$, we have $A(x) = \sum_{w \mid e, e \mid iw} \mu(\frac{e}{w}) e = e \sum_{w \mid e, \frac{e}{d} \mid w} \mu(\frac{e}{w})$ where $d = \gcd(i, e)$. Suppose $w =$

$\frac{e}{d} \cdot u$, then $\frac{e}{w} = \frac{d}{u}$. We can substitute e and w with d and u in the above sum to get

$$A(x) = e \sum_{u|d} \mu(\tfrac{d}{u}) = \begin{cases} e, & \text{if } d = 1, \\ 0, & \text{if } d > 1, \end{cases}$$

which is equivalent to saying $A(x) = \begin{cases} e, & \text{if } x \in C_i^{(e)} \text{ and } i \in \mathbb{Z}_e^\times, \\ 0, & \text{otherwise.} \end{cases}$ □

Theorem 3.1.3. *Let $e \geq 2$ and $t \geq 1$ be positive integers and $q \equiv 1 \pmod{e}$ be a prime power. Suppose $a_j, b_j \in \mathbb{F}_q^*$ and $c_j \in \mathbb{Z}_e$ for $1 \leq j \leq t-1$ such that $\{a_j^{-1} b_j \mid 1 \leq j \leq t-1\} \cup \{0\}$ is a t-subset of $\mathbb{F}_q$. Let*

$$X = \{x \in \mathbb{F}_q \mid x \text{ satisfies the following (i) and (ii)}\}. \tag{3.3}$$

(i) $x \in C_i^{(e)}$ for $i \in \mathbb{Z}_e^\times$;

(ii) $a_j x + b_j \in C_{c_j i}^{(e)}$ for $1 \leq j \leq t-1$ and $i \in \mathbb{Z}_e^\times$.

Then $|X| > n$ whenever

$$q > L(e,t,n) := \left(\frac{c_1 + \sqrt{c_1^2 + 4\varphi(e)c_0}}{2\varphi(e)} \right)^2 \quad \text{with} \tag{3.4}$$

$$c_0 := (en + t - 1)e^{t-1} + e - 1 \quad \text{and} \quad c_1 := \left(e - w^* + \sum_{w|e, \mu(\frac{e}{w}) \neq 0} (e - w) \right) \Psi,$$

where w^* is the largest divisor of e with $\mu(\frac{e}{w}) = -1$ and

$$\Psi := \sum_{\ell=1}^{t-1} \binom{t-1}{\ell} (e-1)^\ell \ell.$$

In particular, X is not empty if $q > L(e,t) := L(e,t,0)$. Furthermore, if e is a prime power of the form p^s with $s \geq 1$ and p prime, then $L(e,t,n) = (\Psi + \sqrt{\Psi^2 + c_0/\varphi(e)})^2$.

Proof. The conditions (i) and (ii) are equivalent to

(i′) $x \in \bigcup_{i \in \mathbb{Z}_e^\times} C_i^{(e)}$;

(ii′) $x^{e-c_j}(a_j x + b_j) \in C_0^{(e)}$ for $1 \leq j \leq t-1$.

In order to find $L(e,t,n)$, we will define a sum S via a series of character sums of $\mathbb{F}_q$. Employing the double counting (estimating) technique on S, an inequality with respect to q which guarantees $|X| > n$ will be derived. This is a classical way for showing the asymptotic existence of DFs and "DF-like" structures over $\mathbb{F}_q$.

First, let

$$B(x) := e + \sum_{w|e, w\neq e} \mu(\tfrac{e}{w}) A_w(x), \tag{3.5}$$

where $A_w(x) = 1 + \sum_{k=1}^{e-1} \chi(x^{wk})$. It follows from (3.2) that $A_e(x)$ is equal to 1 if $x = 0$ and is equal to e otherwise. Since $B(x) = e - A_e(x) + A(x)$ (where $A(x)$ follows the definition in (3.1)), by Lemma 3.1.2 we have

$$B(x) = \begin{cases} e-1, & \text{if } x = 0, \\ e, & \text{if } x \in \bigcup_{i\in\mathbb{Z}_e^\times} C_i^{(e)}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.6}$$

For $1 \leq j \leq t-1$, let $f_j(x) := x^{e-c_j}(a_j x + b_j)$ and

$$B_j(x) := \sum_{k=0}^{e-1} \chi(f_j^k(x)) = \begin{cases} 1, & \text{if } f_j(x) = 0, \\ e, & \text{if } f_j(x) \in C_0^{(e)}, \\ 0, & \text{otherwise.} \end{cases} \tag{3.7}$$

Now we consider

$$S := \sum_{x\in\mathbb{F}_q} B(x) \prod_{j=1}^{t-1} B_j(x). \tag{3.8}$$

It is easy to observe that $S = e^t m + d$, where m is the number of $x \in \mathbb{F}_q$ satisfying conditions (i′) and (ii′), and d is the contribution when at least one of x, $f_1(x)$, …, $f_{t-1}(x)$ is 0. If $x = 0$ and $c_j \neq 0$, then $f_j(x) = 0$ holds for each $1 \leq j \leq t-1$, thus the contribution is $e-1$. Otherwise, if $x \neq 0$ and $f_j(x) = 0$, then the contribution is at most e^{t-1} for each $1 \leq j \leq t-1$. In order to prove $m \geq n$, it suffices to show $S > e^t n + (t-1)e^{t-1} + e - 1 = c_0$.

Now we begin to consider each part of the sum $S = e\sum_{x\in\mathbb{F}_q}\prod_{j=1}^{t-1} B_j(x) + \sum_{w|e,w\neq e} \mu(\frac{e}{w}) \sum_{x\in\mathbb{F}_q} A_w(x) \prod_{j=1}^{t-1} B_j(x)$. Let

$$S_w := \sum_{x\in\mathbb{F}_q} A_w(x) \prod_{j=1}^{t-1} B_j(x) \quad \text{and} \quad S_w^- := \sum_{x\in\mathbb{F}_q} (e - A_w(x)) \prod_{j=1}^{t-1} B_j(x). \tag{3.9}$$

Here we simply denote by $\sum'$ the sum extended over $\sum\limits_{\ell=1}^{t-1} \sum\limits_{\substack{1\leq j_1<\cdots<j_\ell\leq t-1 \\ 1\leq k_1,\ldots,k_\ell\leq e-1}}$. Then,

$$\begin{aligned} \frac{1}{w} S_w &= \sum_{x\in\mathbb{F}_q} \sum_{u=0}^{\frac{e}{w}-1} \chi(x^{wu}) \prod_{j=1}^{t-1} \sum_{k=0}^{e-1} \chi(f_j^k(x)) \\ &= \sum_{x\in\mathbb{F}_q} 1 + U + \sum_{u=1}^{\frac{e}{w}-1} {\sum}' \sum_{x\in\mathbb{F}_q} \chi\left(x^{wu} f_{j_1}^{k_1}(x) \cdots f_{j_\ell}^{k_\ell}(x)\right), \end{aligned}$$

$$
\begin{aligned}
S_w^- &= \sum_{x\in\mathbb{F}_q}\left(e-w-w\sum_{u=1}^{\frac{e}{w}-1}\chi(x^{wu})\right)\prod_{j=1}^{t-1}\sum_{k=0}^{e-1}\chi(f_j^k(x))\\
&= \sum_{x\in\mathbb{F}_q}(e-w)+(e-w){\sum}'\sum_{x\in\mathbb{F}_q}\chi\Big(f_{j_1}^{k_1}(x)\cdots f_{j_\ell}^{k_\ell}(x)\Big)\\
&\quad -wU-w\sum_{u=1}^{\frac{e}{w}-1}{\sum}'\sum_{x\in\mathbb{F}_q}\chi\Big(x^{wu}f_{j_1}^{k_1}(x)\cdots f_{j_\ell}^{k_\ell}(x)\Big),
\end{aligned}
$$

where $\sum_{x\in\mathbb{F}_q}1=q$ and $U=\sum_{u=1}^{\frac{e}{w}-1}\sum_{x\in\mathbb{F}_q}\chi(x^{wu})=0$. Let

$$\Gamma_w := S_w - wq \quad\text{and}\quad \Gamma_w^- := S_w^- - (e-w)q. \tag{3.10}$$

It follows from Weil's Theorem 1.4.7 that $\left|\sum_{x\in\mathbb{F}_q}\chi\Big(f_{j_1}^{k_1}(x)\cdots f_{j_\ell}^{k_\ell}(x)\Big)\right|\le \ell\sqrt{q}$ and $\left|\sum_{x\in\mathbb{F}_q}\chi\Big(x^{wu}f_{j_1}^{k_1}(x)\cdots f_{j_\ell}^{k_\ell}(x)\Big)\right|\le\ell\sqrt{q}$. We have

$$|\Gamma_w|\le w\sum_{u=1}^{\frac{e}{w}-1}{\sum}'\ell\sqrt{q}=(e-w)\Psi\sqrt{q}\quad\text{and}\quad\left|\Gamma_w^-\right|\le 2(e-w)\Psi\sqrt{q}, \tag{3.11}$$

where $\Psi={\sum}'\ell=\sum_{\ell=1}^{t-1}\binom{t-1}{\ell}(e-1)^\ell\ell$. Now we are in a position to estimate $|S|$. Noting that $\mu(\frac{e}{w^*})=-1$, we have

$$S=S_{w^*}^-+\sum_{\substack{w|e\\ w\notin\{e,w^*\}}}\mu(\tfrac{e}{w})S_w=\sum_{w|e}\mu(\tfrac{e}{w})wq+\Gamma_{w^*}^-+\sum_{\substack{w|e\\ w\notin\{e,w^*\}}}\mu(\tfrac{e}{w})\Gamma_w,$$

where $\sum_{w|e}\mu(\frac{e}{w})wq=\varphi(e)q$. Moreover, we have

$$
\begin{aligned}
\varphi(e)q-|S|\le|S-\varphi(e)q| &= \left|\Gamma_{w^*}^-+\sum_{w|e,w\notin\{e,w^*\}}\mu(\tfrac{e}{w})\Gamma_w\right|\\
&\le \left|\Gamma_{w^*}^-\right|+\sum_{w|e,w\notin\{e,w^*\}}\left|\mu(\tfrac{e}{w})\Gamma_w\right|\\
&\le (e-w^*)\Psi\sqrt{q}+\sum_{w|e,\mu(\frac{e}{w})\neq 0}(e-w)\Psi\sqrt{q}\\
&= c_1\sqrt{q},
\end{aligned}
$$

where the last inequality follows from (3.11). Obviously, if $q>\left(\frac{c_1+\sqrt{c_1^2+4\varphi(e)c_0}}{2\varphi(e)}\right)^2$, then $|S|>c_0$, so that $|X|>n$.

When $e=p^s$ is a prime power with p prime, we have $w^*=p^{s-1}$ and $c_1=2(e-p^{s-1})\Psi=2\varphi(e)\Psi$. Therefore, $L(e,t,n)=(\Psi+\sqrt{\Psi^2+c_0/\varphi(e)})^2$. $\square$

We want to show that $L(e,t,n)$ is better (smaller) than $Q(e,t,n)$ in most cases. To prove this proposition, we need a simple inequality on integers.

Lemma 3.1.4. *Let n be a positive integer and let $d(n)$ denote the number of divisors of n. Then $d(n) < \varphi(n)$ whenever $n \notin \{1,2,3,4,6,10,12,30\}$.*

Proof. Both $d(\cdot)$ and $\varphi(\cdot)$ are multiplicative functions. Now suppose p is prime and $\alpha \geq 1$. Clearly, $d(p^\alpha) = \alpha + 1 < \varphi(p^\alpha) = (p-1)p^{\alpha-1}$ whenever $p \geq 5$ and $\alpha \geq 1$, or $p = 3$ and $\alpha \geq 2$, or $p = 2$ and $\alpha \geq 3$. Furthermore, suppose $p \geq 5$. For $n = 2^2 p^\alpha$, or $n = 3^1 p^\alpha$, or $n = 2^2 3^1 p^\alpha$, $d(n) < \varphi(n)$ always holds. For $n = 2p^\alpha$ or $n = 2^1 3^1 p^\alpha$, $d(n) < \varphi(n)$ holds except when $p^\alpha = 5^1$. Thus $d(n) < \varphi(n)$ for any positive integer $n \notin \{1,2,3,4,6,10,12,30\}$. ☐

Proposition 3.1.5. For any integers $e \geq 3$, $e \neq 6$, $t \geq 2$, and $n \geq 0$, $L(e,t,n) < Q(e,t,n)$. In particular, if $t \geq 3$ and $e = p^s$ with p prime and $s \geq 1$, then $\frac{(e-1)^2}{4} L(e,t) < Q(e,t)$.

Proof. For $e \notin \{3,4,6,10,12,30\}$, it follows from Lemma 3.1.4 that $d(e) < \varphi(e)$, thus $\gamma(e) := e - w^* + \sum_{w|e,\mu(\frac{e}{w})\neq 0}(e-w) \leq e - w^* + \sum_{w|e,w\neq e}(e-w) \leq \sum_{w|e}(e-1) = (e-1)d(e) < (e-1)\varphi(e)$. For $e \in \{3,4,10,12,30\}$, it can be directly verified that $\gamma(e) \leq (e-1)\varphi(e)$. Moreover,

$$\begin{aligned}\frac{U}{e-1} - \Psi &= \sum_{\ell=1}^{t-1}\binom{t}{\ell+1}(e-1)^\ell \ell - \sum_{\ell=1}^{t-1}\binom{t-1}{\ell}(e-1)^\ell \ell \\ &= \sum_{\ell=1}^{t-1}\frac{t-\ell-1}{\ell+1}\binom{t-1}{\ell}(e-1)^\ell \ell\end{aligned}$$

which is greater than or equal to $e-1$ when $t \geq 3$, and is equal to 0 if $t = 2$. Hence, $\frac{c_1}{\varphi(e)} = \frac{\gamma(e)}{\varphi(e)}\Psi \leq \frac{(e-1)\varphi(e)}{\varphi(e)} \cdot \frac{U}{e-1} = U$. Furthermore, since $\frac{c_0}{\varphi(e)} < c_0 = (en+t-1)e^{t-1} + e - 1 < (en+t)e^{t-1}$, we have $\frac{c_1+\sqrt{c_1^2+4\varphi(e)c_0}}{\varphi(e)} < U + \sqrt{U^2+4te^{t-1}}$, which immediately implies $L(e,t) < Q(e,t)$.

Next, in the case of $n = 0$, we suppose $t \geq 3$ and e is a prime power. Proving $\frac{(e-1)^2}{4}L(e,t) < Q(e,t)$ is equivalent to showing $\Psi + \sqrt{\Psi^2 + c_0/\varphi(e)} < \frac{1}{e-1}(U + \sqrt{U^2+4te^{t-1}})$. As shown above, $\Psi < \frac{U}{e-1}$. So it suffices to show $\Psi^2 + \frac{c_0}{\varphi(e)} < \frac{U^2}{(e-1)^2} + \frac{4te^{t-1}}{(e-1)^2}$. This inequality can be obtained by combining $(\frac{U}{e-1})^2 - \Psi^2 > \frac{e-1}{2}te^{t-1} \geq te^{t-1}$ and $\frac{c_0}{\varphi(e)} - \frac{4te^{t-1}}{(e-1)^2} < \frac{c_0}{\varphi(e)} = \frac{(t-1)e^{t-1}+e-1}{\varphi(e)} < \frac{te^{t-1}}{\varphi(e)} < te^{t-1}$, where the first inequality follows from $\frac{U}{e-1} - \Psi \geq e-1$ and $\frac{U}{e-1} + \Psi = \sum_{\ell=1}^{t-1}\binom{t-1}{\ell}(e-1)^\ell(\frac{\ell t}{\ell+1} + \ell) > \sum_{\ell=1}^{t-1}\binom{t-1}{\ell}(e-1)^\ell(\frac{t}{2}+1) = (\frac{t}{2}+1)(e^{t-1}-1) > \frac{t}{2}e^{t-1}$. ☐

3.2 Direct constructions and asymptotic existence of grid-block difference families

First, we need some notation. Let G be an additive group and let $A = \{a_1, a_2, \dots, a_t\}$ be a subset of G. Let $\Delta A = \{a_i - a_j \mid 1 \le i, j \le t, i \ne j\}$ and $\Delta^{+} A = \{a_i - a_j \mid 1 \le i < j \le t\}$. Further, suppose $\mathsf{B} = [b_{ij}]_{r\times k}$ is an $r \times k$ grid-block whose elements are in G. Similarly, let

$$\Delta\mathsf{B} = \left(\bigcup_{i=1}^{r} \Delta\{b_{i1}, b_{i2}, \dots, b_{ik}\}\right) \cup \left(\bigcup_{j=1}^{k} \Delta\{b_{1j}, b_{2j}, \dots, b_{rj}\}\right).$$

Let $\mathcal{B}$ be a collection of grid-blocks, and denote $\Delta\mathcal{B} = \bigcup_{\mathsf{B}\in\mathcal{B}} \Delta\mathsf{B}$.

Lemma 3.2.1 ([131] Lemma 1.7)**.** *Let $e = rk(r + k - 2)/2$ and let $q \equiv 1 \pmod{2e}$ be a prime power. If there exists an $r \times k$ array A over $\mathbb{F}_q$ such that $\Delta^{+}\mathsf{A}$ is a system of representatives of $\mathcal{C}^{(e)}$, then there exists a $(q, L_{r\times k}, 1)$-DF over $\mathbb{F}_q$.*

Next, we propose more theorems which extend Lemma 3.2.1.

3.2.1 Grid-block difference families with a multiplier of order 3

In this section, we give a direct construction of a $(q, L_{r,3u}, 1)$-DF with a multiplier of order 3, which requires $q \equiv 1 \pmod{3ur(r + 3u - 2)}$.

Theorem 3.2.2. *For any positive integer r and u, let $e = \frac{ru(r+3u-2)}{2}$ and let $q \equiv 1 \pmod{6e}$ be a prime power. Let g be a primitive element in $\mathbb{F}_q$ and ω be a primitive cubic root of unity of $\mathbb{F}_q$. Suppose there exist $x_1, \dots, x_{r-1}, y_1, \dots, y_{u-1} \in \mathbb{F}_q^*$ such that $\frac{1}{\omega-1}H_{r,u}$ forms a complete system of representatives of $\mathcal{C}^{(e)}$, where*

$$H_{r,u} = (\omega - 1)\cdot X \cdot Y \cup X \cdot \Delta^{+}_{\omega} Y \cup Y \cdot \Delta^{+} X$$

with

$$\begin{aligned} \Delta^{+}_{\omega} Y &= \{y_{j_1} - y_{j_2}\omega^k \mid 0 \le j_1 < j_2 \le u-1, 0 \le k \le 2\}, \\ X &= \{x_0, x_1, \dots, x_{r-1}\}, \\ Y &= \{y_0, y_1, \dots, y_{u-1}\}, \end{aligned}$$

and $x_0 = y_0 = 1$. Let $\mathsf{B} = [b_{ij}]_{r\times 3u}$ be a grid-block with $b_{ij} = x_{i-1} y_{\lceil \frac{j-1}{3} \rceil}\omega^{j-1}$ for $1 \le i \le r$ and $1 \le j \le 3u$. Then $\mathcal{B} = \{g^{ei}\mathsf{B} \mid 0 \le i < \frac{q-1}{6e}\}$ forms a $(q, L_{r,3u}, 1)$-DF in $\mathbb{F}_q$.

Proof. It is sufficient to show that $\Delta\mathcal{B} = \mathbb{F}_q^*$. Let $n = \frac{q-1}{6e}$. First, we have $\Delta\mathsf{B} = X \cdot \Delta(\{1, \omega, \omega^2\}\cdot Y\}) \cup (\{1, \omega, \omega^2\}\cdot Y\}) \cdot \Delta X = \{1, -1\}\cdot\{1, \omega, \omega^2\}\cdot H_{r,u} = C^{(en)} \cdot H_{r,u}$ with $|H_{r,u}| = e$. Note that $T := \{g^{ei} \mid 0 \le i < n\}$ is a system of representatives for the cosets of $C^{(en)}$ in $C^{(e)}$. With the assumption that $H_{r,u}$ forms a complete system of representatives of $\mathcal{C}^{(e)}$, we have $\Delta\mathcal{B} = T \cdot \Delta\mathsf{B} = C^{(e)} \cdot H_{r,u} = \mathbb{F}_q^*$. $\square$

Table 3.1: $(p, L_{6,2}, 1)$-DF that cannot obtained from Theorem 3.2.2

p	g	ω	x	y	z	p	g	ω	x	y	z
73	5	8	43	59	2	433	5	198	116	125	114
577	5	363	433	5	80	937	5	614	383	5	417
1009	11	374	385	322	981	1153	5	650	101	5	819
1297	17	931	95	513	113	1657	11	70	1258	11	1232
2089	7	1262	1266	49	515	3313	11	2189	939	121	1388
3529	17	3080	795	289	2530	7489	7	5021	1616	343	7176

Example 3.2.3. Let $r = 2$, $u = 1$, and $q = 37$. Take $g = 2$, then $\omega = g^{12} = 26$. Take $x_1 = 2$, we have $(\zeta - 1, x_1(\zeta - 1), x_1 - 1) = (25, 13, 1) \in C_1^{(3)} \times C_2^{(3)} \times C_0^{(3)}$. Then,

$$\left\{ \begin{bmatrix} 1 & 26 & 10 \\ 2 & 15 & 20 \end{bmatrix}, \begin{bmatrix} 6 & 8 & 23 \\ 12 & 16 & 9 \end{bmatrix} \right\}$$

forms a cyclic $(37, L_{2,3}, 1)$-DF.

Remark. When $u = 2$ and $r = 1$, Theorem 3.2.2 becomes Wilson [120] Theorem 11 for a $(q, 6, 1)$-DF (see also Chen and Zhu [28]).

Remark. For $r = u = 2$, we have checked that Theorem 3.2.2 can be applied to every prime $p \equiv 1 \pmod{72}$ with $p < 10^7$ except when $p \in P$, where $P = \{p \equiv 1 \pmod{72} \text{ is prime} \mid p \leq 1657\} \cup \{2089, 3313, 3529, 7489\}$. In other words, $H_{2,2}$ never forms a system of representatives of $\mathcal{C}^{(12)}$ for any choice of a pair (x_1, y_1) in $\mathbb{F}_p^*$ with $p \in P$. However, by introducing an extra variable, a $(p, L_{2,6}, 1)$-DF with a multiplier of order 3 can be constructed for any $p \in P$. With the parameters listed in Table 3.1, $\mathcal{B} := \{g^{12i}\mathsf{B} \mid 0 \leq i < \frac{p-1}{72}\}$ forms a $(p, L_{2,6}, 1)$-DF, where

$$\mathsf{B} = \begin{bmatrix} 1 & \omega & \omega^2 & y & \omega y & \omega^2 y \\ x & \omega x & \omega^2 x & z & \omega z & \omega^2 z \end{bmatrix}.$$

In addition, other examples of $(p, L_{2,6}, 1)$-DFs with $p \in \{73, 433\}$ can be found from Wang and Colbourn [115].

Theorem 3.2.4. *For any positive integer r and u, let $e = \frac{ru(r+3u-2)}{2}$. Then a $(q, L_{r,3u}, 1)$-DF exists for all $q > L(e, \max\{r, 3u-2\})$ with $q \equiv 1 \pmod{6e}$ a prime power.*

Proof. With the notation of X, Y, and $\Delta_\omega^+ Y$ in Theorem 3.2.2, it suffices to find $X, Y \subset \mathbb{F}_q^*$ satisfying the following conditions in two cases:

(a) If r is odd,

  (a1) $x_i \in C_i^{(e)}$ for $i \in [r-1]$;

  (a2) $y_j \in C_{jr}^{(e)}$ for $j \in [u-1]$;

(a3) $\frac{1}{\omega-1}\Delta^+_\omega Y$ forms a system of representatives of $\{C^{(e)}_{ur+jr} \mid j \in [0, \frac{3u(u-1)}{2} - 1]\}$;

(a4) $\frac{1}{\omega-1}\Delta^+ X$ forms a system of representatives of $\bigcup_{\ell=0}^{\frac{r-3}{2}} \{C^{(e)}_{s_\ell+i} \mid i \in [0, r-1]\}$ with $s_\ell = \frac{ru(3u-1+2\ell)}{2}$.

(b) If r is even,

(b1) $x_i \in C^{(e)}_i$ for $i \in [\frac{r}{2}-1]$ and $x_i \in C^{(e)}_{\frac{r}{2}\cdot\frac{u(3u-1)}{2}+i}$ for $i \in [\frac{r}{2}, r-1]$;

(b2) $y_j \in C^{(e)}_{j\frac{r}{2}}$ for $j \in [u-1]$;

(b3) $\frac{1}{\omega-1}\Delta^+_\omega Y$ forms a system of representatives of $\{C^{(e)}_{u\frac{r}{2}+j\frac{r}{2}} \mid j \in [0, \frac{3u(u-1)}{2} - 1]\}$;

(b4) $\frac{1}{\omega-1}\Delta^+ X$ forms a system of representatives of $\bigcup_{\ell=0}^{r-2} \{C^{(e)}_{s_\ell+i} \mid i \in [0, \frac{r}{2}-1]\}$ with $s_\ell = \frac{ru(3u-1+\ell)}{2}$.

The subscript i of $C^{(e)}_i$ can be regarded as an element in $\mathbb{Z}_e$. Clearly, by multiplying all the above subscripts by any unit in $\mathbb{Z}_e^\times$, we can obtain another quadruple of conditions which is also admissible. Note that there are precisely r (resp. $3u-2$) conditions with respect to x_i (resp. y_j) for each $i \in [r-1]$ (resp. $j \in [u-1]$). By repeatedly employing Theorem 3.2.2 for each x_i and y_j, it can be guaranteed that $X, Y \subset \mathbb{F}_q^*$ satisfying the above conditions exist whenever $q > L(\frac{e}{6}, \max\{r, 3u-2\})$. □

In Table 3.2, some existence bounds for a $(q, L_{r,3u}, 1)$ DF are listed, where $L(e,t) = L(e,t,0)$ and $Q(e,t) = Q(e,t,0)$ are defined in Theorems 3.1.3 and 1.4.8, respectively. It is remarkable that a $(q, L_{1,6}, 1)$ DF is nothing more than a $(q, 6, 1)$-DF, and the value $L(5,4)$ was first derived by Chen and Zhu [28] via the same estimation. The last columns for $(q, L_{1,9}, 1)$-DF and $(q, L_{1,12}, 1)$-DF show the known bound obtained by Chen and Zhu [30] without considering any multiplier. In addition, it can be observed that $L(e,t)$ is more effective when e is a prime power. For real world applications to biology experiments, 8×12 grid-block designs are the most important. Here we also give a bound for $(q, L_{8,12}, 1)$ DF, although it is still quite large and unsatisfactory.

3.2.2 Row-radical grid-block difference families

As an analogue of radical DFs, it is natural to consider row-radical (column-radical) $(q, L_{r,k}, 1)$-DFs.

Definition 3.2.5 (row-radical DF)**.** An elementary abelian $(q, L_{r,k}, 1)$-DF is *row-radical* (resp., *column-radical*) if the rows (resp., columns) are cosets of $C^{(\frac{q-1}{k})}$ (resp., $C^{(\frac{q-1}{r})}$) in all base grid-blocks. Moreover, an elementary abelian $(q, L_{r,k}, 1)$-DF is *radical* if it is both row-radical and column-radical.

Table 3.2: Improved existence bounds for $(q, L_{r,3u}, 1)$-DFs

$r \times 3u$	t	e	$L(e,t)$	$Q(e,t)$	Remark / Reference
4×3	4	10	3.3215×10^{8}	6.7606×10^{8}	
5×3	5	15	1.1810×10^{12}	7.7528×10^{12}	
1×6	4	5	3.6019×10^{5}	1.8944×10^{6}	$= L(5,4)$ [28]
2×6	4	12	1.2702×10^{9}	3.0578×10^{9}	
3×6	4	21	2.1179×10^{10}	2.9855×10^{11}	
4×6	4	32	3.6277×10^{10}	9.0882×10^{12}	
5×6	5	45	8.5043×10^{15}	5.1496×10^{17}	
1×9	7	12	1.5171×10^{16}	3.7671×10^{16}	4.7864×10^{20} [30]
2×9	7	27	2.0042×10^{19}	3.6060×10^{21}	
1×12	10	22	4.2694×10^{27}	5.1514×10^{28}	4.1773×10^{31} [30]
8×12	10	288	8.4072×10^{47}	1.2387×10^{51}	

Note that, for the radical cases, we necessarily have $\gcd(r,k) = \gcd(rk,2) = 1$, and the vertex-set of each base grid-block is a coset of $C^{(\frac{q-1}{rk})}$. It is clear that a row-radical (column-radical) grid-block DF must be a disjoint grid-block DF.

Now, we concentrate on direct constructions of elementary abelian $(q, L_{r,k}, 1)$-DDF with odd k. First, we consider a row-radical $(q, L_{r,k}, 1)$-DF over $\mathbb{F}_q$, which necessarily requires k to be odd and $q \equiv 1 \pmod{rk(r+k-2)}$. The following is the main theorem of our construction, which can imply a series of existence results.

Theorem 3.2.6 (Row-radical DF). *Let k be an odd integer. Suppose $q = n \cdot rk(r+k-2)+1$ is a prime power for a positive integer n. There exists a row-radical $(q, L_{r,k}, 1)$-DF over $\mathbb{F}_q$ if there exist $\alpha_1, \alpha_2, \ldots, \alpha_{r-1} \in \mathbb{F}_q^*$ such that $\frac{1}{\zeta_k - 1} X_{r,k}$ forms a system of representatives of the cosets of $C^{(f^{e+1})}$ in $C^{(f^e)}$ for a suitable e such that f^e divides n, where*

$$\begin{aligned} A_r &= \{1, \alpha_1, \alpha_2, \ldots, \alpha_{r-1}\}, \\ H_k &= \{\zeta_k - 1, \zeta_k^2 - 1, \ldots, \zeta_k^{\frac{k-1}{2}} - 1\}, \\ X_{r,k} &= A_r \cdot H_k \cup \Delta^+ A_r, \end{aligned}$$

and $f = |X_{r,k}| = \frac{r}{2}(r+k-2)$.

Proof. Let $Z = \left\{1, \zeta_k, \ldots, \zeta_k^{k-1}\right\} = C^{(2nf)}$. Since $-\zeta_k^{\frac{k-1}{2}+j}\left(\zeta_k^{\frac{k-1}{2}+1-j} - 1\right) = \zeta_k^{\frac{k-1}{2}+j} - 1$, we have $-\left(\zeta_k^{\frac{k-1}{2}+1-j} - 1\right) Z = \left(\zeta_k^{\frac{k-1}{2}+j} - 1\right) Z$ for any $j \in [\frac{k-1}{2}]$. Hence, $\Delta Z = \left\{\zeta_k^i(\zeta_k^j - 1) \mid i, j \in \mathbb{Z}_k, j \neq 0\right\} = Z \cdot \left\{\zeta_k^j - 1, \zeta_k^{\frac{k-1}{2}+j} - 1 \mid 1 \leq j \leq \frac{k-1}{2}\right\} = \pm Z \cdot H_k = C^{(nf)} \cdot H_k$.

Let $\mathsf{B} = [b_{ij}]_{r \times k}$ with $b_{ij} = \alpha_{i-1}\zeta_k^{j-1}$ for $i \in [r]$ and $j \in [k]$, where $\alpha_0 = 1$.

Then $\Delta \mathsf{B} = A_r \cdot \Delta Z \cup Z \cdot \Delta A_r = C^{(nf)} \cdot X_{r,k}$. Let

$$\mathcal{B} = \left\{ g^{f^{e+1}i+j} \cdot \mathsf{B} \middle| i \in [\tfrac{n}{f^e}], j \in [f^e] \right\}.$$

Then, $\Delta\mathcal{B} = \left\{ g^{f^{e+1}i+j} \cdot X_{r,k} \middle| i \in [\frac{n}{f^e}], j \in [f^e] \right\} \cdot C^{(nf)}$. Now we show the distinctness of all the elements in $\frac{1}{\zeta_k - 1}\Delta\mathcal{B}$. Assume there exist $i_1, i_2 \in [\frac{n}{f^e}]$, $j_1, j_2 \in [f^e]$, $x_1, x_2 \in \frac{1}{\zeta_k-1}X_{r,k}$, and $u_1, u_2 \in [\frac{q-1}{nf}]$ with $(i_1, j_1, x_1, u_1) \neq (i_2, j_2, x_2, u_2)$ such that $g^{f^{e+1}i_1+j_1} \cdot x_1 \cdot g^{nfu_1} = g^{f^{e+1}i_2+j_2} \cdot x_2 \cdot g^{nfu_2}$, where $x_1 = g^{f^{e+1}s_1+f^e t_1}$ and $x_2 = g^{f^{e+1}s_2+f^e t_2}$. This is equivalent to saying $f^{e+1}i_1 + j_1 + f^{e+1}s_1 + f^e t_1 + nfu_1 \equiv f^{e+1}i_2 + j_2 + f^{e+1}s_2 + f^e t_2 + nfu_2 \pmod{q-1}$ which implies $j_1 \equiv j_2 \pmod{f^e}$ and $(i_1 + s_1 + \frac{n}{f^e}u_1)f + t_1 \equiv (i_2 + s_2 + \frac{n}{f^e}u_2)f + t_2 \pmod{\frac{q-1}{f^e}}$. The second congruence implies that $t_1 \equiv t_2 \pmod{\frac{q-1}{f^e}}$. Recalling that $\frac{1}{\zeta_k-1}X_{r,k}$ forms a system of representatives of the cosets of $C^{(f^{e+1})}$ in $C^{(f^e)}$, there must be $x_1 = x_2$ as well. So, $s_1 = s_2$. Hence, $i_1 + \frac{n}{f^e}u_1 \equiv i_2 + \frac{n}{f^e}u_2 \pmod{\frac{q-1}{f^{e+1}}}$, i.e., $i_1 \equiv i_2 \pmod{\frac{q-1}{f^{e+1}}}$ and $u_1 \equiv u_2 \pmod{\frac{q-1}{nf}}$. This conclusion contradicts the assumption $(i_1, j_1, x_1, u_1) \neq (i_2, j_2, x_2, u_2)$. In summary, $\left|\frac{1}{\zeta_k-1}\Delta\mathcal{B}\right| = q - 1$. Therefore, $\Delta\mathcal{B} = (\zeta_k - 1) \cdot \mathbb{F}_q^* = \mathbb{F}_q^*$. □

For the case when $r = 1$, we can set $A_r = \{1\}$ and $\Delta^+ A_r = \emptyset$. Then Theorem 3.2.6 becomes the construction of radical DF due to Bose [10] ($e = 0$ and $k \in \{3, 5\}$), Wilson [120] ($e = 0$ and k odd), and Buratti [15, 16] (who also showed the necessity when $k \leq 7$).

For $r = 2$ and $k = 3$, by using Theorem 1.4.8, we can meet the criteria in Theorem 3.2.6 with $e = 0$ for any admissible $q > 26$. Here we only state the conclusion without proof, since the existence has been presented in [9].

Corollary 3.2.7. *There exists an elementary abelian $(q, L_{2,3}, 1)$-DDF for any prime power $q \equiv 1 \pmod{18}$.*

Actually, when $r = 2$, we have $X_{2,k} = \{1, \alpha_1\} \cdot H_k \cup \{\alpha_1 - 1\}$ with cardinality $|X_{2,k}| = k$. For the case when p is a prime and $e = 0$ in Theorem 3.2.6, in order for $X_{2,k}$ to form a system of representatives of $\mathcal{C}^{(k)}$, p is necessarily a good prime (cf. Definition 3.3.1). In particular, for $r = 2$ and $k = 5$, the cyclotomic condition $1 + \zeta_5 \notin C^{(5)}$ for p to be good is sufficient when p is an admissible prime.

First we present the equivalence between the existence of a row-radical $(q, L_{r,k}, 1)$-DF and a row-radical $(q^m, L_{r,k}, 1)$-DF.

Lemma 3.2.8. *Let $q \equiv 1 \pmod{rk(r+k-2)}$ be a prime power. Theorem 3.2.6 gives a $(q, L_{r,k}, 1)$-DDF if and only if it gives a $(q^m, L_{r,k}, 1)$-DDF for any positive integer m.*

Proof. A $(q, L_{r,k}, 1)$-DDF obtained from Theorem 3.2.6 must be of the form $\mathcal{B} = \{x\mathsf{B} \mid x \in X\}$, where $X \subset \mathbb{F}_q^*$. Let T be a transversal (a complete system of representatives) of the cosets of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^m}^*$. Since $q^m - 1$ can also be divided by $rk(r+k-2)$, then $\mathcal{B}_m := \{tx\mathsf{B} \mid x \in X, t \in T\}$ forms a $(q^m, L_{r,k}, 1)$-DDF in $\mathbb{F}_{p^m}$. It is clear that each row of any grid-block in $\mathcal{B}_m$ forms a coset of the kth root of unity in $\mathbb{F}_{q^m}$, thus $\mathcal{B}_m$ can be derived by Theorem 3.2.6.

Conversely, suppose $\mathcal{B}_m$ consists of the base grid-blocks of a $(q^m, L_{r,k}, 1)$-DDF obtained from Theorem 3.2.6. Then $\mathcal{B}_m$ must be of the form $\{y\mathsf{B} \mid y \in Y\}$ for some $Y \subset \mathbb{F}_{q^m}^*$. It is easily seen that $\mathcal{B}' := \{x\mathsf{B} \mid x \in Y \cap \mathbb{F}_q\}$ forms a $(q, L_{r,k}, 1)$-DDF in $\mathbb{F}_q$. Moreover, each row of any grid-block in $\mathcal{B}'$ is a coset of the kth root of unity in $\mathbb{F}_q$. Hence $\mathcal{B}_m$ can be derived by Theorem 3.2.6. $\square$

As a generalization of Corollary 3.2.7 on a $(q, L_{2,3}, 1)$-DDF, we consider a row-radical $(q, L_{r,3}, 1)$-DF over $\mathbb{F}_q$ with $r \geq 3$. It is necessary to suppose $v \equiv 1 \pmod{3r(r+1)}$.

Theorem 3.2.9 (Asymptotic existence for $k = 3$)**.** *For any positive integer $r \geq 3$, let $q \equiv 1 \pmod{3r(r+1)}$ be a prime power with $q > r^2\binom{r+1}{2}^{2r}$. Then there exists a row-radical $(q, L_{r,3}, 1)$-DF over $\mathbb{F}_q$.*

Proof. Set $k = 3$ and $e = 0$ in Theorem 3.2.6 . We have $X_{r,3} = (1-\zeta_3)A_r \cup \Delta^+ A_r$ with $|X_{r,3}| = r + \binom{r}{2} = \binom{r+1}{2}$, which we want to form a system of representatives of $\mathcal{C}^{(|X_{r,3}|)}$. Then it suffices to bound q by setting $n = |X_{r,3}| = \binom{r+1}{2}$ and $s = r$ in Theorem 1.4.8 and using the fact $s^2 n^{2s} > Q(n, s)$ to meet the claim. $\square$

Corollary 3.2.10. *There exists an elementary abelian $(q, L_{3,3}, 1)$-DDF for any prime power $q \equiv 1 \pmod{36}$.*

Proof. It follows from Theorem 3.2.9 that a $(q, L_{3,3}, 1)$-DDF exists for any prime power $q \equiv 1 \pmod{36}$ with $q \geq 105841 > Q\left(\binom{4}{2}, 3\right)$. Let $S_1 = \{p : \text{prime} \mid p \equiv 1 \pmod{36}, p < 105841\}$. For non-prime q, by Lemma 3.2.8, we only need to check the prime powers in $S_2 := \{p^2 \mid p \equiv -1, \pm 17 \pmod{36}, p \leq 307, p : \text{prime}\} \cup \{13^3, 5^6\}$.We have individually checked every $q \in S_1 \cup S_2$ and succeeded in constructing a desired $(q, L_{3,3}, 1)$-DF by Theorem 3.2.6 with $e = 0$. $\square$

Similarly, we can consider a row-radical $(p, L_{r,5}, 1)$-DF.

Theorem 3.2.11 (Asymptotic existence for $k = 5$)**.** *For any positive integer $r \geq 3$, let $p \equiv 1 \pmod{5r(r+3)}$ be a prime with $p \geq r^{2r+2}(\frac{r+3}{2})^{2r}$ such that $\zeta_5 + 1 \notin C^{(\frac{r(r+3)}{2})}$. Then there exists a row-radical $(p, L_{r,5}, 1)$-DF.*

Proof. This is similar to the proof of Theorem 3.2.9. In this case, $X_{r,5} = \{1-\zeta_5, 1-\zeta_5^2\} \cdot A_r \cup \Delta A_r$ is desired to form a system of representatives of $\mathcal{C}^{(|X_{r,5}|)}$. When $\zeta_5 + 1 \notin C^{(|X_{r,5}|)}$, it suffices to bound p by setting $n = |X_{r,5}| = \frac{r(r+3)}{2}$ and $s = r$ in Theorem 1.4.8 and use the fact $s^2 n^{2s} > Q(n, s)$ to meet the claim. $\square$

For $k \geq 5$, we will discuss row-radical $(p, L_{2,k}, 1)$-DFs in details in Section 3.3. For row-radical $(p, L_{3,5}, 1)$-DFs, we have the following:

Corollary 3.2.12. *There exists a row-radical $(p, L_{3,5}, 1)$-DF for any prime $p \equiv 1 \pmod{90}$ satisfying $\zeta_5 + 1 \notin C^{(9)}$.*

Proof. By setting $r = 3$ in Theorem 3.2.11, we can obtain a row-radical $(p, L_{3,5}, 1)$-DDF satisfying the claimed condition with $p > 1,479,142 > Q(9,3)$. We individually checked the remaining admissible primes satisfying $\zeta_5 + 1 \notin C^{(9)}$ and succeeded in constructing the difference families. $\square$

Next, we consider a radical (namely, both row- and column-radical) $(q, L_{r,k}, 1)$-DF. This is actually a very special but nice case of Theorem 3.2.6 obtained by setting $A_r = \{1, \zeta_r, \zeta_r^2, \ldots, \zeta_r^{r-1}\}$. In this case, we can obtain a sufficient cyclotomic condition for the existence. We indicate such a DF is nice because it is quite simple to calculate, in particular when q is not so huge.

Theorem 3.2.13 (Radical DF)**.** *Let $r > k > 1$ be odd integers which are relatively prime. Suppose $q = n \cdot rk(r+k-2)+1$ is a prime power for a positive integer n. There exists a radical $(q, L_{r,k}, 1)$-DF over $\mathbb{F}_q$ if $\frac{1}{\zeta_k - 1} Y_{r,k}$ forms a system of representatives of the cosets of $C^{(h^{e+1})}$ in $C^{(h^e)}$ for a suitable e such that h^e divides n, where*

$$\begin{aligned} Y_{r,k} &= H_r \cup H_k \\ &= \{\zeta_r - 1, \zeta_r^2 - 1, \ldots, \zeta_r^{\frac{r-1}{2}} - 1\} \cup \{\zeta_k - 1, \zeta_k^2 - 1, \ldots, \zeta_k^{\frac{k-1}{2}} - 1\} \end{aligned}$$

and $h = |Y_{r,k}| = \frac{r+k-2}{2}$.

Proof. Since $\Delta^+ A_r = A_r \cdot H_r$, we have $X_{r,k} = A_r \cdot (H_k \cup H_r) = C^{(n \cdot k(r+k-2))} \cdot Y_{r,k}$. Then it is easy to deduce the conclusion from Theorem 3.2.6 by using the fact that $\gcd(r,k) = 1$. $\square$

Remark. Among all the 4679 admissible primes with $p < 1,479,141$ (the bound obtained from Theorem 3.2.11), there are 1058 of them satisfying the existence condition for a radical DF (including 1020 primes with $e = 0$, 36 primes with $e = 1$, and two primes with $e = 2$ which are also the only two satisfying $\zeta_5 + 1 \in C^{(9)}$), where the first two primes are $p = 541$ (with $e = 1$) and $p = 1171$ (with $e = 0$). Moreover, besides the "radical" ones, only 500 of the remaining admissible primes lead to $\zeta_5 + 1 \in C^{(9)}$ (the case when $e = 0$), in which 50 primes satisfy the existence conditions for $e = 1$. The smallest primes p such that we failed to construct a row-radical $(p, L_{3,5}, 1)$-DF are $p = 2161$ and $p = 8461$.

On the other hand, we can consider a row-radical $(p, L_{5,3}, 1)$-DF as a column-radical $(p, L_{3,5}, 1)$-DF. Then we can conclude, by Theorem 3.2.9, that a column-radical $(p, L_{3,5}, 1)$-DF exists for any prime $p \equiv 1 \pmod{90}$ with $p > N = L(15,5) > 1.1810 \times 10^{12}$ (see Table 3.2). However, it is still hard to do a computer search for each prime satisfying $\zeta_5 + 1 \in C^{(9)}$ that less than such a huge N.

By using an idea similar to the constructions of $(q, 6, 1)$-DFs (see Wilson [120]) and $(q, 7, 1)$-DFs (see Chen, Wei, and Zhu [27]), we can efficiently reduce the size of $X_{r,k}$ in Theorem 3.2.6, where a criterion similar to that of $Y_{r,k}$ proposed in Theorem 3.2.13 is necessary. For instance, when $r = 6$ and $k = 5$, we can take $A_r = A_6 = \{1, \alpha\} \cdot \{1, \zeta_3, \zeta_3^2\}$ in Theorem 3.2.6, so that $X_{r,k} = X_{6,5} = \{1, \zeta_3, \zeta_3^2\} \cdot \left(\{1, \alpha\} \cdot Y_{\frac{r}{2},k} \cup \{\alpha - 1, \alpha - \zeta_3, \alpha - \zeta_3^2\}\right)$, where $Y_{\frac{r}{2},k} = Y_{3,5} = \{\zeta_3 - 1, \zeta_5 - 1, \zeta_5^2 - 1\}$ as defined in Theorem 3.2.13. Then we can conclude that, for any prime $p \equiv 1 \pmod{270}$ with $p > 2.82 \times 10^8 > Q(9,4)$ such that each element of $Y_{3,5}$ lies in a distinct coset of $\mathcal{C}^{(9)}$, there exists a row-radical $(p, L_{5,6}, 1)$-DF. Actually, we have verified that such an α does exist for each admissible prime $p < 2^{26}$ ($\approx 6.71 \times 10^7$) whose corresponding $Y_{3,5}$ does not have any pair of elements that lies in the same coset of $\mathcal{C}^{(9)}$ except when $p \in \{541, 1621, 3511, 6481\}$.

3.3 Row-radical $2 \times k$ grid-block difference families with $k \geq 5$

Next, we propose the concepts of good and bad primes for the construction of $(q, L_{2,k}, 1)$-DF with $k \geq 5$.

Definition 3.3.1. Let $k \geq 5$ be odd. Let $p \equiv 1 \pmod{k^2}$ be a prime. If $\frac{1-\zeta_k^i}{1-\zeta_k^j} \notin C^{(k)}$ holds for any $1 \leq j < i \leq \frac{k-1}{2}$, then p is said to be *a good prime* with respect to k, otherwise, *a bad prime*.

In particular, for $k = 5$, if $1 + \zeta_5 \in C^{(5)}$, then p is bad. The following Theorem 3.3.2 characterizes a bad prime with respect to 5 from the aspect of algebraic number theory.

Theorem 3.3.2. *For a prime* $p \equiv 1 \pmod{25}$*,* p *is bad with respect to* 5 *if and only if there exists a primary prime* π *in* $\mathbb{Z}[\zeta_5]$ *such that* $\mathrm{N}(\pi) = p$ *and* $\pi \equiv a \pmod{5}$*, where* $\mathrm{N}(\pi)$ *denotes the norm of* π *and* a *is a rational integer with* $a \not\equiv 0 \pmod{5}$*.*

Before coming to the proof of Theorem 3.3.2, we first present a brief review of basic definitions and properties on the cyclotomic field $\mathbb{Q}(\zeta)$, where ζ denotes a primitive kth root of unity for an odd prime k. We make use the set $\{\zeta^i \mid 1 \leq i \leq k-1\}$ as an integral basis of $\mathbb{Q}(\zeta)$. The conjugate mappings of $\mathbb{Q}(\zeta)/\mathbb{Q}$ are given by $\sigma_i(\zeta) = \zeta^i$ for $1 \leq i \leq k-1$. Hence, for an element $\xi = a_1\zeta + a_2\zeta^2 + \cdots + a_{k-1}\zeta^{k-1}$ with $a_i \in \mathbb{Q}$ $(1 \leq i \leq k-1)$, the conjugate can be expressed by

$$\sigma_i(\xi) = a_1\zeta^i + a_2\zeta^{2i} + \cdots + a_{k-1}\zeta^{(k-1)i}.$$

Denote the complex conjugate of ξ by $\overline{\xi} = \sigma_{k-1}(\xi)$. The norm of ξ is defined by $\mathrm{N}(\xi) = \prod_{i=1}^{k-1} \sigma_i(\xi)$.

The properties of primary ideals in $\mathbb{Q}(\zeta)$ and Kummer's reciprocity law play important roles in the proof. First, it is important to introduce the notion of *primary elements* in $\mathbb{Z}[\zeta]$ for Kummer's reciprocity law.

Definition 3.3.3 (primary cyclotomic integers)**.** Let λ denote the prime $1-\zeta \in \mathbb{Z}[\zeta]$. An element $\alpha \in \mathbb{Z}[\zeta]$ is said to be *primary* if there exists $s \in \mathbb{Z}$ such that the following hold:

$$\alpha \not\equiv 0 \pmod{\lambda}, \quad \alpha \equiv s \pmod{\lambda^2}, \quad \text{and} \quad \alpha\overline{\alpha} \equiv s^2 \pmod{k}.$$

Remark. For any $\alpha \in \mathbb{Z}[\zeta]$ satisfying $\alpha \not\equiv 0 \pmod{\lambda}$, if k is a *regular prime* (i.e., the class number of $\mathbb{Q}(\zeta)$ is not divisible by k), then there exists a unit $u \in \mathbb{Z}[\zeta]^\times$ such that αu is primary.

Let $\alpha, \pi \in \mathbb{Z}[\zeta]$, where $\pi \neq \lambda$ is a prime. We denote by $\left(\frac{\alpha}{\pi}\right)_k$ the kth power residue symbol of α modulo π. We now state Kummer's reciprocity law.

Theorem 3.3.4 (Kummer's reciprocity law)**.** *Let $\pi, \psi \in \mathbb{Z}[\zeta]$ be two distinct primary elements with $(\pi, \psi) = 1$. Then,*

$$\left(\frac{\psi}{\pi}\right)_k \left(\frac{\pi}{\psi}\right)_k^{-1} = 1.$$

Definition 3.3.5 (Kummer's quotients of logarithmic derivatives)**.** Let $\alpha = a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{k-1}\zeta^{k-1}$ be an element in $\mathbb{Z}[\zeta]$ with $\lambda \nmid \alpha$. Let

$$\alpha(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1} \in \mathbb{Z}[x],$$

then *Kummer's quotients of logarithmic derivatives* are defined by

$$\ell_i(\alpha) = \begin{cases} \left.\frac{\mathrm{d}^i \log \alpha(e^x)}{\mathrm{d}x^i}\right|_{x=0} & \text{if } i = 1, 2, \ldots, k-2, \\ \left.\frac{\mathrm{d}^{k-1} \log \alpha(e^x)}{\mathrm{d}x^{k-1}}\right|_{x=0} + \frac{\alpha(1)-1}{k} & \text{if } i = k-1, \alpha \equiv 1 \pmod{\lambda}. \end{cases}$$

Remark. Kummer's quotients of logarithmic derivatives $\ell_i(\alpha)$ are independent of the representation of α. In other words, $\ell_i(\alpha)$ is uniquely determined by modulo k for each $1 \leq i \leq k-1$.

Theorem 3.3.6 (Kummer's complementary law)**.** *If $\alpha \in \mathbb{Z}[\zeta]$ is a primary prime, then $\left(\frac{k}{\alpha}\right)_k = \zeta^{\frac{\ell_k(\alpha)}{k}}$. (If $\alpha \equiv 1 \pmod{\lambda}$, then α is not necessarily primary.) Moreover,*

$$\left(\frac{u}{\alpha}\right)_k = \zeta^{\ell_1(u)\frac{\mathrm{N}(\alpha)-1}{k} + \sum_{i=1}^{\frac{k-3}{2}} \ell_{2i}(u)\ell_{k-2i}(\alpha)} \tag{3.12}$$

for any $u \in \mathbb{Z}[\zeta]^\times$.

By employing Kummer's reciprocity law (Theorem 3.3.4) and complementary law (Theorem 3.3.6), we prove Theorem 3.3.2 as follows:

Proof. (Proof of Theorem 3.3.2). Since $\mathbb{Z}[\zeta]$ is a principal ideal domain, there must exist a prime π such that $\mathfrak{p} = (\pi)$. Since 5 is a regular prime, without loss of generality, we suppose π is a primary prime. Then, p is bad if and only if $\left(\frac{\zeta+1}{\pi}\right)_5 = 1$. Recall that $\mathrm{N}(\pi) = p \equiv 1 \pmod{5^2}$, thus $\zeta^{\frac{\mathrm{N}(\pi)-1}{5}} = 1$. By substituting $u = 1 + \zeta$ and $\alpha = \pi$ in (3.12) of Kummer's complementary law (Theorem 3.3.6), we obtain the following equivalent criterion for p to be a bad prime:

$$\left(\frac{\zeta+1}{\pi}\right)_5 = \zeta^{\ell_2(1+\zeta)\ell_3(\alpha)} = 1. \tag{3.13}$$

Now we calculate the exponent explicitly. The first factor is

$$\ell_2(1+\zeta) = \left.\frac{\mathrm{d}^2\log(1+e^x)}{\mathrm{d}x^2}\right|_{x=0} = \frac{1}{4} \equiv -1 \pmod{5}. \tag{3.14}$$

Next, we suppose $\pi = a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$, then the second factor is

$$\ell_3(\pi) = \left.\frac{\mathrm{d}^3\log(a_0 + a_1e^x + a_2e^{2x} + a_3e^{3x})}{\mathrm{d}x^3}\right|_{x=0}$$

On the other hand, π is primary if and only if there exist $s, t \in \mathbb{Z}$ with $s \not\equiv 0 \pmod{5}$, such that the following hold:

$$a_0 \equiv s + 2t, \quad a_1 \equiv -t, \quad a_2 \equiv t, \quad a_3 \equiv -2t \pmod{5}.$$

Therefore,

$$\ell_3(\pi) \equiv \frac{-2s^2t}{s^3} = \frac{-2t}{s} \pmod{5}. \tag{3.15}$$

In summary, it can be derived from (3.13), (3.14), and (3.15) that $\left(\frac{\zeta+1}{\pi}\right)_5 = \zeta^{\frac{2t}{s}} = 1$, which implies $t \equiv 0 \pmod{5}$. Therefore, there must exist $a \in \mathbb{Z}$ with $a \not\equiv 0 \pmod{5}$ such that $\pi \equiv a \pmod{5}$ when p is a bad prime with respect to 5. □

In general, it is possible to give the explicit condition for a prime $p \equiv 1 \pmod{k^2}$ to be a bad prime with respect to any odd prime k. However, the calculation would be complicated and the results may not have a simple form of congruences. For instance, when $k = 7$, we denote by ζ the 7th root of unity. Then, a necessary condition for a prime $p \equiv 1 \pmod{7^2}$ to be a bad prime with respect to 7 is

$$\pi \equiv \begin{cases} a + b(\zeta + 3\zeta^3 - 2\zeta^4 + \zeta^5), \\ a + b(\zeta + 3\zeta^2 + \zeta^3 - 2\zeta^5), \quad \text{or} \\ a + b(\zeta - \zeta^2 - \zeta^3 + 2\zeta^4 + 2\zeta^5). \end{cases} \pmod{7} \tag{3.16}$$

for $a \not\equiv -3b \pmod{7}$. For further information on reciprocity laws, algebraic numbers, and cyclotomic fields, the interested reader is referred to [69], [99], [117], and [118].

Example 3.3.7. For $p = 1151$, we can choose $\pi = 2 - 5\zeta_5 - 10\zeta_5^2 - 5\zeta_5^3$ as a primary prime in $\mathbb{Z}[\zeta_5]$ which divides 1151. Since $\pi \equiv 2 \pmod{5}$, it follows from Theorem 3.3.2 that $p = 1151$ is a bad prime with respect to 5.

Example 3.3.8. For $p = 1667$, the smallest bad prime with respect to 7, we can choose $\pi = 1 - 4\zeta - 5\zeta^2 - 4\zeta^3 + 7\zeta^4 - 6\zeta^5 \equiv 1 - 4(\zeta + 3\zeta^2 + \zeta^3 - 2\zeta^5) \pmod{7}$ to meet the criterion in (3.16).

Remark. All of the bad primes $p \equiv 1 \pmod{25}$ with respect to 5 with $p < 10^4$ are 1151, 1601, 1951, 3001, 3251, 3851, 4651, 4751, 5801, 6101, 7451, and 9901.

Table 3.3: Parameters for some $(p, L_{2,5}, 1)$-DDF

p	n	e	g	ζ_5	α	p	n	e	g	ζ_5	α
101	2	0	2	95	11	3001	60	1	23	1125	54
151	3	0	7	8	13	3251	65	1	23	1364	481
251	5	0	11	219	13	4751	95	1	19	3944	346

Corollary 3.3.9. *There exists a cyclic $(p, L_{2,5}, 1)$-DDF for every good prime $p \equiv 1 \pmod{50}$.*

Proof. For a good prime p, $\zeta_5 - 1$ and $\zeta_5^2 - 1$ must lie in different cyclotomic classes, say $\zeta_5 - 1 \in C_i^{(5)}$ and $\zeta_5^2 - 1 \in C_j^{(5)}$, where $i \neq j$ and $i, j \in \mathbb{Z}_5$. If there exists $\alpha \in C_{2i-2j}^{(5)}$ such that $\alpha - 1 \in C_{2j-1}^{(5)}$, then $X_{2,5} = \{\zeta_5 - 1, \zeta_5^2 - 1, \alpha(\zeta_5 - 1), \alpha(\zeta_5^2 - 1), \alpha - 1\}$ is desired to be a system of representatives of $\mathcal{C}^{(5)}$. This is the case when $e = 0$ in Theorem 3.2.6 . So it suffices to show the existence of such an element $\alpha \in \mathbb{F}_p^*$. Then, by setting $n = 5$ and $s = 2$ in Theorem 1.4.8, we have $Q(5, 2) \approx 275.6$, which implies a $(p, L_{2,5}, 1)$-DDF exists for any admissible prime $p > 275$. For each of the remaining three primes, namely $p \in \{101, 151, 251\}$, we list a suitable α in Table 3.3. $\square$

Remark. If we consider the cases when $r = 2$, $k = 5$, and $e = 1$ in Theorem 3.2.6, then a $(p, L_{2,5}, 1)$-DDF can be constructed for a bad prime $p \in \{3001, 3251, 4751\}$. See Table 3.3 for details.

Now we begin to consider a $(q, L_{2,5}, 1)$-DF when q is a prime power but is not necessarily a prime.

By Theorem 3.2.6, for $r = 2$ and $k = 5$, it is necessary to check if $1 + \zeta_5$ is a 5^{e+1}th power in $\mathbb{F}_q^*$. In other words, we have to investigate if $(1 + \zeta_5)^{\frac{q-1}{5^{e+1}}}$ is 1. Let $q = p^s$ with prime p. The congruence $q \equiv 1 \pmod{50}$ holds exactly in the following cases:

(i) $p \equiv 1 \pmod{50}$ and s arbitrary,

(ii) $p \equiv -1 \pmod{50}$ and s even,

(iii) $p \equiv \pm 7 \pmod{50}$ and $4 \mid s$,

(iv) $p \equiv 1 \pmod{10}$ and $5 \mid s$,

(v) $p \equiv -1 \pmod{10}$ and $10 \mid s$.

The following Lemma 3.3.10 characterizes each case.

Lemma 3.3.10. *The following hold when p is a prime:*

(i) For $p \equiv 1 \pmod{50}$, Theorem 3.2.6 gives a $(p^s, L_{2,5}, 1)$-DF if and only if it gives a $(p, L_{2,5}, 1)$-DF.

(ii) For $p \equiv -1 \pmod{50}$, Theorem 3.2.6 gives no $(p^{2s}, L_{2,5}, 1)$-DF.

Table 3.4: Cyclic $(p, L_{2,k}, 1)$-DDFs for $k \geq 7$ and $p < 2 \times 10^4$

k	p	n	g	ζ_k	α	k	p	n	g	ζ_k	α
7	491	5	2	138	25	7	883	9	2	707	20
7	1471	15	7	785	7	7	2549	26	2	2119	5
7	5881	60	31	4332	10	7	6469	66	2	1833	12
7	6959	71	7	2841	56	7	7253	74	2	3268	7
7	7351	75	7	6671	93	7	8429	86	2	6249	2
7	8527	87	5	6472	7	7	11369	116	3	5420	13
7	16661	170	11	12349	21	9	2593	16	7	251	43
9	3889	24	11	923	21	9	15391	95	17	13218	18
9	17659	109	3	10277	62	11	727	3	5	662	173
11	17183	71	5	14225	44	13	9803	29	2	2774	36

(iii) *For* $p \equiv \pm 7 \pmod{50}$, *Theorem 3.2.6 gives no* $(p^{4s}, L_{2,5}, 1)$*-DF.*

(iv) *For* $p \equiv 1 \pmod{10}$, *Theorem 3.2.6 gives a* $(p^{5s}, L_{2,5}, 1)$*-DF if and only if it gives a* $(p^5, L_{2,5}, 1)$*-DF.*

(v) *For* $p \equiv -1 \pmod{10}$, *Theorem 3.2.6 gives no* $(p^{10s}, L_{2,5}, 1)$*-DF.*

Proof. (i) and (iv) are direct consequences of Lemma 3.2.8. Similarly, it suffices to consider the following cases by Lemma 3.2.8:

(ii) For $q = p^2$, since $p+1 \equiv 0 \pmod{50}$, we have $n = \frac{p^2-1}{50} \equiv 0 \pmod{p-1}$. Moreover, since $\gcd(p-1, 5) = 1$, we have $\frac{p^2-1}{5^{e+1}} = \frac{50n}{5^{e+1}} = 5r(p-1)$ with $r = \frac{2n}{5^e(p-1)}$. Then, $(1+\zeta_5)^{\frac{q-1}{5^{e+1}}} = (1+\zeta_5)^{5r(p-1)} = \big((1+\zeta_5)^{-1}(1+\zeta_5^p)\big)^{5r} = \big((1+\zeta_5)^{-1}(1+\zeta_5^{-1})\big)^{5r} = (\zeta_5^{-1})^{5r} = 1$. Therefore, in this case, the criteria in Theorem 3.2.6 cannot be satisfied.

(iii) For $q = p^4$, since $p^2+1 \equiv 0 \pmod{50}$, we have $n = \frac{p^4-1}{50} \equiv 0 \pmod{p+1}$. Moreover, since $\gcd(p+1, 5) = 1$, we have $\frac{p^4-1}{5^{e+1}} = \frac{50n}{5^{e+1}} = 5r(p+1)$ with $r = \frac{2n}{5^e(p+1)}$ is even. Then, $z := (1+\zeta_5)^{\frac{q-1}{5^{e+1}}} = (1+\zeta_5)^{5r(p+1)} = \big((1+\zeta_5)(1+\zeta_5^p)\big)^{5r}$. Thus $z = (-\zeta_5^4)^{5r} = 1$ if $p \equiv 7 \pmod{50}$, and $z = (-\zeta_5^2)^{5r} = 1$ if $p \equiv -7 \pmod{50}$. Therefore, in this case, Theorem 3.2.6 cannot be used.

(v) For $q = p^{10}$, we have $p^5 \equiv -1 \pmod{50}$. Then one can obtain $(1+\zeta_5)^{\frac{q-1}{5^{e+1}}} = (1+\zeta_5)^{\frac{(p^5)^2-1}{5^{e+1}}} = 1$ by proceeding similarly to case (ii), which indicates that Theorem 3.2.6 cannot be used in this case.

□

Example 3.3.11. More examples of cyclic $(p, L_{2,k}, 1)$-DDFs for $k \geq 7$ are shown in Table 3.4.

3.4 Kronecker density related to row-radical $2 \times k$ grid-block difference families

In this section, we consider the existence of row-radical $(p, L_{2,k}, 1)$-DFs with prime p from the viewpoint of Kronecker density.

Let K be a Galois extension of an algebraic number field F. For some $\sigma \in \mathrm{Gal}(K/F)$, let C_σ denote the conjugate class of σ, i.e., $C_\sigma = \{\tau\sigma\tau^{-1} \mid \tau \in \mathrm{Gal}(K/F)\}$. Then we define a set M_σ of prime ideals in F for given σ as follows:

$$M_\sigma = \{\mathfrak{P} \cap F \mid \mathfrak{P} \text{ is a prime ideal in } K \text{ such that } \sigma_{\mathfrak{P}} \in C_\sigma\},$$

where $\sigma_{\mathfrak{P}}$ is the Frobenius automorphism of $\mathfrak{P}$ over K. Now we investigate the Kronecker density of primes with specific properties by using Chebotarëv's Density Theorem (see [99] §25.3) concerning Galois extensions.

Theorem 3.4.1 (Chebotarëv's Density Theorem)**.** *The Kronecker density $\delta(M_\sigma)$ of M_σ is equal to $\frac{|C_\sigma|}{|\mathrm{Gal}(K/F)|}$, i.e.,*

$$\delta(M_\sigma) = \lim_{s \to 1+0} \sum_{\mathfrak{p} \in M_\sigma} \frac{1}{\mathrm{N}(\mathfrak{p})} \Big/ \log \frac{1}{s-1} = \frac{|C_\sigma|}{|\mathrm{Gal}(K/F)|},$$

where $\mathrm{N}(\mathfrak{p})$ is the norm of the prime ideal $\mathfrak{p}$ in K. If the extension K/F is abelian, then there exist infinitely many prime ideals in F, say $\mathfrak{p}$, such that $(\mathfrak{p}, K/F) = \sigma$ for each $\sigma \in \mathrm{Gal}(K/F)$, and the density of the set of all those prime ideals is equal to $\frac{1}{[K:F]}$, where $(\mathfrak{p}, K/F)$ is the Artin symbol.

For simplicity, we slightly change the notation in this section. Let ζ_0 denote a primitive k^2-th root of unity and $\zeta = \zeta_0^k$ in $\mathbb{F}_p^*$. Then, for $p \equiv 1 \pmod{k^2}$, we can see that $\left(\frac{\alpha}{\mathfrak{p}}\right)_k = 1$ if and only if $(\mathfrak{p}, \mathbb{Q}(\zeta_0, \sqrt[k]{\alpha})/\mathbb{Q}(\zeta_0)) = \mathrm{id}$.

3.4.1 The Kronecker density of "good" primes

In this subsection, we give a number theoretic discussion of the criteria for p to be a "bad" prime. Let $p \equiv 1 \pmod{k^2}$ be a prime. For any odd integer k, this congruence is equivalent to $p \equiv 1 \pmod{2k^2}$.

In Corollary 3.3.9, we settled a necessary condition for the construction of $(p, L_{2,5}, 1)$-DFs (see also Definition 3.3.1):

$$\zeta + 1 \notin C^{(5)}. \tag{$\mathtt{C}_5$}$$

Under the assumption that $p \equiv 1 \pmod{25}$, the primes satisfying the condition $(\mathtt{C}_5)$ are said to be *"good" primes*, otherwise, *"bad" primes*. It follows from the following lemma that, among all the primes satisfying $p \equiv 1 \pmod{50}$, the ratios (densities) of "good" primes and "bad" primes are respectively $\frac{4}{5}$ and $\frac{1}{5}$.

Lemma 3.4.2. *For $k = 5$, the Kronecker densities of "good" primes and "bad" primes are respectively $\frac{1}{25}$ and $\frac{1}{100}$.*

Proof. Denote $F = \mathbb{Q}(\zeta_0)$ and $K = F(\sqrt[5]{1+\zeta})$. Let $\mathfrak{p}$ be a prime ideal in $\mathbb{Z}[\zeta_0]$ lying over (p) and let $\sigma_{\mathfrak{p}} := (\mathfrak{p}, K/F)$ (the Artin symbol). Then $p \equiv 1 \pmod{25}$ is "good" if, and only if, $\sigma_{\mathfrak{p}}(\sqrt[5]{1+\zeta}) \neq \sqrt[5]{1+\zeta}$. Note that $[K : F] = 5$ and $[F : \mathbb{Q}] = \varphi(25) = 20$. By Chebotarëv's Density Theorem 3.4.1, the Kronecker density of "bad" primes is

$$\delta_b(5) = \frac{1}{5} \cdot \frac{1}{20} = \frac{1}{100}.$$

Accordingly, the Kronecker density of "good" primes is

$$\delta_g(5) = \left(1 - \frac{1}{5}\right) \cdot \frac{1}{20} = \frac{1}{25}.$$

□

One can check that, among the first 10,000 primes, there are 101 "bad" primes not satisfying condition ($\mathtt{C_5}$). The ratio is extremely close to 1/100.

In general, let $k \geq 5$ be an odd prime. With the notation of Definition 3.3.1, denote $d = \frac{k-1}{2}$, and $\eta_{ij} = \sqrt[k]{\frac{1-\zeta^i}{1-\zeta^j}}$ for each $1 \leq j < i \leq d$. For $p \equiv 1 \pmod{k^2}$, we consider $F := \mathbb{Q}(\zeta_0)$ and $K := F(\eta_{21}, \eta_{31}, \ldots, \eta_{d1})$ in what follows.

It is desired that $H_k \cup \alpha H_k \cup \{\alpha - 1\}$ forms a system of representatives of $\mathcal{C}^{(k)}$ for some $\alpha \in \mathbb{F}_p^*$, where

$$H_k = \left\{\zeta^i - 1 \,\middle|\, i \in \{1, 2, \ldots, d\}\right\}.$$

Therefore, as a generalization of ($\mathtt{C_5}$), we have a necessary condition for $k \geq 5$ as follows:

$$\eta_{ij}^k \notin C_0^{(k)}, \qquad \text{for any } 1 \leq j < i \leq d. \tag{$\mathtt{C_k}$}$$

The primes satisfying condition ($\mathtt{C_k}$) are said to be *"good" primes* with respect to k, otherwise, *"bad" primes.*

Lemma 3.4.3. *For an odd prime k, let $\delta_g(k)$ and $\delta_b(k)$ denote the Kronecker densities, respectively, of "good" and "bad" primes with respect to k. Then,*

$$\delta_g(k) = \frac{(k-1)!}{(k-d)! \cdot k^{d-1}} \cdot \frac{1}{k(k-1)},$$
$$\delta_b(k) = \left(1 - \frac{(k-1)!}{(k-d)! \cdot k^{d-1}}\right) \frac{1}{k(k-1)}.$$

Proof. Note that $\eta_{ij} = \frac{\eta_{i1}}{\eta_{j1}}$ holds for any i, j. Moreover, $\{\eta_{21}, \eta_{31}, \ldots, \eta_{d1}\}$ is multiplicatively independent when k is prime. (However, for any d-tuple of η_{ij}'s, it may not be independent.) Hence, K/F is an abelian extension whose Galois group is of type $(\underbrace{k, k, \ldots, k}_{d-1 \text{ times}})$. Accordingly, we have

$$\mathrm{Gal}(K/F) \cong \prod_{i=2}^{d} \mathrm{Gal}(F(\eta_{i1})/F).$$

Moreover, $p \equiv 1 \pmod{k^2}$ is "good" with respect to k, if and only if $\sigma_{\mathfrak{p}}(\eta_{ij}) \neq \eta_{ij}$ holds for every $1 \leq j < i \leq d$, where $\mathfrak{p}$ is a prime ideal in $\mathbb{Z}[\zeta_0]$ lying over (p), and $\sigma_{\mathfrak{p}} := (\mathfrak{p}, K/F)$ (the Artin symbol). By applying Chebotarëv's Density Theorem 3.4.1, we can deduce the Kronecker densities of "good" and "bad" primes with respect to k as follows:

$$\delta_g(k) = \frac{\lambda(k)}{k^{d-1}} \cdot \frac{1}{\varphi(k^2)} \quad \text{and} \quad \delta_b(k) = \left(1 - \frac{\lambda(k)}{k^{d-1}}\right) \frac{1}{\varphi(k^2)},$$

where $\lambda(k)$ denotes the number of elements of $\mathrm{Gal}(K/F)$ which do not leave η_{ij} fixed for all $1 \leq j < i \leq d$, i.e.,

$$\lambda(k) = \left|\left\{\sigma \in \mathrm{Gal}(K/F) \mid \sigma(\eta_{ij}) \neq \eta_{ij},\ 1 \leq j < i \leq d\right\}\right|.$$

Suppose $\sigma_i \in \mathrm{Gal}(F(\eta_{i1})/F)$ for $2 \leq i \leq d$. First, there are $(k-1)$ ways to choose a σ_2 which does fix η_{21}. Next, there are $(k-2)$ ways to choose a σ_3 so that $\langle \sigma_2, \sigma_3 \rangle$ does not fix η_{31} and η_{32}. Analogously, the number of choices of σ_d is $(k-d+1)$. Thus, we have $\lambda(k) = (k-1)(k-2)\cdots(k-d+1) = \frac{(k-1)!}{(k-d)!}$. Last, by combining with the fact that $[F : \mathbb{Q}] = \varphi(k^2) = k(k-1)$, we complete the proof. $\square$

3.4.2 The Kronecker density of "arithmetic" primes

Now we begin to study the condition that $H_k \cup \alpha H_k \cup \{\alpha - 1\}$ forms a system of representatives of $\mathcal{C}^{(k)}$ for an element $\alpha \in \mathbb{F}_p^*$. In other words, if we denote

$$R_k = \{\log_g x \pmod{k} \mid x \in H_k\},$$

then this is equivalent to considering the following condition:

$$R_k \cup (R_k + a) \cup \{b\} = \mathbb{Z}_k, \tag{$\mathtt{R_k}$}$$

where $a = \log_g \alpha$, $b = \log_g(1-\alpha)$ and $\log_g x$ denotes the discrete logarithm of $x \in \mathbb{F}_p^*$ to a primitive element $g \in \mathbb{F}_p^*$.

It is remarkable that $|R_k| = \frac{k-1}{2}$, provided that the equality ($\mathtt{R_k}$) holds, namely, p is a "good" prime with respect to k.

In order to characterize the condition ($\mathtt{R_k}$), we first introduce some definitions. For an odd k, let S be a subset of $\mathbb{Z}_k$ with $|S| = \frac{k-1}{2}$. S is said to be *arithmetic* if there exists $a \in \mathbb{Z}_k$ such that $S \cap (S+a) = \emptyset$. Conversely, if $S \cap (S+a) = \emptyset$ holds, then S is said to be *a-arithmetic*. Then, the only element, say b, in $\mathbb{Z}_k \setminus (S \cup (S+a))$ can be uniquely determined, which is called the *exceptional element* of S.

Proposition 3.4.4. Given $a, b \in \mathbb{Z}_k$, the a-arithmetic subset having b as its exceptional element is unique, that is, $\{a+b, 3a+b, \ldots, (k-2)a+b\}$.

Proof. It is clear that, if $\gcd(a,k) = 1$ (which must hold when k is prime), then $\mathbb{Z}_k = \{b, a+b, 2a+b, \ldots, (k-1)a+b\}$ holds for any b. Suppose S is an a-arithmetic subset having b as its exceptional element. Then, $b \notin S$. Moreover,

$S' := S + a = \mathbb{Z}_k \setminus (S \cup \{b\})$ should hold. Hence, $a + b \notin S'$, otherwise, $b \in S$. Thus, $a + b \in S$. Thereby, we consequently have $2a + b \in S'$, $3a + b \in S$, ... Finally, we uniquely determine $S = \{a + b, 3a + b, 5a + b, \ldots, (k-2)a + b\}$. $\square$

More precisely, we can rewrite R_k as follows by avoiding the usage of discrete logarithms:

$$R_k = \left\{ s \in \mathbb{Z}_k \,\middle|\, \left(\frac{1-\zeta^i}{\mathfrak{p}}\right) = \zeta^s,\ 1 \leq i \leq \frac{k-1}{2} \right\},$$

where $\mathfrak{p}$ is a prime ideal in $\mathbb{Z}[\zeta_0]$ lying over (p). A prime $p \equiv 1 \pmod{k^2}$ is said to be *"arithmetic"* with respect to k if p is "good" and R_k is arithmetic. The property of being arithmetic is independent of the choice of the ideal $\mathfrak{p}$.

Lemma 3.4.5. *For an odd prime k, let $\delta_a(k)$ denote the Kronecker density of "arithmetic" primes with respect to k. Then*

$$\delta_a(k) = \frac{d \cdot d!}{k^{d-1}} \cdot \frac{1}{k(k-1)}.$$

Proof. Let S be an a-arithmetic subset having b as the exceptional element. Then, $-S + (2b - a) = -\{a + b, 3a + b, \ldots, (k-2)a + b\} + (2b - a) = \{b - 2a, b - 4a, \ldots, b - (k-1)a\} \equiv S \pmod{k}$, i.e., S is also a $(-a)$-arithmetic subset having $b - a$ as the exceptional element. In general, for any arithmetic subsets $T \subset \mathbb{Z}_k$, there exist exactly two pairs $(u, w), (u', w') \in \mathbb{Z}_k^2$ such that $S = uT + w$ and $S = u'T + w'$ hold, where $u' = -u$, $w' = -w + 2b + a$. In other words, each arithmetic subset has exactly two presentations in terms of the pairs (a, b) and $(-a, b - a)$. Therefore, the number of all arithmetic subsets of $\mathbb{Z}_k$ is $\frac{k\varphi(k)}{2} = \frac{k(k-1)}{2}$. By considering the orders of elements in R_k, we have $\frac{k(k-1)}{2} \cdot \left(\frac{k-1}{2}\right)!$ different ways to determine which cyclotomic class $(1 - \zeta^i)$ lies in. Furthermore, since a cyclic permutation acting on R_k (regarded as an ordered set) does not change the value of η_{ij} for each $1 \leq j < i \leq \frac{k-1}{2}$, by a similar procedure as in the proof of Lemma 3.4.3, we assert that the ratio of the "arithmetic" primes among the "good" primes is $(d \cdot d!)/\frac{(k-1)!}{(k-d)!}$. Combining with the expression of $\delta_g(k)$ in Lemma 3.4.3, we have $\delta_a(k) = \frac{d \cdot d!}{k^{d-1}} \cdot \frac{1}{k(k-1)}$. $\square$

Remark. For $k = 5$, a prime p is "arithmetic" if and only if it is "good".

In particular, given a nonzero α satisfying ($\mathtt{C_k}$), the condition ($\mathtt{R_k}$) can be satisfied for infinitely many primes. Therefore, the following theorem is straightforward from Lemma 3.4.5:

Theorem 3.4.6. *There are infinitely many row-radical $L_{2,k}$-DFs when k is an odd prime.*

3.5 Recursive constructions

In this section, we present a recursive construction of $(v, L_{r,k}, 1)$-DDF by using difference matrices. Let G be an additive group. Let $\Gamma = (V, E)$ be a graph with $V = \{x_1, x_2, \ldots, x_k\}$. A $k \times |G|$ matrix M with entries from G and row vectors $\boldsymbol{r}_1, \boldsymbol{r}_1, \ldots, \boldsymbol{r}_k$ is called a $(G, \Gamma, 1)$-*difference matrix (DM for short)* if $\boldsymbol{r}_i - \boldsymbol{r}_j$ covers all elements of G exactly once for every $\{x_i, x_j\} \in E$. Moreover, if $\boldsymbol{r}_i$ contains no repeated entries for any $1 \leq i \leq k$, then we say M is a $(G, \Gamma, 1)^*$-DM.

Clearly, the existence of a $(G, \Gamma, 1)$-DM (resp., a $(G, \Gamma, 1)^*$-DM) implies that of a $(G, \Gamma', 1)$-DM (resp., a $(G, \Gamma', 1)^*$-DM) for any subgraph Γ' of Γ. When Γ is the complete graph K_k, a $(G, \Gamma, 1)$-DM is also known as a $(G, k, 1)$-DM. It is clear that a $(G, k+1, 1)$-DM can give a $(G, K_k, 1)^*$-DM. In particular, an $(\mathbb{F}_q, q, 1)$-DM (resp., an $(\mathbb{F}_q, q-1, 1)^*$-DM) can be created by simply taking the multiplicative table of $\mathbb{F}_q$ (and removing the row multiplied by 0).

Proposition 3.5.1. For every prime power q and every graph Γ of order not greater than $q-1$, there exists an $(\mathbb{F}_q, \Gamma, 1)^*$-DM.

By using the notion of $(G, \Gamma, 1)^*$-DM, we can obtain the recursive constructions of $(v, \Gamma, 1)$-DDF, which generalize the recursive constructions of $(v, \Gamma, 1)$-DF (see [20, 22, 60, 61]), and $(v, k, 1)$-DDF (see [24, 49]).

Theorem 3.5.2. *If there exist a $(G_1, \Gamma, 1)$-DDF, a $(G_2, \Gamma, 1)^*$-DM, and a $(G_2, \Gamma, 1)$-DDF, then there exists a $(G_1 \oplus G_2, \Gamma, 1)$-DDF. In particular, if $G_1 = \mathbb{Z}_u$ and $G_2 = \mathbb{Z}_v$, then there exists a $(\mathbb{Z}_{uv}, \Gamma, 1)$-DDF.*

Proof. This is very similar to the proof of [20] Theorem 3.2 and [22] Theorem 7.3 due to Buratti and Pasotti on $(v, \Gamma, 1)$-DF. The disjointness of the resultant DDF is guaranteed by the disjointness of the "ingredient DDFs", and the definition of a $(G_2, \Gamma, 1)^*$-DM. Actually, the case when Γ is not complete are weaker than that of Fuji-Hara, Miao, and Shinohara [49] Theorem 2.2 on complete sets of DDF, and Chang and Ding [24] Proposition 26 on DDF (for the case of cyclic groups). Thus we omit the proof and refer the readers to the above literature. □

Corollary 3.5.3. *Let $q_1, q_2, \ldots, q_s$ be prime powers and suppose that there exists a $(q_i, L_{r,k}, 1)$-DDF over $\mathbb{F}_{q_i}$for every $1 \leq i \leq s$. Then there exists a $(q_1 q_2 \cdots q_s, L_{r,k}, 1)$-DDF over $\bigoplus_{i=1}^{s} \mathbb{F}_{q_i}$. In particular, if $q_1, q_2, \ldots, q_s$ are primes, then there exists a cyclic $(q_1 q_2 \cdots q_s, L_{r,k}, 1)$-DDF.*

Proof. Since the existence of a $(q, L_{r,k}, 1)$-DF requires $q \equiv 1 \pmod{rk(r+k-2)}$, there must be $q - 1 > rk$ for $r + k \geq 4$. By Proposition 3.5.1, an $(\mathbb{F}_q, L_{r,k}, 1)^*$-DM always exists. By repeatedly applying Theorem 3.5.2 together with the DM, we can obtain the desired DDF. □

Example 3.5.4 (A cyclic $(37{\times}19, L_{2,3}, 1)$-DF)**.** Define a $(\mathbb{Z}_{19}, K_6, 1)$-DM (which is obviously a $(\mathbb{Z}_{19}, L_{2,3}, 1)$-DM) by $D = (d_{ij})$ with $d_{ij} \equiv ij \pmod{19}$ for

$1 \le i \le 6$ and $1 \le j \le 19$ as follows:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 0 \\ 2 & 4 & 6 & 8 & 10 & 12 & 14 & 16 & 18 & 1 & 3 & 5 & 7 & 9 & 11 & 13 & 15 & 17 & 0 \\ 3 & 6 & 9 & 12 & 15 & 18 & 2 & 5 & 8 & 11 & 14 & 17 & 1 & 4 & 7 & 10 & 13 & 16 & 0 \\ 4 & 8 & 12 & 16 & 1 & 5 & 9 & 13 & 17 & 2 & 6 & 10 & 14 & 18 & 3 & 7 & 11 & 15 & 0 \\ 5 & 10 & 15 & 1 & 6 & 11 & 16 & 2 & 7 & 12 & 17 & 3 & 8 & 13 & 18 & 4 & 9 & 14 & 0 \\ 6 & 12 & 18 & 5 & 11 & 17 & 4 & 10 & 16 & 3 & 9 & 15 & 2 & 8 & 14 & 1 & 7 & 13 & 0 \end{pmatrix}$$

Denote $S_j = \begin{bmatrix} d_{1j} & d_{2j} & d_{3j} \\ d_{4j} & d_{5j} & d_{6j} \end{bmatrix}$ with the entries in the j-th column of D. By using the base grid-blocks in Example 3.2.3, for each $1 \le j \le 19$, we define

$$\mathcal{B}_j = \left\{ \begin{bmatrix} 1 & 26 & 10 \\ 2 & 15 & 20 \end{bmatrix} + 37 \cdot S_j,\ \begin{bmatrix} 6 & 8 & 23 \\ 12 & 16 & 9 \end{bmatrix} + 37 \cdot S_j \right\}.$$

Next, by using the base grid-block of a cyclic $(19, L_{2,3}, 1)$-DF, we denote

$$\mathcal{B}_0 = \left\{ 37 \cdot \begin{bmatrix} 1 & 7 & 11 \\ 3 & 2 & 14 \end{bmatrix} \right\}.$$

Then, $\bigcup_{j=0}^{19} \mathcal{B}_j$ is the set of base grid-blocks of a cyclic $(37 \times 19, L_{2,3}, 1)$-DF.

Chapter 4

Resolvable grid-block coverings

For practical applications, in order to run an experiment such that all the treatments (viz. a parallel class) can be performed simultaneously with each other, *resolvability* is taken into account. However, "designs" do not always exist, especially when resolvability is desired.

In the case when $r = k$ is odd, Mutoh, Jimbo, and Fu [85] proposed a construction of resolvable $r \times k$ grid-block designs via cyclic $L_{r,k}$-DF with mutually disjoint base grid-blocks. We will generalize their work in Section 4.1.

Moreover, in the application to group testing for identifying all defective items, it is usually desired to test every pair of items at least once. Thus *coverings* are more desirable than packings. In a resolvable $(v, r \times k, 1)$ grid-block covering, the number of parallel classes ρ should satisfy $\rho \geq \lceil \frac{v-1}{r+k-2} \rceil$. If the equality holds, the covering is said to be *optimal.*

In Section 4.2, we will characterize the optimal resolvable $2 \times c$ grid-block coverings for any $c > 2$. Then, in Section 4.3, we will prove that an optimal resolvable 2×3 grid-block covering with v points exists if and only if $v \equiv 0 \pmod 6$.

4.1 Construction of resolvable grid-block designs via grid-block difference families

A $(q, L_{r,k}, 1)$-DDF has been used for constructions of resolvable grid-block designs and packings by Mutoh *et al.* [85].

Theorem 4.1.1 (Mutoh *et al.* [85] Theorem 29)**.** *For a prime power q, suppose there exists an elementary abelian $(q, L_{r,k}, 1)$-DDF. If an $(rk, r \times k, 1)$ grid-block design exists, then a resolvable $(rkq, r \times k, 1)$ grid-block design exists.*

Here Theorem 4.1.1 is generalized to resolvable coverings as well. Furthermore, we allow the "input design", a DDF, to have a non-prime-power order.

This can also be viewed as a generalization of the famous construction for resolvable BIBDs due to Ray-Chaudhuri and Wilson [98] (see also the monograph [50] Theorem 3.2.5).

Theorem 4.1.2. *Suppose there exists a cyclic $(v, L_{r,k}, 1)$-DDF over (the additive group of) a ring $\mathbf{R}$. Let $\mathbf{R}^\times$ denote the group of units of $\mathbf{R}$. If*

(i) there exist $u_1, u_2, \ldots, u_{rk} \in \mathbf{R}^\times$, such that $u_i - u_j \in \mathbf{R}^\times$ for any $1 \le i < j \le rk$, and

(ii) there exists an $(rk, r \times k, 1)$ grid-block design (resp., packing, covering),

then a resolvable $(rkv, r\times k, 1)$ grid-block design (resp., packing, covering) exists.

Proof. Let $M = [rk]$. Suppose $(M, \mathcal{E})$ is an $(rk, r \times k, 1)$ grid-block design (resp., packing, covering). Let $\mathcal{E} = \{\mathsf{E}_0, \mathsf{E}_1, \ldots, \mathsf{E}_{b-1}\}$, where $b = \frac{rk-1}{r+k-2}$ (resp., $b \le \frac{rk-1}{r+k-2}$, $b \ge \frac{rk-1}{r+k-2}$). Clearly, E_h contains every element in M exactly once for each $0 \le h \le b-1$. For any rk-set $S = \{a_1, a_2, \ldots, a_{rk}\}$, let $\mathsf{E}_h(S)$ denote the grid-block obtained by substituting every $i \in [rk]$ with $a_i \in S$ in E_h.

Let $\mathcal{A} = \{\mathsf{A}_1, \mathsf{A}_2, \ldots, \mathsf{A}_s\}$ be a $(v, L_{r,k}, 1)$-DDF, where $s = \frac{v-1}{rk(r+k-2)}$. Since $\mathcal{A}$ contains $rk \cdot s = \frac{v-1}{r+k-2}$ distinct elements which are less than v, without loss of generality, we can assume that 0 does not appear in any A_ℓ for $1 \le \ell \le s$.

Now, we begin to construct the resolvable design of order rkv with point-set $V = \mathbf{R} \times M$. We define two types of new grid-blocks,

$$\mathsf{C}_x^h = \mathsf{E}_h(\{(xu_1, 1), (xu_2, 2), \ldots, (xu_{rk}, rk)\}), \text{ for } x \in \mathbf{R} \text{ and } 0 \le h \le b-1,$$
$$\mathsf{B}_\ell^j = (u_j \cdot \mathsf{A}_\ell) \times \{j\}, \text{ for } 1 \le \ell \le s \text{ and } j \in M,$$

whose total number is $vb + rks = vb + \frac{v-1}{r+k-2}$ ($= \frac{rkv-1}{r+k-2}$ if $\mathcal{E}$ forms a design).

For any $g \in \mathbf{R}$, let $\tau_g : (a, j) \mapsto (a+g, j)$ be a mapping over $\mathbf{R} \times M$. Let

$$\mathcal{C} = \left\{\tau_g \mathsf{C}_x^h \mid g, x \in \mathbf{R}, 0 \le h \le b-1\right\},$$
$$\mathcal{B} = \left\{\tau_g \mathsf{B}_\ell^j \mid g \in \mathbf{R}, j \in M, 1 \le \ell \le s\right\}.$$

Next, we will show that $(V, \mathcal{C} \cup \mathcal{B})$ is an $r \times k$ grid-block design (resp., packing, covering) by calculating the *pure (resp., mixed) differences* derived from C_x^h and B_ℓ^j. For a grid-block B over $V = \mathbf{R} \times M$ and $i, j \in M$, we define a multiset

$$\partial_{ij}\mathsf{B} = \{s - t \mid \mathbf{R} \times M \ni (s, i), (t, j) : \text{collinear in } \mathsf{B}\},$$

which is called the *pure (resp., mixed) difference list* of B when $i = j$ (resp., $i \ne j$). For any distinct $i, j \in M$, the pure difference $\partial_{jj}\mathsf{B}_\ell^i = \emptyset$. Moreover, E_h contains no duplicated points. So $\partial_{jj}\mathsf{C}_x^h = \emptyset$ for each $0 \le h \le b-1$. On the other hand, since $\mathcal{A}$ is a difference family and u_j is a unit in $\mathbf{R}$, we have

$$\bigcup_{\ell=1}^{s} \partial_{jj}\mathsf{B}_\ell^j = u_j \bigcup_{\ell=1}^{s} \Delta\mathsf{A}_\ell = u_j \Delta\mathcal{A} = u_j(\mathbf{R} \setminus \{0\}) = \mathbf{R} \setminus \{0\}.$$

Similarly, for any $i, j, k \in M$ with $i \neq j$, it is obvious that $\partial_{ij}\mathsf{B}_\ell^k = \emptyset$. On the other hand, for each $0 \leq h \leq b-1$ and each $x \in \mathbf{R}$,

$$\partial_{ij}\mathsf{C}_x^h = \begin{cases} \{(u_i - u_j)x\} & \text{if } i, j \text{ are collinear in } \mathsf{E}_h, \\ \emptyset & \text{otherwise.} \end{cases}$$

If $(M, \mathcal{E})$ is a design, by recalling that $u_i - u_j \in \mathbf{R}^\times$, we have

$$\bigcup_{x \in \mathbb{Z}_v} \bigcup_{h=0}^{b-1} \partial_{ij}\mathsf{C}_x^h = \bigcup_{x \in \mathbb{Z}_v} \{(u_i - u_j)x\} = (u_i - u_j)\mathbf{R} = \mathbf{R}.$$

Therefore, $(V, \mathcal{C} \cup \mathcal{B})$ is a design. When $(M, \mathcal{E})$ is a packing, if $i, j \in M$ are not collinear in any $\mathsf{E}_h \in \mathcal{E}$, then $\bigcup_{h=0}^{b-1} \partial_{ij}\mathsf{C}_x^h = \emptyset$. In this case, $(V, \mathcal{C} \cup \mathcal{B})$ is a packing. When $(M, \mathcal{E})$ is a covering, if $i, j \in M$ are collinear in m ($m \geq 2$) grid-blocks in $\mathcal{E}$, then $\bigcup_{x \in \mathbb{Z}_v} \bigcup_{h=0}^{b-1} \partial_{ij}\mathsf{C}_x^h$ (as a multiset) consists of all the elements of $\mathbb{Z}_v$ with multiplicity m. Thus, $(V, \mathcal{C} \cup \mathcal{B})$ is a covering.

It remains to show the resolvability. Let

$$\mathcal{P}_g = \{\tau_g\mathsf{B}_\ell^j \mid j \in M, 1 \leq \ell \leq s\} \cup \left\{\tau_g\mathsf{C}_x^0 \,\middle|\, x \notin \bigcup_{i=1}^{s} \mathsf{A}_i\right\}, \text{ for each } g \in \mathbf{R}, \tag{4.1}$$

$$\mathcal{R}_x^0 = \{\tau_g\mathsf{C}_x^0 \mid g \in \mathbf{R}\}, \text{ for each } x \in \bigcup_{i=1}^{s} \mathsf{A}_i, \tag{4.2}$$

$$\mathcal{R}_x^h = \{\tau_g\mathsf{C}_x^h \mid g \in \mathbf{R}\}, \text{ for each } x \in \mathbf{R} \text{ and } 1 \leq h \leq b-1. \tag{4.3}$$

Then, (4.1), (4.2), and (4.3) give rise to $\rho := v + srk + v(b-1) = vb + \frac{v-1}{r+k-2}$ resolution classes. In particular, if $\mathcal{E}$ forms a design, then $\rho = \frac{rkv-1}{r+k-2}$. □

Remark. Let ρ_- (resp., ρ_+) denote the number of resolution classes of the $(vkr, k \times r, 1)$ grid-block packing (resp., covering) we constructed. Then, $\rho_- = v\lfloor\frac{rk-1}{r+k-2}\rfloor + \frac{v-1}{r+k-2}$ (resp., $\rho_+ = v\lceil\frac{rk-1}{r+k-2}\rceil + \frac{v-1}{r+k-2}$). A maximal packing (resp., minimal covering) should satisfy $\rho_- = \tilde{\rho}_- := \lfloor\frac{rkv-1}{r+k-2}\rfloor$ (resp., $\rho_+ = \tilde{\rho}_+ := \lceil\frac{rkv-1}{r+k-2}\rceil$). More precisely, for an $r \times k$ grid-block covering, we have

$$\varrho_+ = \lim_{v \to \infty} \frac{\tilde{\rho}_+}{\rho_+} = \lim_{v \to \infty} \frac{\lceil\frac{rkv-1}{r+k-2}\rceil}{v\lceil\frac{rk-1}{r+k-2}\rceil + \frac{v-1}{r+k-2}} = \frac{\frac{rk}{r+k-2}}{\frac{1}{r+k-2} + \lceil\frac{rk-1}{r+k-2}\rceil} \leq 1,$$

where equality holds if and only if $r = k$ is odd (hence it becomes a design). For example, when $r = k+2$, we have $\varrho_+ = \frac{k^2+2k}{k^2+3k+1}$, which is greater than 0.95 if $k \geq 19$. In addition, when k is a large odd integer, Theorems 3.2.6 and 3.2.13 can also give quite a few cyclic DF, which derive "nearly optimal" coverings via Theorem 4.1.2.

In order to simplify criterion (i) in Theorem 4.1.2, we need a simple lemma.

Lemma 4.1.3. *Let s and $m > 1$ be positive integers. Let $q_1 \leq q_2 \leq \cdots \leq q_s$ be prime powers. For $\mathbf{R} = \bigoplus_{\ell=1}^{s} \mathbb{F}_{q_\ell}$, if $m < q_1$, then there exist $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m \in \mathbf{R}^\times$ such that $\boldsymbol{u}_i - \boldsymbol{u}_j \in \mathbf{R}^\times$ for any $1 \leq i < j \leq m$.*

Proof. This is obvious when $s = 1$. Suppose $s \geq 2$. Since $m < q_1 \leq q_2 \leq \cdots \leq q_s$, we can take m distinct nonzero elements arbitrarily in $\mathbb{F}_{q_\ell}$ for each $1 \leq \ell \leq s$, say $u_1^{(\ell)}, u_2^{(\ell)}, \ldots, u_m^{(\ell)}$. Let $\boldsymbol{u}_i = (u_i^{(1)}, u_i^{(2)}, \ldots, u_i^{(s)})$ for each $1 \leq i \leq m$. It is easy to verify that $\boldsymbol{u}_1, \boldsymbol{u}_2, \ldots, \boldsymbol{u}_m$ are the required units in $\mathbf{R}^\times$. $\square$

By combining Lemma 4.1.3, Corollary 3.2.10, Corollary 3.5.3, and a $(9, 3 \times 3, 1)$ grid-block design (see [57], [85] for the existence), we have the following:

Corollary 4.1.4. *There exists a resolvable $(9v, 3 \times 3, 1)$ grid-block design if $v = q_1 q_2 \cdots q_s$ and $q_i \equiv 1 \pmod{36}$ is a prime power for every $1 \leq i \leq s$.*

4.2 Optimal resolvable grid-block coverings

Let G be a (finite, simple, and undirected) graph and let V be a finite set. Suppose $(V, \mathcal{A})$ is a G-covering. The *excess graph* of $(V, \mathcal{A})$ is the multigraph (V, E), where each edge $\{x, y\}$ occurs in E with multiplicity

$$|\{A \in \mathcal{A} \mid \{x, y\} \text{ is an edge in } A\}| - 1.$$

Clearly, an $r \times c$ grid-block covering is equivalent to an $L_{r,c}$-covering. Now we consider a resolvable $L_{2,c}$-covering and simply write an $L_{2,c}$-RC or a $(v, L_{2,c}, 1)$-RC for short.

Lemma 4.2.1. *Let $(V, \mathcal{A})$ be a $(2ch, L_{2,c}, 1)$-RC. Then $(V, \mathcal{A})$ is optimal if and only if its excess graph forms a 1-factor of K_{2ch} over V.*

Proof. Since every grid-block contains c^2 edges, the number of edges in the excess graph of an optimal $L_{2,c}$-RC is $2h \cdot h \cdot c^2 - \binom{2ch}{2} = hc$. For a fixed vertex x, there are c edges adjacent to x in a grid-block. The total degree of x in an optimal $L_{2,c}$-RC is $2h \cdot c$. Whereas, the degree of x in K_{2ch} is $2ch - 1$. Since $2ch - (2ch - 1) = 1$, the excess graph in an optimal $L_{2,c}$-RC forms a 1-factor of K_{2ch}. Conversely, if the excess graph of $(V, \mathcal{A})$ forms a 1-factor of K_{2ch}, then the total number of grid-blocks in $\mathcal{A}$ is clearly $2h^2$, i.e., $\rho = 2h$. $\square$

It is remarkable that, unlike the leave of an optimal packing, which is known to be a $(c-1)$-factor (see [73] Theorem 2.1), the excess graph of an optimal covering is much smaller and independent with c. Especially when c is large, it becomes a stronger condition for a covering to reach optimality. In particular, an optimal covering with the smallest possible order does not always exist.

Lemma 4.2.2. *There exists an optimal $(2c, L_{2,c}, 1)$-RC if and only if $c \leq 4$.*

Proof. Let $V = \mathbb{Z}_c \times \mathbb{Z}_2 = \{x_i \mid x \in \mathbb{Z}_c, i \in \mathbb{Z}_2\}$. An optimal $(2c, L_{2,c}, 1)$-RC should consist of two grid-blocks, say B_1 and B_2. Without loss of generality, let

$$\mathsf{B}_1 = \begin{bmatrix} 0_0 & 1_0 & \cdots & (c-1)_0 \\ 0_1 & 1_1 & \cdots & (c-1)_1 \end{bmatrix}.$$

Let $M_1 = (\mathbb{Z}_c \setminus \{0\}) \times \{1\}$. In order to cover the pairs of the form $\{0_0, \mu_1\}$ with $\mu_1 \in M_1$, at least $c-2$ points in M should be collinear with 0_0 in B_2. In this case, at least a $(c-2)$-clique is contained in the excess graph, which contradicts Lemma 4.2.1 when $c \geq 5$. Therefore, an optimal $(2c, L_{2,c}, 1)$-RC does not exist for $c \geq 5$.

For $c = 4$, let $\mathsf{B}_1 = \begin{bmatrix} 0_0 & 1_0 & 2_0 & 3_0 \\ 0_1 & 1_1 & 2_1 & 3_1 \end{bmatrix}$ and $\mathsf{B}_2 = \begin{bmatrix} 0_0 & 1_0 & 3_1 & 2_1 \\ 1_1 & 0_1 & 2_0 & 3_0 \end{bmatrix}$. For $c = 3$, let $\mathsf{B}_1 = \begin{bmatrix} 0_0 & 1_0 & 2_0 \\ 0_1 & 1_1 & 2_1 \end{bmatrix}$ and $\mathsf{B}_2 = \begin{bmatrix} 0_0 & 1_1 & 2_1 \\ 0_1 & 2_0 & 1_0 \end{bmatrix}$. Then $(V, \{\mathsf{B}_1, \mathsf{B}_2\})$ is an optimal $(2c, L_{2,c}, 1)$-RC for $c \in \{3, 4\}$. $\square$

In design theory, RGDDs (resolvable group divisible designs) and frames are commonly used for constructions of new designs. For the standard notions of design theory, the reader is referred to [7, 50]. The "block sizes" of RGDDs and frames can be generalized to graph type. In particular, we need to introduce $L_{2,c}$-RGDDs (resolvable group divisible designs) and $L_{2,c}$-frames (see also [73]).

Let $K_{g_1, g_2, \ldots, g_u}$ denote a complete u-partite graph with vertex set V whose partite sets are $G_1, G_2, \ldots, G_u$ with $|G_i| = g_i$ for every $1 \leq i \leq u$. Suppose $\mathcal{A}$ is an $L_{2,c}$-decomposition of $K_{g_1, g_2, \ldots, g_u}$. Let $\mathcal{G} = \{G_1, G_2, \ldots, G_u\}$. Then $(V, \mathcal{G}, \mathcal{A})$ is called an $L_{2,c}$ *group divisible design* (*GDD*) of type $(g_1, g_2, \ldots, g_u)$, where G_i is referred to as a *group* for every $1 \leq i \leq u$. Moreover, if $\mathcal{A}$ can be partitioned into parallel classes, then $(V, \mathcal{G}, \mathcal{A})$ is called a *resolvable group divisible design* (*RGDD*). If $g = g_1 = g_2 = \cdots = g_u$, the GDD is said to be uniform. In this case, $(V, \mathcal{G}, \mathcal{A})$ is called an $L_{2,c}$-GDD of type g^u for convenience. Clearly, a (resolvable) $L_{2,c}$-GDD of type 1^v is nothing but a (resolvable) $(v, L_{2,c}, 1)$ design.

Proposition 4.2.3 ([73] Lemma 2.2)**.** There are exactly $\frac{g(u-1)}{c}$ parallel classes in any $L_{2,c}$-RGDD of type g^u.

Let $(V, \mathcal{G}, \mathcal{A})$ be an $L_{2,c}$-GDD with $\mathcal{G} = \{G_1, G_2, \ldots, G_u\}$. A partial parallel class of $(V, \mathcal{G}, \mathcal{A})$ is a collection of subgraphs of $\mathcal{A}$ whose vertex sets are mutually disjoint. If $\mathcal{A}$ can be partitioned into partial parallel classes, each of which forms a partition of $V \setminus G_i$ for some $G_i \in \mathcal{G}$, then $(V, \mathcal{G}, \mathcal{A})$ is called an $L_{2,c}$-frame of type $(g_1, g_2, \ldots, g_u)$, where $|G_i| = g_i$ for every $1 \leq i \leq u$. If $g = g_1 = g_2 = \cdots = g_u$, then $(V, \mathcal{G}, \mathcal{A})$ is called an $L_{2,c}$-frame of type g^u for convenience.

Proposition 4.2.4 ([73] Lemma 2.7)**.** Let $(V, \mathcal{G}, \mathcal{A})$ be an $L_{2,c}$-frame. For any $G_i \in \mathcal{G}$, the number of partial parallel classes over V missing G_i is $|G_i|/c$.

Some fundamental constructions for an optimal $L_{2,c}$-RC by using $L_{2,c}$-RGDDs and $L_{2,c}$-frames are given as follows.

Construction 4.2.5. Let u be an even positive integer. If there exists an $L_{2,c}$-RGDD of type c^u, then an optimal $(cu, L_{2,c}, 1)$-RC exists.

Proof. Since u is even, let $(V, \mathcal{G}, \mathcal{A})$ be an $L_{2,c}$-RGDD of type c^u with $\mathcal{G} = \{G_1, G_2, \dots, G_{u/2}\} \cup \{H_1, H_2, \dots, H_{u/2}\}$. Let $G_i = \{g_1^{(i)}, g_2^{(i)}, \dots, g_c^{(i)}\}$ and $H_i = \{h_1^{(i)}, h_2^{(i)}, \dots, h_c^{(i)}\}$ for every $1 \le i \le u/2$. Then, we have $u/2$ new grid-blocks given by

$$\mathsf{F}_i = \begin{bmatrix} g_1^{(i)} & g_2^{(i)} & \cdots & g_c^{(i)} \\ h_1^{(i)} & h_2^{(i)} & \cdots & h_c^{(i)} \end{bmatrix} \text{ for every } 1 \le i \le u/2.$$

F_i covers all edges in two complete graphs whose vertex sets are G_i and H_i, and

$$\mathcal{F}_i = \big\{\{g_j^{(i)}, h_j^{(i)}\} \mid 1 \le j \le c\big\}.$$

Then $(V, \mathcal{A} \cup \{\mathsf{F}_1, \mathsf{F}_2, \dots, \mathsf{F}_{u/2}\})$ is an $L_{2,c}$-RC, in which $\{\mathsf{F}_1, \mathsf{F}_2, \dots, \mathsf{F}_{u/2}\}$ forms one more parallel class. Moreover, $\bigcup_{i=1}^{u/2} \mathcal{F}_i$ is a partition of V into pairs, which is nothing but the excess graph of $(V, \mathcal{A} \cup \{\mathsf{F}_1, \mathsf{F}_2, \dots, \mathsf{F}_{u/2}\})$. By Lemma 4.2.1, $(V, \mathcal{A} \cup \{\mathsf{F}_1, \mathsf{F}_2, \dots, \mathsf{F}_{u/2}\})$ is a desired optimal $L_{2,c}$-RC. □

Construction 4.2.6. Let g be a multiple of $2c$. Suppose a $(g, L_{2,c}, 1)$-RC exists. If there exists an $L_{2,c}$-RGDD of type g^u, then an optimal $(gu, L_{2,c}, 1)$-RC exists.

Proof. Let $(V, \mathcal{G}, \mathcal{A})$ be an $L_{2,c}$-RGDD of type g^u with $\mathcal{G} = \{G_1, G_2, \dots, G_u\}$. Suppose $(G_i, \mathcal{B}_i)$ is an optimal $(g, L_{2,c}, 1)$-RC for every $1 \le i \le u$. Then every $(G_i, \mathcal{B}_i)$ has the same number of parallel classes, because the $|G_i|$ are identical with each other for $1 \le i \le u$. Hence $(V, \bigcup_{i=1}^{u} \mathcal{B}_i)$ is resolvable, where $V = \bigcup_{i=1}^{u} G_i$. Clearly, $(V, \bigcup_{i=1}^{u} \mathcal{B}_i \cup \mathcal{A})$ is an $L_{2,c}$-RC as well. Moreover, by Lemma 4.2.1, the excess graph of $(G_i, \mathcal{B}_i)$ forms a 1-factor of K_g on G_i for each $1 \le i \le u$. The excess graph of $(V, \bigcup_{i=1}^{u} \mathcal{B}_i \cup \mathcal{A})$ is obviously the union of 1-factors, each of which consists of a partition of G_i. Thus, $(V, \bigcup_{i=1}^{u} \mathcal{B}_i \cup \mathcal{A})$ is also optimal by Lemma 4.2.1. □

Construction 4.2.7. Let g be a multiple of $2c$. Suppose a $(g, L_{2,c}, 1)$-RC exists. If there exists an $L_{2,c}$-frame of type g^u, then an optimal $(gu, L_{2,c}, 1)$-RC exists.

Proof. Let $h = \frac{g}{2c}$. Let $(V, \mathcal{G}, \mathcal{A})$ be an $L_{2,c}$-frame of type g^u with $\mathcal{G} = \{G_1, G_2, \dots, G_u\}$. By Proposition 4.2.4, the number of partial parallel classes over V missing G_i is $2h$ for every $G_i \in \mathcal{G}$. On the other hand, it is shown in the proof of Lemma 4.2.1 that the number of parallel classes in any $(g, L_{2,c}, 1)$-RC is also $2h$. For $1 \le i \le u$, let $(G_i, \mathcal{B}_i)$ be a $(g, L_{2,c}, 1)$-RC. Clearly, $(V, \bigcup_{i=1}^{u} \mathcal{B}_i \cup \mathcal{A})$ is an $L_{2,c}$-covering. By combining a parallel class in $(G_i, \mathcal{B}_i)$ with a partial parallel class of $(V, \mathcal{G}, \mathcal{A})$ missing G_i, a new parallel class over V can be obtained. Proceeding similarly for each $1 \le i \le u$, we obtain $2h$ parallel classes over V. Therefore, $(V, \bigcup_{i=1}^{u} \mathcal{B}_i \cup \mathcal{A})$ is resolvable. Finally, similarly to the proof of Construction 4.2.6 that the excess graph of $(V, \bigcup_{i=1}^{u} \mathcal{B}_i \cup \mathcal{A})$ forms a 1-factor of K_{gu} on V. By Lemma 4.2.1, $(V, \bigcup_{i=1}^{u} \mathcal{B}_i \cup \mathcal{A})$ is an optimal $(gu, L_{2,c}, 1)$-RC. □

Li and Yin [73] described several recursive constructions of $L_{2,c}$-RGDDs and $L_{2,c}$-frames, which generalize the classical RGDDs, frames, and RBIBDs. We will use the following two theorems from [73].

Theorem 4.2.8 ([73] Construction 2.9)**.** *Suppose there exists an $L_{2,c}$-frame of type $(mg)^h$. If an $L_{2,c}$-RGDD of type g^{m+1} exists, then an $L_{2,c}$-RGDD of type g^{1+mh} exists.*

Theorem 4.2.9 ([73] Construction 2.13)**.** *Suppose there exists a k-frame of type g^u. If an $L_{2,c}$-RGDD of type m^k exists, then an $L_{2,c}$-frame of type $(mg)^u$ exists.*

4.3 Optimal resolvable 2×3 grid-block coverings

Lemma 4.3.1. *There exists an optimal $(12, L_{2,3}, 1)$-RC.*

Proof. The grid-blocks of an optimal $(12, L_{2,3}, 1)$-RC over $\mathbb{Z}_{12}$ are shown as follows, consisting of 4 parallel classes.

$$\begin{bmatrix}0 & 9 & 2\\ 8 & 3 & 4\end{bmatrix}, \begin{bmatrix}10 & 6 & 11\\ 1 & 7 & 5\end{bmatrix}, \qquad \begin{bmatrix}0 & 6 & 1\\ 11 & 2 & 3\end{bmatrix}, \begin{bmatrix}9 & 10 & 4\\ 5 & 8 & 7\end{bmatrix},$$
$$\begin{bmatrix}0 & 10 & 7\\ 5 & 2 & 3\end{bmatrix}, \begin{bmatrix}1 & 11 & 4\\ 9 & 8 & 6\end{bmatrix}, \qquad \begin{bmatrix}0 & 3 & 10\\ 4 & 6 & 5\end{bmatrix}, \begin{bmatrix}8 & 1 & 2\\ 9 & 11 & 7\end{bmatrix}.$$

□

Lemma 4.3.2. *There exists an $L_{2,3}$-RGDD of type 3^u for $u \in \{8, 12, 14\}$.*

Proof. Let $X_{3u} = I_3 \times (\mathbb{Z}_{u-1} \cup \{\infty\})$, where $I_3 = \{1, 2, 3\}$. For each $u \in \{8, 12, 14\}$, we define $u/2$ base grid-blocks, say $\mathsf{B}_1, \mathsf{B}_2, \ldots, \mathsf{B}_{u/2}$, shown in Table 4.1. Let $\mathcal{G}_{3u} = \big\{I_3 \times \{x\} \mid x \in \mathbb{Z}_{u-1} \cup \{\infty\}\big\}$ and $\mathcal{B}_{3u} = \{\mathsf{B}_i + (*, j) \mid 1 \le i \le u/2, j \in \mathbb{Z}_{u-1}\}$, where the second component is deduced cyclically modulo $u-1$ leaving ∞ fixed. Then $\bigcup_{i=1}^{u/2}\{\mathsf{B}_i + (*, j)\}$ is a parallel class for every $j \in \mathbb{Z}_{u-1}$. Therefore $(X_{3u}, \mathcal{G}_{3u}, \mathcal{B}_{3u})$ is a desired $L_{2,3}$-RGDD of type 3^u. □

Lemma 4.3.3. *There exists an $L_{2,3}$-RGDD of type 6^u for $u \in \{3, 5\}$.*

Proof. An $L_{2,3}$-RGDD of type 6^3 is given in [73] Lemma 3.6. For $u = 5$, take $X_{30} = I_3 \times (\mathbb{Z}_8 \cup \{\infty_1, \infty_2\})$ and $\mathcal{G}_{30} = \big\{I_3 \times \{x, x+4\} \mid 0 \le x \le 3\big\} \cup \big\{I_3 \times \{\infty_1, \infty_2\}\big\}$, where $I_3 = \{1, 2, 3\}$. Let

$$\mathsf{B}_1 = \begin{bmatrix}(3,0) & (1,5) & (1,\infty_2)\\ (1,2) & (1,3) & (2,0)\end{bmatrix}, \mathsf{B}_2 = \begin{bmatrix}(2,1) & (1,0) & (2,2)\\ (2,\infty_1) & (3,1) & (1,7)\end{bmatrix},$$
$$\mathsf{B}_3 = \begin{bmatrix}(1,1) & (3,6) & (3,\infty_2)\\ (1,6) & (3,\infty_1) & (2,5)\end{bmatrix}, \mathsf{B}_4 = \begin{bmatrix}(3,7) & (2,4) & (2,6)\\ (3,5) & (3,2) & (2,3)\end{bmatrix},$$
$$\mathsf{B}_5 = \begin{bmatrix}(2,\infty_2) & (2,7) & (3,4)\\ (1,4) & (1,\infty_1) & (3,3)\end{bmatrix},$$

Table 4.1: $L_{2,3}$-RGDD of type 3^u

u	$\mathsf{B}_1, \mathsf{B}_2, \ldots, \mathsf{B}_{u/2}$
$u = 8$	
	$\mathsf{B}_1 = \begin{bmatrix} (3,0) & (1,2) & (3,4) \\ (2,5) & (2,\infty) & (3,3) \end{bmatrix}, \mathsf{B}_2 = \begin{bmatrix} (3,6) & (2,0) & (3,\infty) \\ (3,1) & (2,4) & (1,0) \end{bmatrix},$
	$\mathsf{B}_3 = \begin{bmatrix} (1,1) & (3,5) & (1,\infty) \\ (1,4) & (2,2) & (2,3) \end{bmatrix}, \mathsf{B}_4 = \begin{bmatrix} (1,6) & (2,1) & (3,2) \\ (1,5) & (2,6) & (1,3) \end{bmatrix}.$
$u = 12$	
	$\mathsf{B}_1 = \begin{bmatrix} (3,0) & (1,2) & (1,3) \\ (1,8) & (2,7) & (1,6) \end{bmatrix}, \mathsf{B}_2 = \begin{bmatrix} (2,8) & (3,1) & (3,9) \\ (2,4) & (3,10) & (3,3) \end{bmatrix},$
	$\mathsf{B}_3 = \begin{bmatrix} (1,1) & (3,6) & (2,9) \\ (1,5) & (3,7) & (1,0) \end{bmatrix}, \mathsf{B}_4 = \begin{bmatrix} (2,10) & (3,4) & (1,\infty) \\ (2,0) & (2,6) & (1,4) \end{bmatrix},$
	$\mathsf{B}_5 = \begin{bmatrix} (1,9) & (3,8) & (2,1) \\ (3,2) & (1,7) & (2,\infty) \end{bmatrix}, \mathsf{B}_6 = \begin{bmatrix} (2,5) & (1,10) & (2,3) \\ (2,2) & (3,\infty) & (3,5) \end{bmatrix}.$
$u = 14$	
	$\mathsf{B}_1 = \begin{bmatrix} (3,0) & (3,12) & (2,1) \\ (3,7) & (2,3) & (3,4) \end{bmatrix}, \mathsf{B}_2 = \begin{bmatrix} (3,3) & (3,11) & (2,6) \\ (1,2) & (2,4) & (2,7) \end{bmatrix},$
	$\mathsf{B}_3 = \begin{bmatrix} (2,2) & (2,9) & (1,3) \\ (2,11) & (1,0) & (1,7) \end{bmatrix}, \mathsf{B}_4 = \begin{bmatrix} (1,\infty) & (3,5) & (2,10) \\ (1,11) & (2,\infty) & (2,12) \end{bmatrix},$
	$\mathsf{B}_5 = \begin{bmatrix} (3,6) & (3,2) & (2,0) \\ (1,10) & (1,8) & (2,5) \end{bmatrix}, \mathsf{B}_6 = \begin{bmatrix} (1,12) & (1,9) & (3,1) \\ (3,10) & (3,8) & (1,4) \end{bmatrix},$
	$\mathsf{B}_7 = \begin{bmatrix} (1,6) & (1,1) & (3,9) \\ (1,5) & (2,8) & (3,\infty) \end{bmatrix}.$

and $\mathcal{B}_{30} = \{\mathsf{B}_i + (*, j) \mid 1 \leq i \leq 5, j \in \mathbb{Z}_8\}$, where the second component is deduced cyclically modulo 8 leaving ∞_1 and ∞_2 fixed. Clearly, $\bigcup_{i=1}^{5}\{\mathsf{B}_i+(*, j)\}$ is a parallel class for every $j \in \mathbb{Z}_8$. Then $(X_{30}, \mathcal{G}_{30}, \mathcal{B}_{30})$ is a desired $L_{2,3}$-RGDD of type 6^5. $\square$

Lemma 4.3.4 ([73] Lemma 3.7)**.** *For any integer $u \geq 4$ and $u \notin \{8, 12, 14, 18\}$, an $L_{2,3}$-frame of type 12^u exists.*

Lemma 4.3.5. *An $L_{2,3}$-frame of type 24^h exists for $h \in \{4, 6, 7, 9\}$.*

Proof. The cases when $h \in \{6, 7, 9\}$ are shown in [73] Lemma 3.8. For $h = 4$, take a 3-frame of type 4^4 (see [34] IV.5.30 for the existence). Then apply Theorem 4.2.9 with $c = 3$, $k = 3$, $g = 4$, $u = 4$, and $m = 6$ to the $L_{2,3}$-RGDD of type 6^3 in Lemma 4.3.3 to complete the proof. $\square$

Lemma 4.3.6. *There exists an optimal $(24, L_{2,3}, 1)$-RC.*

Proof. By applying Construction 4.2.5 to the $L_{2,3}$-RGDD of type 3^8 in Lemma 4.3.2, we can show the claim. $\square$

Theorem 4.3.7. *There exists an optimal $(12u, L_{2,3}, 1)$-RC for any positive integer u.*

Proof. This holds for $u = 1, 2$ by Lemmas 4.3.1 and 4.3.6. By Construction 4.2.7, Lemmas 4.3.1, and 4.3.6, it suffices to find $L_{2,3}$-frames of type 12^u or 24^u. Lemma 4.3.4 gives the $L_{2,3}$-frame of type 12^u for any integer $u \geq 4$ and $u \notin \{8, 12, 14, 18\}$. Lemma 4.3.5 gives the $L_{2,3}$-frame of type 24^h for $2h \in \{8, 12, 14, 18\}$. For $u = 3$, by applying Construction 4.2.5 to the $L_{2,3}$-RGDD of type 3^{12} in Lemma 4.3.2, we obtain an optimal $(36, L_{2,3}, 1)$-RC. $\square$

Theorem 4.3.8. *There exists an optimal $(12u+6, L_{2,3}, 1)$-RC for any positive integer u.*

Proof. By Construction 4.2.6 and Lemma 4.2.2, it suffices to find $L_{2,3}$-RGDDs of type 6^u. An $L_{2,3}$-RGDD of type 6^u exists for $u \in \{3, 5\}$ by Lemma 4.3.3. By applying Theorem 4.2.8 with $c = 3$, $g = 6$, and $m = 2$ to the $L_{2,3}$-frames of type 12^u in Lemma 4.3.4, one can obtain an $L_{2,3}$-RGDD of type 6^{2u+1} for any positive integer u with $u \notin \{2, 3, 8, 12, 14, 18\}$. Similarly, by applying Theorem 4.2.8 with $c = 3$, $g = 6$, and $m = 4$ to the $L_{2,3}$-frames of type 24^h in Lemma 4.3.5, an $L_{2,3}$-RGDD of type 6^{4h+1} can be obtained for any $h \in \{1, 4, 6, 7, 9\}$. For $u = 3$, by applying Construction 4.2.5 to the $L_{2,3}$-RGDD of type 3^{14} in Lemma 4.3.2, we obtain the desired RC. $\square$

Chapter 5

Concluding remarks and further problems

This dissertation is concerned with affine-invariant quadruple systems, grid-block difference families, and resolvable grid-block coverings, which can be considered as special kinds of cyclic 3-designs, generalizations of cyclic 2-designs, and generalizations of resolvable 2-designs, respectively.

In Chapter 2, we developed two series of constructions for affine-invariant quadruple systems, which depend on 1-factors of a graph and a hypergraph, respectively. On one hand, the graph $\mathrm{CG}(\Omega_p)$ plays an essential role for Construction 2.2.6 for $\mathrm{AsSQS}^A(2p)$ in Section 2.2.2, and Construction 2.5.1 for affine-invariant $\mathrm{TQS}(p)$ in Section 2.5. However, it is still a challenging problem to theoretically show that $\mathrm{CG}(\Omega_p)$ has a 1-factor for any prime $p \equiv 1, 5 \pmod{12}$. Since we have clarified the relationship between the graph $\mathrm{CG}(\Omega_p)$ and the group $\mathrm{PSL}(2, p)$, we shall find a new way to challenge the problem via group theory.

Problem 1. Prove the existence of 1-factor of $\mathrm{CG}(\Omega_p)$ for any prime $p \equiv 1 \pmod 4$ with the help of group theoretic methods.

On the other hand, Constructions 2.2.20 relies heavily on an edge-colored hypergraph. However, the definition of the hypergraph and its coloring are complicated. Also, less is known about the existence problem of factors (parallel classes) of hypergraphs (designs). Hence, for that special hypergraph, which is also a PBD, we need to make progress towards the following direction:

Problem 2. Characterize the hypergraph (PBD) defined for Constructions 2.2.20, and derive an algebraic or a design-theoretic criterion for the existence of a rainbow 1-factor.

By the recursive constructions presented in Sections 2.3.2 and 2.3.3, we showed for a prime $p \equiv 1, 5 \pmod{12}$ that if the criteria developed for Construction 2.2.6 or Construction 2.2.20 can be satisfied, then an $\mathrm{AsSQS}(2p^m)$ exists for any positive integer m.

Together with the results obtained by computer search for Construction 2.2.6 (see Corollary 2.2.8), we conclude that an AsSQS($2p^m$) exists for every prime $p \equiv 1, 5 \pmod{12}$ with $p < 10^5$ and any positive integer m. We leave the following as an open problem:

Problem 3. Find an AsSQS($2p_1p_2$) for distinct primes $p_1, p_2 \equiv 1, 5 \pmod{12}$, or prove the non-existence of such kind of AsSQSs.

In Section 2.7, new applications of affine-invariant designs are illustrated. The affine-invariant property provides stronger symmetry and so it is expected to have more applications.

In Chapter 3, we proposed an intermediate algebraic consequence for showing the asymptotic existence of "DF-like" designs, and then used it to improve the existence bounds for grid-block difference families over finite fields. However, for many cases, the bounds are still not good enough.

Problem 4. Improve the bound in Theorem 3.1.3 by considering more relaxed restrictions instead of Theorem 3.1.3 (i) and (ii).

In Section 3.4, the concept of Kronecker density for prime numbers are utilized for grid-block difference families. In general, we should consider the following problem:

Problem 5. Consider the Kronecker density with respect to other combinatorial constructions, such as t-designs and combinatorial codes.

It is shown in Section 3.2 that there are "bad" primes when the grid-block size is large, and in that case the radical construction does not work. In order to settle the existence for grid-block difference families, we still need to solve the following:

Problem 6. Provide constructions and existence theorems for the grid-block difference families over the finite fields of "bad" prime orders.

In Chapter 4, we constructed resolvable grid-block designs (packings, coverings) via grid-block difference families. Moreover, we considered the recursive constructions for optimal resolvable grid-block coverings by using frames and RGDDs. Indeed, all the RGDDs in Section 4.3 are computed with the aid of a SAT-based constraint solver – Sugar (cf. [112]; see http://bach.istc.kobe-u.ac.jp/sugar/). We can observe that all those RGDDs admit a "rotational" type automorphism, so we should consider the combinatorial nature of those designs.

List of papers related to this dissertation

- X.-N. Lu, On affine-invariant two-fold quadruple systems, *Graphs and Combinatorics*, **31**(6): 1915–1927, 2015.
- X.-N. Lu, M. Jimbo, Affine-invariant strictly cyclic Steiner quadruple systems, *Designs, Codes and Cryptography*, in press.
- X.-N. Lu, Optimal resolvable $2 \times c$ grid-block coverings, *Utilitas Mathematica*, in press.

Bibliography

[1] J. Akiyama and M. Kano. *Factors and Factorizations of Graphs: Proof Techniques in Factor Theory*, volume 2031 of *Lecture Notes in Math.* Springer, 2011.

[2] B. Alspach. Research problems. *Discrete Math.*, **97**:419–423, 1991.

[3] T. M. Apostol. *Introduction to Analytic Number Theory.* Springer-Verlag New York., 1976.

[4] G. K. Atia and V. Saligrama. Boolean compressed sensing and noisy group testing. *IEEE Trans. Inform. Theory*, **58**(3):1880–1901, 2012.

[5] H. Behr and J. Mennicke. A presentation of the groups $\mathrm{PSL}(2, p)$. *Canad. J. Math*, **20**(6):1432–1438, 1968.

[6] G. Berman. The application of difference sets to the design of a balanced multiple-valued filing scheme. *Inf. Control*, **32**(2):128–138, 1976.

[7] T. Beth, D. Jungnickel, and H. Lenz. *Design Theory. Vol.1.* Cambridge University Press, 1999.

[8] S. Bitan and T. Etzion. The last packing number of quadruples, and cyclic SQS. *Des. Codes Cryptogr.*, **3**(4):283–313, 1993.

[9] A. Bonisoli, M. Buratti, and G. Rinaldi. Sharply transitive decompositions of complete graphs into generalized Petersen graphs. *Innov. Incidence Geom*, **6**(7):95–109, 2009.

[10] R. C. Bose. On the construction of balanced incomplete block designs. *Ann. Eugenics*, **9**(4):353–399, 1939.

[11] R. C. Bose, S. S. Shrikhande, and E. T. Parker. Further results on the construction of mutually orthogonal Latin squares and the falsity of Euler's conjecture. *Canad. J. Math*, **12**:189–203, 1960.

[12] N. Brand. Design invariants. *Geom. Dedicata*, **21**(2):169–179, 1986.

[13] N. Brand and S. Sutinuntopas. One-factors and the existence of affine designs. *Discrete Math.*, **120**(1):25–35, 1993.

[14] M. Buratti. Constructions of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$. *Discrete Math.*, **138**(1):169–175, 1995.

[15] M. Buratti. Improving two theorems of Bose on difference families. *J. Combin. Des.*, **3**(1):15–24, 1995.

[16] M. Buratti. On simple radical difference families. *J. Combin. Des.*, **3**(2):161–168, 1995.

[17] M. Buratti. A packing problem its application to Bose's families. *J. Combin. Des.*, **4**(6):457–472, 1996.

[18] M. Buratti. Packing the blocks of a regular structure. *Bull. Inst. Combin. Appl*, **21**:49–58, 1997.

[19] M. Buratti. Pairwise balanced designs from finite fields. *Discrete Math.*, **208**:103–117, 1999.

[20] M. Buratti and A. Pasotti. Graph decompositions with the use of difference matrices. *Bull. Inst. Combin. Appl*, **47**:23–32, 2006.

[21] M. Buratti and A. Pasotti. Combinatorial designs and the theorem of Weil on multiplicative character sums. *Finite Fields Appl.*, **15**(3):332–344, 2009.

[22] M. Buratti and A. Pasotti. On perfect Γ-decompositions of the complete graph. *J. Combin. Des.*, **17**(2):197–209, 2009.

[23] E. J. Carter. *Designs on Cubic Multigraphs*. PhD dissertation, McMaster University, 1989.

[24] Y. Chang and C. Ding. Constructions of external difference families and disjoint difference families. *Des. Codes Cryptogr.*, **40**(2):167–185, 2006.

[25] Y. Chang and L. Ji. Optimal $(4up, 5, 1)$ optical orthogonal codes. *J. Combin. Des.*, **12**(5):346–361, 2004.

[26] G. Chartrand, L. Lesniak, and P. Zhang. *Graphs & Digraphs*. CRC Press, 5th edition, 2011.

[27] K. Chen, R. Wei, and L. Zhu. Existence of $(q, 7, 1)$ difference families with q a prime power. *J. Combin. Des.*, **10**(2):126–138, 2002.

[28] K. Chen and L. Zhu. Existence of $(q, 6, 1)$ difference families with q a prime power. *Des. Codes Cryptogr.*, **15**(2):167–173, 1998.

[29] K. Chen and L. Zhu. Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$. *J. Combin. Des.*, **7**(1):21–30, 1999.

[30] K. Chen and L. Zhu. Improving Wilson's bound on difference families. *Util. Math.*, **55**:189–200, 1999.

[31] W. Chu. *Optical Orthogonal Codes and Cyclic t-Designs.* PhD dissertation, University of Southern California, 2002.

[32] F. R. Chung, J. A. Salehi, and V. K. Wei. Optical orthogonal codes: design, analysis and applications. *IEEE Trans. Inform. Theory*, **35**(3):595–604, 1989.

[33] C. Colbourn and M. Colbourn. A recursive construction for infinite families of cyclic SQS. *Ars Combin*, **10**:95–102, 1980.

[34] C. J. Colbourn and J. H. Dinitz. *Handbook of Combinatorial Designs.* CRC Press, 2006.

[35] M. J. Colbourn and C. J. Colbourn. Recursive constructions for cyclic block designs. *J. Statist. Plann. Inference*, **10**(1):97–103, 1984.

[36] H. S. M. Coxeter and W. O. J. Moser. *Generators and Relations for Discrete Groups.* Springer-Verlag, 4th edition, 1980.

[37] R. Diestel. *Graph Theory*, volume 173 of *Grad. Texts in Math.* Springer-Verlag, Heidelberg, 3rd edition, 2006.

[38] K. Diks and P. Stańczyk. Perfect matching for biconnected cubic graphs in $O(nlog^2n)$ time. In *SOFSEM 2010: Theory and Practice of Computer Science*, 321–333. Springer, 2010.

[39] D.-Z. Du and F. K. Hwang. *Combinatorial Group Testing and its Applications.* World Scientific, 2nd edition, 1999.

[40] D.-Z. Du and F. K. Hwang. *Pooling Designs and Nonadaptive Group Testing: Important Tools for DNA Sequencing.* World Scientific, 2006.

[41] A. D'yachkov, V. Rykov, C. Deppe, and V. Lebedev. Superimposed codes and threshold group testing. In *Information Theory, Combinatorics, and Search Theory*, volume 7777 of *Lecture Notes in Comput. Sci.*, 509–533. Springer, 2013.

[42] T. Feng. 3-*Designs and Some Applications (in Chinese).* PhD dissertation, Beijing Jiaotong University, 2008.

[43] T. Feng and Y. Chang. Constructions for cyclic 3-designs and improved results on cyclic Steiner quadruple systems. *J. Combin. Des.*, **19**(3):178–201, 2011.

[44] T. Feng, Y. Chang, and L. Ji. Constructions for strictly cyclic 3-designs and applications to optimal OOCs with $\lambda = 2$. *J. Combin. Theory, Ser. A*, **115**(8):1527–1551, 2008.

[45] R. A. Fisher. The design of experiments. *Oliver and Boyd, Edinburgh*, 1935.

[46] F. Fitting. Zyklische Lösungen des Steiner'schen Problems. *Nieuw. Arch. Wisk*, **11**(2):140–148, 1915.

[47] H.-L. Fu, F. Hwang, M. Jimbo, Y. Mutoh, and C. Shiue. Decomposing complete graphs into $K_r \times K_c$'s. *J. Statist. Plann. Inference*, **119**(2):225–236, 2004.

[48] R. Fuji-Hara and Y. Miao. Optical orthogonal codes: Their bounds and new optimal constructions. *IEEE Trans. Inform. Theory*, **46**(7):2396–2406, 2000.

[49] R. Fuji-Hara, Y. Miao, and S. Shinohara. Complete sets of disjoint difference families and their applications. *J. Statist. Plann. Inference*, **106**(1):87–103, 2002.

[50] S. Furino, Y. Miao, and J. Yin. *Frames and Resolvable Designs: Uses, Constructions and Existence.* CRC Press, 1996.

[51] M. Grannel and T. Griggs. Some recent results on cyclic Steiner quadruple systems - a survey. *Ann. Discrete Math*, **18**:409–418, 1983.

[52] H. Hanani. On quadruple systems. *Canad. J. Math*, **12**:145–157, 1960.

[53] H. Hanani. The existence and construction of balanced incomplete block designs. *Ann. Math. Stat.*, **32**(2):361–386, 1961.

[54] H. Hanani. On balanced incomplete block designs with blocks having five elements. *J. Combin. Theory Ser. A*, **12**(2):184–201, 1972.

[55] A. Hartman and K. T. Phelps. Steiner quadruple systems. In J. H. Dinitz and D. R. Stinson, editors, *Contemporary Design Theory: A Collection of Surveys*, chapter 6, 205–240. New York: Wiley, 1992.

[56] J. Holm, K. de Lichtenberg, and M. Thorup. Poly-logarithmic deterministic fully-dynamic algorithms for connectivity, minimum spanning tree, 2-edge, and biconnectivity. *J. ACM*, **48**(4):723–760, 2001.

[57] F. Hwang. An isomorphic factorization of the complete graph. *J. Graph Theory*, **19**(3):333–337, 1995.

[58] K. Ireland and M. Rosen. *A Classical Introduction to Modern Number Theory*, volume 84 of *Grad. Texts in Math.* Springer-Verlag, 2nd edition, 1990.

[59] L. Ji. A construction for 2-chromatic Steiner quadruple systems. *European J. Combin.*, **28**(6):1832–1838, 2007.

[60] M. Jimbo. Recursive constructions for cyclic BIB designs and their generalizations. *Discrete Math.*, **116**(1):79–95, 1993.

[61] M. Jimbo and S. Kuriki. A product theorem for cyclic graph designs. *Ann. Discrete Math.*, **34**:287–295, 1987.

[62] S. Johnson. A new upper bound for error-correcting codes. *IRE Trans. Inform. Theory*, **8**(3):203–207, 1962.

[63] P. Keevash. The existence of designs. *arXiv preprint arXiv:1401.3665*, 2014.

[64] T. P. Kirkman. On a problem in combinations. *Cambridge and Dublin Math. J*, **2**:191–204, 1847.

[65] E. Köhler. Zyklische quadrupelsysteme. In *Abh. Math. Sem. Univ. Hamburg Vol.48*, 1–24. Springer, 1979.

[66] E. Köhler. k-difference cycles and the construction of cyclic t-designs. In M. Aigner and D. Jungnickel, editors, *Geometries and Groups*, volume 893 of *Lecture Notes in Math.*, 195–203. Springer, 1981.

[67] E. Köhler. Quadruple systems over $\mathbb{Z}_p$ admitting the affine group. In D. Jungnickel and K. Vedder, editors, *Combinatorial Theory*, volume 969 of *Lecture Notes in Math.*, 212–228. Springer, 1982.

[68] E. R. Lamken and R. M. Wilson. Decompositions of edge-colored complete graphs. *J. Combin. Theory Ser. A*, **89**(2):149–200, 2000.

[69] F. Lemmermeyer. *Reciprocity Laws: from Euler to Eisenstein*. Springer, 2000.

[70] H. Lenz. Tripling steiner quadruple systems. *Ars. Combin*, **20**:193–202, 1985.

[71] H. Lenz and G. Ringel. A brief review on Egmont Köhler's mathematical work. *Discrete Math.*, **97**(1):3–16, 1991.

[72] Y. Li and L. Ji. Constructions of dihedral Steiner quadruple systems. *Discrete Math.*, **340**(3):351–360, 2017.

[73] Y. Li and J. Yin. Resolvable packings of K_v with $K_2 \times K_c$'s. *J. Combin. Des.*, **17**(2):177–189, 2009.

[74] Y. Li, J. Yin, R. Zhang, and G. Ge. The decomposition of K_v into $K_2 \times K_5$'s. *Sci. China Math.*, **50**(10):1382–1388, 2007.

[75] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, 1997.

[76] N. B. Limaye. Cross-ratios and projectivities of a line. *Math. Z.*, **129**(1):49–53, 1972.

[77] C. C. Lindner and C. A. Rodger. Decomposition into cycles II: Cycle systems. In J. H. Dinitz and D. R. Stinson, editors, *Contemporary Design Theory: A Collection of Surveys*, chapter 8, 325–369. Wiley New York, 1992.

[78] C. C. Lindner and A. Rosa. Steiner quadruple systems-a survey. *Discrete Math.*, **22**(2):147–181, 1978.

[79] K. Momihara. *Existence and Construction of Difference Families and Their Applications to Combinatorial Codes in Multiple-Access Communications.* PhD dissertation, Nagoya University, 2009.

[80] K. Momihara, M. Müller, J. Satoh, and M. Jimbo. Constant weight conflict-avoiding codes. *SIAM J. Discrete Math.*, **21**(4):959–979, 2007.

[81] D. W. Mount. *Bioinformatics: Sequence and Genome Analysis.* Cold Spring Harbor, NY., 2nd edition, 2004.

[82] A. Munemasa and M. Sawa. Simple abelian quadruple systems. *J. Combin. Theory Ser. A*, **114**(6):1160–1164, 2007.

[83] A. Munemasa and M. Sawa. Steiner quadruple systems with point-regular abelian automorphism groups. *J. Stat. Theory Pract.*, **6**(1):97–128, 2012.

[84] Y. Mutoh. *Existence and Construction of Array Type Block Designs and their Generalization to Edge-Colored Graph Decompositions.* PhD dissertation, Keio University, 2003.

[85] Y. Mutoh, M. Jimbo, and H.-L. Fu. A resolvable $r \times c$ grid-block packing and its application to DNA library screening. *Taiwanese J. Math.*, **8**(4):713–737, 2004.

[86] Y. Mutoh, T. Morihara, M. Jimbo, and H.-L. Fu. The existence of 2×4 grid-block designs and their applications. *SIAM J. Discrete Math.*, **16**(2):173–178, 2003.

[87] E. Netto. Zur Theorie der Tripelsysteme. *Mathematische Annalen*, **42**(1):143–152, 1893.

[88] D. Pei. *Authentication Codes and Combinatorial Designs.* CRC Press, 2006.

[89] R. Peltesohn. Eine Lösung der beiden Heffterschen Differenzenprobleme. *Compositio Mathematica*, **6**:251–257, 1939.

[90] J. Petersen. Die Theorie der regulären graphs. *Acta Math.*, **15**(1):193–220, 1891.

[91] P. A. Peterson and M. C. Loui. The general maximum matching algorithm of Micali and Vazirani. *Algorithmica*, **3**(1-4):511–533, 1988.

[92] K. Phelps and A. Rosa. 2-chromatic Steiner quadruple systems. *European J. Combin.*, **1**(3):253–258, 1980.

[93] W. Piotrowski. *Untersuchungen über S-zyklische Quadrupelsysteme.* PhD dissertation, University of Hamburg, 1985.

[94] J. Plesník. Remarks on regular factors of regular graphs. *Czechoslovak Math. J.*, **24**(2):292–300, 1974.

[95] J. Plücker. *System der analytischen Geometrie, auf neue Betrachtungsweisen gegrûndet, und insbesondere eine ausfûrliche Theorie der Curven dritter Ordnung enthaltend.* Duncker und Humblot, 1835.

[96] J. Plücker. *Theorie der algebraischen Curven.* Adolph Marcus, 1839.

[97] D. Raghavarao. *Constructions and Combinatorial Problems in Design of Experiments.* Wiley, 1971.

[98] D. K. Ray-Chaudhuri and R. M. Wilson. The existence of resolvable block designs. In *A survey of combinatorial theory*, 361–375. North-Holland Amsterdam, 1973.

[99] P. Ribenboim. *Classical Theory of Algebraic Numbers.* Universitext. Springer, 2001.

[100] M. Sawa. A cyclic group action on resolutions of quadruple systems. *J. Combin. Theory Ser. A*, **114**(7):1350–1356, 2007.

[101] M. Sawa. *On Combinatorial Designs via Compositions and Finite Groups.* PhD dissertation, Nagoya University, 2007.

[102] J. Schönheim. On maximal systems of k-tuples. *Studia Sci. Math. Hungar*, **1**:363–368, 1966.

[103] H. Siemon. Some remarks on the construction of cyclic Steiner quadruple systems. *Arch. Math.*, **49**(2):166–178, 1987.

[104] H. Siemon. Infinite families of strictly cyclic Steiner quadruple systems. *Discrete Math.*, **77**(1-3):307–316, 1989.

[105] H. Siemon. Cyclic Steiner quadruple systems and Köhler's orbit graphs. *Des. Codes. Cryptogr.*, **1**(2):121–132, 1991.

[106] H. Siemon. On the existence of cyclic Steiner quadruple systems SQS($2p$). *Discrete Math.*, **97**(1):377–385, 1991.

[107] H. Siemon. Piotrowski's infinite series of Steiner quadruple systems revisited. *Des. Codes. Cryptogr.*, **8**:239–254, 1996.

[108] H. Siemon. A number theoretic conjecture and the existence of S–cyclic Steiner quadruple systems. *Des. Codes. Cryptogr.*, **13**(1):63–94, 1998.

[109] J. Steiner. Combinatorische aufgaben. *Journal für die reine und angewandte Mathematik*, **45**:181–182, 1853.

[110] D. R. Stinson. Some constructions and bounds for authentication codes. *J. Cryptology*, **1**(1):37–51, 1988.

[111] M. Suzuki. *Group Theory*. Springer-Verlag Berlin, 1982.

[112] N. Tamura, A. Taga, S. Kitagawa, and M. Banbara. Compiling finite linear CSP into SAT. *Constraints*, **14**(2):254–272, 2009.

[113] L. Teirlinck. Non-trivial t-designs without repeated blocks exist for all t. *Discrete Math.*, **65**(3):301–311, 1987.

[114] V. V. Vazirani. A theory of alternating paths and blossoms for proving correctness of the $O(\sqrt{V}E)$ general graph maximum matching algorithm. *Combinatorica*, **14**(1):71–109, 1994.

[115] C. Wang and C. J. Colbourn. The existence of $(K_2 \times K_6)$-designs. *Graphs Combin.*, **29**(5):1557–1567, 2013.

[116] W. Wannasit and S. El-Zanati. On cyclic G-designs where G is a cubic tripartite graph. *Discrete Math.*, **312**(2):293–305, 2012.

[117] L. C. Washington. *Introduction to Cyclotomic Fields*, volume 83 of *Grad. Texts in Math.* Springer, 1997.

[118] K. S. Williams. Explicit forms of Kummer's complementary theorems to his law of quintic reciprocity. *J. Reine Angew. Math.*, **228**:207–210, 1976.

[119] R. Wilson and J. J. Watkins, editors. *Combinatorics: Ancient & Modern.* OUP Oxford, 2013.

[120] R. M. Wilson. Cyclotomy and difference families in elementary abelian groups. *J. Number Theory*, **4**(1):17–47, 1972.

[121] R. M. Wilson. An existence theory for pairwise balanced designs I. Composition theorems and morphisms. *J. Combin. Theory Ser. A*, **13**(2):220–245, 1972.

[122] R. M. Wilson. An existence theory for pairwise balanced designs II. The structure of PBD-closed sets and the existence conjectures. *J. Combin. Theory Ser. A*, **13**(2):246–273, 1972.

[123] R. M. Wilson. An existence theory for pairwise balanced designs, III: Proof of the existence conjectures. *J. Combin. Theory Ser. A*, **18**(1):71–79, 1975.

[124] E. Witt. Über Steinersche Systeme. In *Abh. Math. Sem. Univ. Hamburg*, volume 12, 265–275. Springer, 1937.

[125] W. Woolhouse. Prize question 1733. *Lady's and Gentleman's Diary*, **84**, 1844.

[126] S. Yamamoto, T. Teramoto, and K. Futagami. Design of a balanced multiple-valued filing scheme of order two based on cyclically generated spread in finite projective geometry. *Inf. Control*, **21**(1):72–91, 1972.

[127] F. Yates. Incomplete randomized blocks. *Annals of Eugenics*, **7**(2):121–140, 1936.

[128] F. Yates. Lattice squares. *J. Agric. Sci.*, **30**(04):672–687, 1940.

[129] S. Yoshikawa. Constructions of Strictly Cyclic Steiner Quadruple Systems Admitting All Units of $\mathbb{Z}_p$ As Multiplies (in Japanese). Master's thesis, Nagoya University, 2009.

[130] Q. R. Yu and G. Liu. *Graph Factors and Matching Extensions.* Springer, 2009.

[131] R. Zhang, G. Ge, A. C. Ling, H.-L. Fu, and Y. Mutoh. The existence of $r \times 4$ grid-block designs with $r = 3, 4$. *SIAM J. Discrete Math.*, **23**(2):1045–1062, 2009.

[132] X. Zhang and G. Ge. A new existence proof for Steiner quadruple systems. *Des. Codes Cryptogr.*, **69**(1):65–76, 2013.