Existence and Construction of Difference Families and Their Applications to Combinatorial Codes in Multiple-Access Communications

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

September, 2009

Koji Momihara

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

Preface and Acknowledgements

My interest in combinatorics began six years ago when I was studying in the laboratory of Professor Sanpei Kageyama at Hiroshima University as an undergraduate student. I started my study for combinatorics with reading the famous book "*Introduction to Combinatorial Theory*" written by R.C. Bose and B. Manvel. After one and a half years, I decided to enter Nagoya University and join the laboratory of Professor Masakazu Jimbo in order to study more deeply. I was inspired not only by his expert knowledge for combinatorial designs and their applications but also by his personality. This thesis presents results from my four and a half years research on difference families and combinatorial codes at the Department of Computer Science and Mathematical Informatics, Graduate School of Information Science, Nagoya University. The study has been partially funded by JSPS Research Fellowships for Young Scientists during the Ph.D. program at Nagoya University.

This thesis consists of six chapters. In the first chapter, a general introduction to combinatorial design theory, particularly, difference families and their application to combinatorial codes, and a survey of current new results are given. The next four chapters contain the author's results in [88, 89, 90, 91, 92]. These chapters provide various new results on difference families including several known results via purely combinatorial techniques, the theory of finite fields, and number theory. Some of these papers are written jointly with other mathematicians, who are Professor Masakazu Jimbo (Nagoya University), Professor Junya Satoh (Nagoya University), Dr. Minard Müller (Max Planck Institutes for Informatics), and Professor Marco Buratti (University of Perugia). In the final chapter, some concluding remarks and open problems related to results in this thesis are provided.

This thesis demands of a little preparatory knowledge in combinatorial design theory but most concepts are thoroughly defined in each chapter of this thesis or self-explanatory.

I would like to express my deepest appreciation to my advisor Professor Masakazu Jimbo. He has supervised my study for five and a half years and his continuous encouragement, patience, and excellent guidance had led me to successfully complete this thesis. I am most grateful to his invitation me to the academic world.

I would also like to thank Professor Sanpei Kageyama. He had introduced me to the field of combinatorics in my undergraduate course. I am grateful for his kind advices not only on my study but also on my private life.

I am especially indebted to Professor Ryoh Fuji-Hara, Professor Mieko Yamada, and Professor Junya Satoh for helping me to study combinatorics, number theory, and their applications to communication theory. I would like to give special thanks to Professor Marco Buratti and

Dr. Anita Pasotti for their knowledge and fruitful discussions about difference families, the main topic of this thesis. I have learned a lot through joint works with them.

I am very thankful Professor Shinji Kuriki, Professor Ying Miao, Professor Miwako Mishima, Professor Satoshi Shinohara, Professor Nobuko Miyamoto, and Professor Keisuke Shiromoto for their helpful advices on both of my study and private life. Also, I would like to thank Dr. Masanori Sawa, Dr. Yuichiro Fujiwara, and Mr. Masatake Hirao and all our laboratory members.

I am thankful to Professor Yo Matsubara, Professor Masahiko Sakai, and Professor Junya Satoh, who are the members of my thesis committee, for their careful reading and useful comments to improve the readability.

Finally, I wish to express my gratitude to my family, my wife Chieko, and her family for their warm supports. I could not have completed this work without their hearty encouragement.

Koji Momihara
Nagoya University

Contents

1 Introduction **1**

1.1 Difference families 2

1.2 Relative difference families 5

1.3 Cyclotomic cosets and difference families 8

1.4 Combinatorial codes in multiple-access communications 12

1.4.1 Optical orthogonal codes 12

1.4.2 Conflict-avoiding codes 16

1.5 Outline of this thesis 19

2 Cyclic 8-support $(v,4)_2$ difference families and $(v,4,2,1)$ optical orthogonal codes **21**

2.1 Definition of cyclic δ-support difference families 21

2.2 Upper bounds for $M(v,4,2,1)$ 22

2.3 Direct constructions of 8-supp $(np,n,4)_2$-CDFs 25

2.3.1 Perfect 8-supp $(p,4)_2$-CDFs for primes p 26

2.3.2 8-supp $(2p,2,4)_2$-CDFs for primes p 28

2.3.3 8-supp $(4p,4,4)_2$-CDFs for primes p 29

2.3.4 8-supp $(8p,8,4)_2$-CDFs for primes p 30

2.4 Further direct constructions of maximal 8-supp $(np,4)_2$-CDFs 31

2.5 Compositions of 8-supp $(v,4)_2$-CDFs 35

2.6 New infinite series of optimal $(v,4,2,1)$-OOCs 37

3 Cyclic $2(k-1)$-support $(v,k)_{k-1}$ difference families and $(v,k,1)$ conflict-avoiding codes **39**

3.1 Main theorems in this chapter 39

3.2 $(v, k, 1)$-CACs from perfect $2(k-1)$-supp $(v, k)_{k-1}$-CDFs 40
3.3 Perfect packings 41
3.4 Compositions of perfect $2(k-1)$-supp $(v, k)_{k-1}$-CDFs 43
3.5 The Kronecker density 45
3.5.1 Perfect 4-supp $(p, 3)_2$-CDFs 45
3.5.2 Perfect 6-supp $(p, 4)_3$-CDFs 47
3.5.3 Perfect 8-supp $(p, 5)_4$-CDFs 50

4 Strong difference families, difference covers, and relative difference families 53
4.1 Fundamental facts on strong difference families and difference covers 53
4.2 Strong difference families of order 2 54
4.2.1 Sums of squares 54
4.2.2 Existence of cyclic strong difference families of order 2 55
4.3 Difference covers from partial difference sets 57
4.4 Difference covers over a finite field 59
4.5 Relative difference families and strong difference families 63
4.5.1 Fundamental relations 63
4.5.2 An improvement on distributions of differences 65

5 Cyclic relative difference families with variable blocksize 71
5.1 Group characters and basic lemmas 72
5.2 Construction of cyclic relative difference families with variable blocksize . . . 74
5.3 Improvement of a bound on blocksize 78
5.4 New series of $(v, k, 1, 1)$-OOCs 83

6 Further researches and open problems 85

List of papers related to this thesis 89

Bibliography 91

Chapter 1

Introduction

Combinatorial designs have their roots in the work of L.P. Euler, who in 1780s presented the well known "36 officers problem." In 19th century, T.P. Kirkman, J. Steiner, and A. Cayley worked on combinatorial design theory. In 1930s, the area of design theory underwent rapid development due to the development of finite affine and projective geometries. And the development of the theory of Latin squares, which are an example of algebraic systems with binary operations, expedited the progress of design theory. Furthermore, actual demands from an area of applications, namely statistical design of experiments, were also one of the important motivations of the development. The investigation of a connection between finite geometry and group theoretic combinatorial designs was initiated by R. Baer in 1930s. Since 1960s, many researchers including R.J. Turyn, U. Ott, E.F. Assmus, Jr., and H.F. Mattson, Jr. have found a close relation between algebraic design theory and coding theory. Some of those results were based on algebraic number theory.

One of the most successful and famous applications of combinatorial designs is found in the field of statistical design of experiments. Fisher's and Yates's investigations established a connection between combinatorial designs and the theory of statistical planning and inferences [50, 117]. Such applications use an important property, so-called "balancedness," of designs. Subsequently, Bose [14] and some other statisticians studied systematic constructions of experimental designs with balancedness, for example, "balanced incomplete block designs," "group divisible designs," etc. The techniques have been further developed and contributed to the investigation of various kinds of combinatorial designs. Several methods to systematically construct block designs have been appeared in the past fifty years and one of the most useful techniques is "the method of differences" first introduced by Bose [14]. The reason why the method of differences is so useful is that one can easily generate designs. For example, balanced incomplete block designs and group divisible designs can be derived from a "difference families" as we see in Sections 1.1 and 1.2 in this chapter. In combinatorial design theory, fundamental problems related to difference families are their "existence," "constructions," and "classifications." In general, a difference family has an interesting algebraic property and the three problems above are fascinating not only in a practical sense but also in a theoretical one. In particular, existence problems of difference families over finite groups are difficult even in the case of cyclic groups and there are a vast amount of articles trying to solve the problem. For example, Wilson [110] showed an asymptotic existence theorem of

difference families over a finite field and Buratti [16, 17, 18, 19] generalized many of Bose's results. Since then, a number of difference families have been found mainly over abelian groups, and problems related to difference families has been studied as on one of the main topics of combinatorial design theory.

At the earliest stage of the study, there was no application of difference families except for constructions of combinatorial designs used in design of agricultural field experiments or industrial experiments. However, recently there have been found significant roles of the theory of difference families in the field of information science, particularly, in the theory of "multiple-access communications." In communication theory, a technique that two or more users share a communication channel and communicate simultaneously is called a *multiple-access communication*. Though the beginning of multiple-access communications is more than fifty years ago, "optical code-division" multiple-access communications have been developed rapidly from 1980s [62, 63, 102, 103]. In such a multiple-access communication model, a combinatorial code called an "optical orthogonal code" is applied, which is also used for constructing protocol sequences for multiple-access collision channel without feedback [84, 85]. Multiple-access communication systems employ some classical difference families as combinatorial codes whilst they sometimes require new types of difference families proposed in various recent articles. For example, Colbourn, Dinitz, and Stinson [44] provided a survey of applications in this field (see also [38, 39, 42, 48, 72, 73, 97]). Thus, the theory of difference families can help the development of the theory of communications, and new problems in the theory of communications bring fresh insights to the theory of difference families.

In this thesis, we consider several types of difference families, for example, relative difference families, strong difference families, δ-support difference families, etc. As an application of difference families, we also discuss about existence problems and constructions of some kinds of combinatorial codes, in particular, optical orthogonal codes and conflict avoiding codes, which are applied in multiple-access communications. Some results given in this thesis include many known results on difference families and combinatorial codes. This thesis is based on the author's publications [88, 89, 90, 91, 92]. This chapter is dedicated to provide a brief introduction to difference families in combinatorial designs and their applications to codes in multiple-access communication systems. In particular, we will review some definitions, basic notions, and known results related to ordinary difference families, relative difference families, and radical difference families and will take a concise look at their relation to optical orthogonal codes and conflict-avoiding codes.

1.1 Difference families

Let G be a finite group of order v and let k be a positive integer. Throughout this thesis, we call a subset including k elements of G as a *k-subset* of G. Let $\binom{G}{k}$ be the set of all k-subsets of G. Given a k-subset $X \in \binom{G}{k}$, the *list of differences* of X is a multiset defined by

$$\Delta X = \left\{ba^{-1} \,|\, a, b \in X, a \neq b\right\} \text{ or } \left\{b - a \,|\, a, b \in X, a \neq b\right\}$$

depending on whether G is multiplicatively or additively written, respectively. A family $\mathcal{F} \subseteq \binom{G}{k}$ is called a (G, k, λ) *difference family*, briefly (G, k, λ)-DF, if every nonzero element of G occurs λ times in the list $\Delta\mathcal{F} = \bigcup_{B\in\mathcal{F}} \Delta B$. The family $\mathcal{F}$ is also called as a (v, k, λ)-DF

over G. If $|\mathcal{F}| = 1$, the uniquely included set $B \in \mathcal{F}$ is called a (G, k, λ) *difference set*. A difference family is also called a *supplementary difference sets* as a natural generalization of a difference set. In particular, if the group G is cyclic, a (G, k, λ)-DF is called *cyclic*, and we denote it by (v, k, λ)-CDF. In this case, we identify G as $\mathbb{Z}_v$, the residue ring of integers modulo v, and denote each coset $[i]$, $0 \le i \le v-1$, in $\mathbb{Z}_v$ by i for simplicity. Members of $\mathcal{F}$ are called *blocks* or *base blocks*. Obviously, the number of blocks is $\frac{(v-1)\lambda}{k(k-1)}$, which gives the trivial necessary condition

$$\lambda(v-1) \equiv 0 \pmod{k(k-1)} \tag{1.1}$$

for the existence of (v, k, λ)-DFs.

Example 1.1.1. (i) The set of the three blocks

$$B_1 = \{0, 1, 3, 24\},\ B_2 = \{0, 4, 9, 15\},\ \text{and}\ B_3 = \{0, 7, 17, 25\}$$

forms a $(37, 4, 1)$-CDF.

(ii) The set of the five blocks

$$B_1 = \{1, x, x^4\},\ B_2 = \{1, x^2, yx\},\ B_3 = \{1, x^5, y\},$$
$$B_4 = \{1, x^6, yx^2\},\ \text{and}\ B_5 = \{1, x^7, yx^5\}$$

forms a $(16, 3, 2)$-DF over the dihedral group $G = \langle x, y \,|\, x^8 = y^2 = 1; yx = x^7 y\rangle$.

In this thesis, we mainly treat the case when G is abelian. In order to ease some notations and computations, we restate the definition of difference family in terms of a group algebra. For an additive group G and the ring $\mathbb{Z}$ of rational integers, let $\mathbb{Z}G$ denote the ring of formal polynomials

$$\mathbb{Z}G = \left\{ \sum_{a \in G} c_a X^a \,|\, c_a \in \mathbb{Z} \right\},$$

where X is an indeterminate, which has the operations

$$\sum_{a \in G} c_a X^a + \sum_{a \in G} c'_a X^a = \sum_{a \in G} (c_a + c'_a) X^a$$

and

$$\left(\sum_{a \in G} c_a X^a \right) \left(\sum_{a \in G} c_a X^a \right) = \sum_{b \in G} \left(\sum_{a \in G} c_a c'_{b-a} \right) X^b.$$

The zero and the identity elements of $\mathbb{Z}G$ are $\sum_{a \in G} 0 X^a = 0$ and $X^0 = 1$, respectively. For the convenience of notations, we often identify each multiset D defined on G with the group ring element $\sum_{a \in G} c_a X^a \in \mathbb{Z}G$, where c_a means the multiplicity of a in D. We denote $D^{(-1)} = \sum_{a \in G} c_a X^{-a}$. With this notation, we can restate the definition of a (G, k, λ)-DF $\mathcal{F} = \{B_i \,|\, 1 \le i \le m\}$ as

$$\sum_{1 \le i \le m} B_i B_i^{(-1)} = (k - \lambda)\{0\} + \lambda G. \tag{1.2}$$

Many researchers have investigated problems related to difference families over finite fields from the beginning of modern design theory. For $k = 3$, Netto [95] showed that for any prime

power $q \equiv 1 \pmod 6$, there exists a $(q, 3, 1)$-DF over the additive group of $\mathbb{F}_q$, the finite field of order q. For the cases of $k = 4$ and 5, Bose [14], Buratti [16], and Wilson [110] investigated the existence of $(\mathbb{F}_q, k, 1)$-DFs, and Chen and Zhu [34] completely solved the problem. Those results are summarized as follows:

Theorem 1.1.2. ([34, 35, 95, 110]) When $k = 3, 4, 5$, and 6, there exists an $(\mathbb{F}_q, k, 1)$-DF for any prime power $q \equiv 1 \pmod{k(k-1)}$ except for $(k, q) = (6, 61)$.

The cases of $k \geq 6$ were treated in [35, 36, 110]. The following theorem was given by Wilson [110].

Theorem 1.1.3. ([110]) Suppose that q is a prime power such that $\lambda(q-1) \equiv 0 \pmod{k(k-1)}$. Then there exists an $(\mathbb{F}_q, k, \lambda)$-DF if one of the following holds:

(i) λ is a multiple of $k/2$ or $(k-1)/2$,

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

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

In particular, the condition (iii) indicates that $(\mathbb{F}_q, k, 1)$-DFs asymptotically exist, i.e., $(\mathbb{F}_q, k, 1)$-DFs exist for all sufficiently large prime power q for fixed k. Recently, using *the theorem of Weil on multiplicative characters* (Theorem 5.39 in [76]), the bound of (iii) was improved by Buratti and Pasotti [26] (also given by Chang and Ji [31]) as

$$q > \binom{k}{2}^{2k}. \tag{1.3}$$

Peltesohn [98] determined the values v for which a $(v, 3, 1)$-CDF exists long time ago, but it still remains unsolved for each $k \geq 4$.

Theorem 1.1.4. ([98]) For any positive integer $v \equiv 1 \pmod 6$, there exists a $(v, 3, 1)$-CDF except for $v = 9$.

We briefly describe what has been done for the case of $k > 3$. The earliest results are due to Bose [14] who gave sufficient conditions for the existence of a $(p, k, 1)$-CDF for a prime p and $k = 4$ and 5. The necessary and sufficient conditions for this special kind of difference families, called "radical difference family," was given in [18] for $4 \leq k \leq 7$. The formal definition of a radical difference family is given in Section 1.3. Furthermore, the results of Theorems 1.1.2 and 1.1.3 can be applied to the case when q is a prime. Cyclic difference families of composed order $v = v_1 v_2$ can be obtained by applying the recursive construction provided in Theorem 1.2.7 of Section 1.2, see also [21]. Moreover, Buratti and Pasotti [27] obtained the following theorem.

Theorem 1.1.5. ([27]) There exists a $(p_1 p_2, 4, 1)$-CDF for every pair of primes (p_1, p_2) with $p_1 \equiv p_2 \equiv 7 \pmod{12}$ and $7 \leq p_1 \leq p_2 < 1000$. There exists a $(p_1 p_2, 5, 1)$-CDF for every pair of primes (p_1, p_2) with $p_1 \equiv p_2 \equiv 11 \pmod{20}$ and $11 \leq p_1 \leq p_2 < 1000$.

However, existence problems of difference families remain unsolved in many cases.

The concept of "difference families" or "the method of differences" was first introduced by Bose [14] as a useful tool for systematically constructing a "balanced incomplete block design." Let V be a set of v elements, called *points*, and let $\mathcal{B}$ be a family of k-subsets (not multiset), called *blocks*, of V, where $|\mathcal{B}| = b$. A pair $(V, \mathcal{B})$ is called a *balanced incomplete block design* (BIBD) if the following conditions are satisfied:

(i) every point is contained in exactly r blocks,

(ii) every pair of two distinct points of V occurs in exactly λ blocks of $\mathcal{B}$.

From the conditions above, it is easy to see that the relations

$$vr = bk \quad \text{and} \quad \lambda(v-1) = r(k-1) \tag{1.4}$$

hold among the five parameters of a BIBD. By these relations, the five parameters are dependent, so we denote a BIBD by (v, k, λ)-BIBD. If $\lambda = 1$, then a (v, k, λ)-BIBD is called a *Steiner 2-design*. An *automorphism* of a BIBD $(V, \mathcal{B})$ is a bijection on V whose induced mapping from $\mathcal{B}$ to $\mathcal{B}$ is also a bijection. The set of all such mappings forms a group under composition called the *full automorphism group* of the design. Any of its subgroups is called an *automorphism group* of the design. Let $\mathcal{F}$ be a (G, k, λ)-DF, and define the *development* of $\mathcal{F}$ as $\mathrm{dev}\mathcal{F} = \{B + i \,|\, B \in \mathcal{F}, i \in G\}$. Then, the pair $(G, \mathrm{dev}\mathcal{F})$ forms a $(|G|, k, \lambda)$-BIBD which admits G as a point-regular automorphism group.

Example 1.1.6. A $(7, 3, 1)$-BIBD on $V = \{0, 1, 2, 3, 4, 5, 6\}$ is given by

$$\mathcal{B} = \{\{0, 1, 3\} + i \,|\, i \in V\},$$

where each element is reduced modulo 7. The set $\mathcal{F} = \{\{0, 1, 3\}\}$ is a $(7, 3, 1)$-CDF.

Many methods have been developed to construct BIBDs, and the concept of difference families is one of the useful tools as we saw before. When $k = 3$ and 4, it has been proved by Hanani [58] that the necessary conditions (1.4) are also sufficient for the existence of (v, k, λ)-BIBDs. For $k \geq 5$, the conditions of (1.4) are generally not sufficient. However, Hanani [59, 60] settled the case when $k = 5$ and gave partial results for $k = 6$ and 7. For general k, it was proved by Wilson [111, 112, 113] that there exists a constant $v_{k,\lambda}$ such that for any $v > v_{k,\lambda}$ satisfying the conditions of (1.4) there exists a (v, k, λ)-BIBD, in which he used the result of Theorem 1.1.3.

1.2 Relative difference families

Next, we define "relative" difference families which was first introduced by Buratti [21] as a generalization of "relative" difference sets.

Let G be a finite group. A family $\mathcal{F} \subseteq \binom{G}{k}$ is called a *scarce* (G, k, λ) *difference family* or also called a (G, k, λ) *difference packing* with *difference leave* $L \subseteq G$ if every element of $G \setminus L$ occurs λ times in the list $\Delta\mathcal{F} = \bigcup_{B \in \mathcal{F}} \Delta B$ but no element of L. If $L = N$, a subgroup of G,

then we say that $\mathcal{F}$ is a *relative* (G, N, k, λ) *difference family*, briefly denoted by (G, N, k, λ)-DF. If $|G| = nv$ and $|N| = n$, a (G, N, k, λ)-DF is also called as an (nv, n, k, λ)*-DF over* G *relative to* N. If $|\mathcal{F}| = 1$, the uniquely included set $B \in \mathcal{F}$ is called a *relative* (G, N, k, λ) *difference set*. Obviously, the concepts of a scarce difference family and a relative difference family are natural generalizations of that of an ordinary difference family. All notations and terminologies used for ordinary difference families are also applied for scarce difference families and relative difference families. For example, if G is cyclic, a (G, N, k, λ)-DF is called *cyclic* and denoted by (nv, n, k, λ)-CDF.

The number of blocks of (G, N, k, λ)-DF is $\frac{n(v-1)\lambda}{k(k-1)}$, which gives the necessary condition

$$n(v-1)\lambda \equiv 0 \pmod{k(k-1)} \tag{1.5}$$

for the existence of a (G, N, k, λ)-DF. An (nv, n, k, λ)-DF with $n = 1$ is clearly a (v, k, λ)-DF, and it is also called *perfect*.

Example 1.2.1. The set of the three blocks

$$B_1 = \{0, 1, 3, 31, 45\},\ B_2 = \{0, 4, 10, 19, 57\},\ \text{and}\ B_3 = \{0, 5, 16, 41, 48\}$$

forms a $(65, 5, 5, 1)$-CDF.

Here are partial existence results on cyclic relative difference families with small blocksize:

Theorem 1.2.2. There exist $(nv, n, 4, 1)$-CDFs for the following parameters (n, v):

(i) ([30]) $n = 4$, $v = 4^m u$ and every prime factor of u is congruent to 1 modulo 6, where $m \geq 2$ or $m = 1$ and $\gcd(u, 7 \cdot 13 \cdot 19) \neq 1$,

(ii) ([23]) $n = 4$ and every prime factor of v is of the form $6pm + 1$, where $m \geq 1$ and p is a prime with $p \leq 19$,

(iii) ([23, 33]) $n = 6$ and v is any positive integer such that $\gcd(v, 30) = 1$,

(iv) ([23]) $n = 8$ and every prime factor of v is congruent to 1 modulo 6,

(v) ([53]) $n = 9, 15$ and every prime factor of v is congruent to 1 modulo 4 greater than 5.

Theorem 1.2.3. There exist $(nv, n, 5, 1)$-CDFs for the following parameters (n, v):

(i) ([31]) $n = 4$ and $v \equiv 1 \pmod{10}$ is any prime with $v \neq 11$,

(ii) ([31]) $n = 4$ and $v = 2p$ or $3p$, where $p \equiv 11 \pmod{20}$ is any prime,

(iii) ([79]) $n \in \{60, 80, 100, 120, 140, 160, 180\}$ and v is any positive integer such that $\gcd(v, 30) = 1$.

For further results related to relative difference families with small blocksize, see [1].

For general k and λ, several series of relative difference families constructed by using "strong difference families" are known. Some of such known series are listed below.

Theorem 1.2.4. (i) ([56]) There exists an $(\mathbb{F}_{q'} \times \mathbb{F}_q, \{0\} \times \mathbb{F}_q, q, \frac{q-1}{2})$-DFs for odd prime powers q and q' with $q' > q$,

(ii) ([22]) There exists an $(\mathbb{F}_{q'} \times \mathbb{F}_q, \{0\} \times \mathbb{F}_q, q, \frac{q-1}{4})$-DFs for prime powers $q \equiv 1 \pmod 4$ and $q' \equiv 1 \pmod{q-1}$,

(iii) ([56]) There exists an $(\mathbb{F}_{q'} \times \mathbb{F}_q, \{0\} \times \mathbb{F}_q, q+1, q+1)$-DFs for odd prime powers q and q' with $q' > q$,

(iv) ([56]) There exists an $(\mathbb{F}_{q'} \times \mathbb{F}_q, \{0\} \times \mathbb{F}_q, q+1, \frac{q+1}{2})$-DFs for odd prime powers $q, q' \equiv 3 \pmod 4$ with $q' > q$,

(v) ([22]) There exists an $(\mathbb{F}_{q'} \times \mathbb{F}_q \times \mathbb{F}_{q+2}, \{0\} \times \mathbb{F}_q \times \mathbb{F}_{q+2}, (q+1)^2, \frac{(q+1)^2}{2})$-DFs for odd prime powers $q, q+2$, and q' with $q' > q(q+2)$.

Some constructions of relative difference families are known. The following theorem gives one of the construction methods of cyclic relative difference families, called *a recursive construction* using "difference matrices." A *cyclic difference matrix* (v, k, λ)-CDM is a $k \times \lambda v$ matrix $M = [\sigma_{i,j}]$ such that $\sigma_{i,j} \in \mathbb{Z}_v$ and for every pair $(i, i') \in \mathbb{Z}_v \times \mathbb{Z}_v$ every element of $\mathbb{Z}_v$ occurs exactly λ times among the list of differences $\{\sigma_{i,j} - \sigma_{i',j} \mid 1 \le j \le \lambda v\}$. Here is a construction of difference matrices.

Theorem 1.2.5. ([43]) Let v and k be positive integers such that $\gcd(v, (k-1)!) = 1$. Let $\sigma_{i,j} \equiv ij \pmod v$ for $i = 0, 1, \ldots, k-1$ and $j = 0, 1, \ldots, v-1$. Then $M = [\sigma_{i,j}]$ is a $(v, k, 1)$-CDM. In particular, if v is an odd prime power, then there exists a $(v, k, 1)$-CDM for any integer $k\,(\le v)$.

Example 1.2.6. The matrix

$$\begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 0 & 2 & 4 & 6 & 1 & 3 & 5 \\ 0 & 3 & 6 & 2 & 5 & 1 & 4 \end{pmatrix}$$

is a $(7, 4, 1)$-CDM.

The following theorem was provided by Jimbo and Kuriki [65].

Theorem 1.2.7. ([65]) Assume that there exist:

(i) an $(n_1 v_1, n_1, k, \lambda)$-CDF,

(ii) an $(n_1 v_2, n_2, k, \lambda)$-CDF, where $n_2 \mid n_1 v_2$,

(iii) a (v_2, k, λ)-CDM.

Then, there exists an $(n_1 v_1 v_2, n_2, k, \lambda)$-CDF.

The concept of "relative difference families" was introduced for constructing "group divisible designs" in [21]. Similar to BIB designs, let V be a finite set of elements, called *points*, with $|V| = nv$, and let $\mathcal{B}$ be a family of k-subsets of V, called *blocks*. Moreover, let $\mathcal{G}$ be a family of n-subsets of V, called *groups* (or *groops* to distinguish from "groups" as algebraic systems), which partition V. An (nv, n, k, λ) *group divisible design* (GDD) is a triple $(V, \mathcal{G}, \mathcal{B})$ satisfying the following:

(i) for each group $C \in \mathcal{G}$ and each block $B \in \mathcal{B}$, $|C \cap B| \leq 1$

(ii) any two points belonging to distinct groups are contained, together, in exactly λ blocks.

From the definition of a GDD, it is easy to see that the following are the necessary conditions for the existence of an (nv, n, k, λ)-GDD:

$$v \geq k, \quad \lambda(v-1)n \equiv 0 \pmod{k-1}, \quad \text{and} \quad \lambda v(v-1)n^2 \equiv 0 \pmod{k(k-1)}. \tag{1.6}$$

Clearly, the existence of a $(v, 1, k, \lambda)$-GDD is equivalent to that of a (v, k, λ)-BIBD. Let $\mathcal{F}$ be a (G, N, k, λ)-DF, and let $\mathcal{G}$ be the set of cosets of N in G. Then, the triple $(G, \mathcal{G}, \mathrm{dev}\mathcal{F})$ forms a $(|G|, |N|, k, \lambda)$-GDD.

Example 1.2.8. An $(8, 2, 3, 1)$-GDD on $V = \{0, 1, 2, 3, 4, 5, 6, 7\}$ is given by

$$\mathcal{B} = \{\{0, 1, 3\} + i \mid i \in V\},$$

where each element is reduced modulo 8. The set $\mathcal{F} = \{\{0, 1, 3\}\}$ is an $(8, 2, 3, 1)$-CDF.

For the case when $k = 3$, Hanani [60] proved that the necessary condition (1.6) for the existence of (nv, n, k, λ)-GDDs is also sufficient. When $k = 4$, a similar sufficiency was established by Brouwer, Schrijver, and Hanani [15].

1.3 Cyclotomic cosets and difference families

The study of "cyclotomic cosets" (or also known as "cyclotomy") is an old topic of elementary number theory and has been widely used to construct many kinds of combinatorial designs. In this section, we provide some known results on difference families based on cyclotomic cosets.

Let α be a primitive root of the finite field $\mathbb{F}_q$ and let e be a positive integer such that $e \mid q-1$. *Cyclotomic cosets of index* e are the e cosets of the multiplicative subgroup $\langle \alpha^e \rangle$ generated by α^e in the multiplicative group $\mathbb{F}_q^\times$ of $\mathbb{F}_q$. More concretely, all such cosets are written as

$$C_0^e = \langle \alpha^e \rangle, \, C_1^e = \alpha \cdot \langle \alpha^e \rangle, \, \ldots, C_{e-1}^e = \alpha^{e-1} \cdot \langle \alpha^e \rangle.$$

Here is an easy example of difference families derived from cyclotomic cosets.

Example 1.3.1. The family $\mathcal{F}$ of cyclotomic cosets C_i^e, $0 \leq i \leq e-1$, forms an $(\mathbb{F}_q, (q-1)/e, (q-e-1)/e)$-DF. For example, put $q = 13$, $e = 3$ and $\alpha = 2$, then we have

$$C_0^3 = \{1, 5, 8, 12\}, \, C_1^3 = \{2, 3, 10, 11\}, \, C_2^3 = \{4, 6, 7, 9\}.$$

It is easy to check that the set $\{C_0^3, C_1^3, C_2^3\}$ forms a $(13, 4, 3)$-CDF.

The most important concept related to cyclomotic cosets is "cyclotomic numbers." *Cyclotomic numbers* of order e are defined as

$$(i,j)_e = \left|(C_i^e + 1) \cap C_j^e\right| \tag{1.7}$$

for $i, j \in \{0, 1, \ldots, e-1\}$. It is obvious that $(i,j)_e$ is the number of pairs $(x,y) \in C_i^e \times C_j^e$ such that $x + 1 = y$.

Cyclotomic numbers are related to Waring's problem [46], difference sets [10, 68, 105], coding theory [80, 81, 86], and cryptography [48]. The concept of cyclotomic cosets was initiated by Gauss in his "Disquisitiones Arithmetica" [54], where he introduced the concepts so-called "Gaussian periods" and "cyclotomic numbers." The cyclotomic numbers of order e have been partially calculated for $e \leq 24$ using various kinds of character sums.

The following basic lemmas are given in [105] and we will use these in Section 4.4 of Chapter 4.

Lemma 1.3.2. ([105]) Let $q = ef + 1$ be a prime power. Then, the following hold:

(i) $(i,j)_e = (i',j')_e$ when $i \equiv i' \pmod{e}$ and $j \equiv j' \pmod{e}$.

(ii) $(i,j)_e = (e-i, j-i)_e = \begin{cases} (j,i)_e & \text{if } f \text{ or } q \text{ is even,} \\ (j+e/2, i+e/2)_e & \text{if } f \text{ and } q \text{ are odd.} \end{cases}$

(iii) $\sum_{j=0}^{e-1}(i,j)_e = f - \eta_i$, where

$$\eta_i = \begin{cases} 1 & \text{if } i \equiv 0 \pmod{e} \text{ and } f \text{ is even,} \\ 1 & \text{if } i \equiv e/2 \pmod{e} \text{ and } f \text{ is odd,} \\ 0 & \text{otherwise.} \end{cases}$$

(iv) $\sum_{i=0}^{e-1}(i,j)_e = f - \theta_j$, where

$$\theta_j = \begin{cases} 1 & \text{if } j \equiv 0 \pmod{e}, \\ 0 & \text{otherwise.} \end{cases}$$

In the following lemma, we identify a subset (cyclotomic coset) on a finite field $\mathbb{F}_q$ with a group ring element in $\mathbb{Z}\mathbb{F}_q$.

Lemma 1.3.3. ([105]) Let $q = ef + 1$ be a prime power. Then, it holds that

$$C_i^e C_j^{e\,(-1)} = \begin{cases} fC_\infty + \sum_{0 \leq \ell \leq e-1}(j-\ell, j-\ell)_e C_\ell^e & \text{if } i \equiv j \bmod e, \\ \sum_{0 \leq \ell \leq e-1}(j-\ell, i-\ell)_e C_\ell^e & \text{otherwise,} \end{cases}$$

where $C_\infty = \{0\}$ (or $0 \in \mathbb{Z}\mathbb{F}_q$).

There are some further basic properties of cyclotomic numbers, for example, see [11, 105], whereas we use only the above lemmas for constructing "difference covers" over $\mathbb{F}_q$, which is defined in Section 4.1 of Chapter 4.

Now, we provide examples of difference families constructed from cyclotomic cosets.

Theorem 1.3.4. (i) ([116]) For a prime power q, let $e = q+1$ and $d \mid e$. Let C_l^e be the lth cyclotomic coset of $\mathbb{F}_{q^2}$. Let $\{A_0, A_1, \ldots, A_{d-1}\}$ be a partition of $\{0, 1, \ldots, q\}$, where $|A_i| = e/d$ for all i. Then, the family of $D_i = \bigcup_{l \in A_i} C_l^e$, $i = 0, 1, \ldots, d-1$, is an $(\mathbb{F}_{q^2}, (q^2-1)/d, (q^2-d-1)/d)$-DF.

(ii) ([116]) Let q be a prime power $\equiv 1 \pmod 4$ and put $e = q+1$. Let $E = \{0, 1, \ldots, e-1\} = E_0 \cup E_1$, $E_0 = \{i \in E \mid i \equiv 0 \pmod 2\}$ and $E_1 = \{i \in E \mid i \equiv 1 \pmod 2\}$. Assume that A_0 and A_1 are subsets of E_0 and E_1, respectively, such that $|A_0| = |A_1| = (q-1)/4$. Further, let $A_2 = A_0$ and $A_3 = A_1$. Then, the family of $D_i = \bigcup_{l \in A_i} C_l^e \cup C_i^4$, $i = 0, 1, 2, 3$, is an $(\mathbb{F}_{q^2}, q(q-1)/2, q(q-2))$-DF.

(iii) ([114]) Let q be a prime power $\equiv 3 \pmod 4$ and put $e = q+1$. Let E, E_0, and E_1 be the same with (ii). Let $\{A_0, A_2\}$ and $\{A_1, A_3\}$ be partitions of E_1 and E_2, respectively, where $|A_i| = (q+1)/4$ for all i. Then the family of $D_i = \bigcup_{l \in A_i} C_l^e \cup C_i^4$, $i = 0, 1, 2, 3$, is an $(\mathbb{F}_{q^2}, (q^2-1)/2, q^2-3)$-DF.

(iv) ([109]) Let $q \equiv 3 \pmod 4$ be a prime power. Set $M = \{a \mid g^{2a} - 1 \in C_0^2\}$ and $N = \{a \mid g^{2a} + 1 \in C_0^2\}$, where C_i^2 is a cyclotomic coset of $\mathbb{F}_q$. Then, the family of M and N is a $((q-1)/2, (q-3)/4, (q-7)/4)$-CDF.

Hereafter, in relation to cyclotomic cosets, we treat "radical difference family." Let $q \equiv 1 \pmod{k(k-1)}$ be a prime power. We say that an $(\mathbb{F}_q, k, 1)$-DF $\mathcal{F}$ is *radical* if each of blocks in $\mathcal{F}$ is a coset of $C_0^{(q-1)/k}$ for odd k or the union of a coset of $C_0^{(q-1)/(k-1)}$ and $\{0\}$ for even k. The terminology of radical difference family was first introduced by Buratti [18] as a powerful tool for constructing $(\mathbb{F}_q, k, 1)$-DFs. However, some results on radical difference families were obtained by Netto [95] much earlier.

Theorem 1.3.5. ([95]) For any prime power $q \equiv 1 \pmod 6$, there exists a radical $(\mathbb{F}_q, 3, 1)$-DF.

As a general result, Wilson [110] showed the following for the existence of a radical $(\mathbb{F}_q, k, 1)$-DF.

Theorem 1.3.6. ([110]) Let $q \equiv 1 \pmod{k(k-1)}$ be a prime power. When k is odd, let ϵ be a primitive kth root of unity in $\mathbb{F}_q$, and put

$$m = \frac{k-1}{2}, \ S = \{\epsilon^i - 1 \mid 1 \le i \le m\}.$$

When k is even, let ϵ be a primitive $(k-1)$th root of unity in $\mathbb{F}_q$, and put

$$m = \frac{k}{2}, \ S = \{\epsilon^i - 1 \mid 1 \le i \le m-1\} \cup \{1\}.$$

If S is a complete system of representatives for the cosets of mth powers in $\mathbb{F}_q^\times$, i.e., each coset of mth powers in $\mathbb{F}_q^\times$ contains exactly one of the elements of S, then there exists a radical $(\mathbb{F}_q, k, 1)$-DF.

Buratti [17] has shown a necessary and sufficient condition for the existence of radical $(\mathbb{F}_q, k, 1)$-DFs for the cases when $k = 4$ and 5, which improved the results of Bose [14]. Furthermore, Theorem 1.3.6 has been also improved by Buratti [18] as follows:

Theorem 1.3.7. ([18]) Let $q = nk(k-1)+1$ be a prime power. Under the same assumptions and notations as Theorem 1.3.6, if there is a chain of divisors of mn of the form

$$d_0 = 1 \,|\, d_1 \,|\, \cdots \,|\, d_{2t} \,|\, d_{2t+1} = mn$$

such that

$$n = \prod_{i=0}^{t} \frac{d_{2i+1}}{d_{2i}} \quad \text{and} \quad \Phi(S) \subset \bigcup_{0 \le i \le t} (C_0^{d_{2i-1}} \setminus C_0^{d_{2i}}) \cup \{1\},$$

where $\Phi(S) = \{xy^{-1} \,|\, x, y \in S\}$, there exists a radical $(\mathbb{F}_q, k, 1)$-DF.

Buratti [18] proved that the condition given in Theorem 1.3.7 is also necessary for the existence of radical $(\mathbb{F}_q, k, 1)$-DFs for the cases when $k = 6$ and 7. Furthermore, in [19, 20], Buratti introduced the concept of "perfect packings" (different from that of "difference packings" defined in Section 1.2) in order to systematically treat radical difference families. This concept is defined in Chapter 3.

Lastly, we provide the following useful theorem on relative difference families.

Theorem 1.3.8. ([26]) Let $q \equiv 1 \pmod{e}$ be a prime power and ℓ be a positive integer. Put

$$r_q(\ell, e) = q - \sqrt{q} \sum_{0 \le i \le \ell-2} (\ell - i - 1) \binom{\ell}{i} (e-1)^{\ell-i} - \ell e^{\ell-1}. \tag{1.8}$$

If $r_q(\ell, e) > 0$, then for any ℓ-tuple $(j_1, j_2, \ldots, j_\ell) \in \{0, 1, \ldots, e-1\}^\ell$ and for any ℓ distinct elements $x_1, x_2, \ldots, x_\ell$ of $\mathbb{F}_q$ there exist at least $\lceil r_q(\ell, e)/e^\ell \rceil$ elements $x \in \mathbb{F}_q$ such that $x - x_i \in C_{j_i}^e$ for each i, $1 \le i \le \ell$.

In this thesis, we denote the set of all prime powers q satisfying $\lceil r_q(\ell, e)/e^\ell \rceil \ge t$ by $P(e, \ell, t)$ and we will use this theorem in Chapters 2 and 4. Theorem 1.3.8 was proved by Buratti and Pasotti [26] using the theorem of Weil on multiplicative character sums and they applied the theorem to show the bound (1.3). Furthermore, they also utilized Theorem 1.3.8 to obtain asymptotic existence theorems of "$\mathbb{Z}$-cyclic triplewhist tournaments" and "$(\mathbb{F}_q, \Gamma, \lambda)$ difference families" where Γ is an arbitrary graph. Especially, they gave the following existence theorem related to relative difference families using the concept of (N, k, μ) strong difference families, that is, a family $\{A_i \,|\, 1 \le i \le m\}$ of "multisets" of size k defined on an abelian (additively written) group N such that the multiset $\{b - a \,|\, a, b \in A_i; 1 \le i \le m\}$ of differences covers all elements in N (including 0) exactly μ times.

Theorem 1.3.9. ([26]) If there exists an (N, k, μ) strong difference family, then there is a sufficiently large integer $q_{k,\mu}$ such that there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, 1)$-DF for any prime power $q \equiv \mu + 1 \pmod{2\mu} > q_{k,\mu}$.

The concepts of strong difference families and difference covers play an important roll in treating problems related to relative difference families.

1.4 Combinatorial codes in multiple-access communications

Recently, wireless communications have become important not only for professional applications but also for many fields in our daily routine. For example, mobile telephones are widely used not only for calls but also for data transmissions. The communications make use of a sophisticated technique which is known as "multiple-access communication systems" including code-division mutiple-access (CDMA) communications, frequency hopping spread-spectrum communications, etc. Many kinds of combinatorial subjects are inhered in these communication systems besides information-theoretical problems. For example, Colbourn, Dinitz, and Stinson [44] provided a survey on such applications in this field (see also [38, 39, 42, 48, 72, 73, 97]).

In this section, applications of difference families to combinatorial codes in multiple-access communication systems are stated. Although there are many applications where a problem related to differences of subsets defined on a finite group plays important roles, we restrict ourselves to describing about "optical orthogonal codes" and "conflict-avoiding codes" since a typical manifestation of applications of "difference families" to multiple-access communications can been seen in these two areas.

1.4.1 Optical orthogonal codes

Let v, k, λ_a and λ_c be positive integers. A $(v, k, \lambda_a, \lambda_c)$-OOC $\mathcal{C}$ is a family of $(0,1)$ sequences, called *codewords*, of length v and Hamming weight k satisfying the following properties:

(i) (*The auto-correlation property*)

$$\sum_{i=0}^{v-1} x_i x_{i+s} \leq \lambda_a$$

holds for any $X = (x_i) \in \mathcal{C}$ and every $s \not\equiv 0 \,(\mathrm{mod}\ v)$,

(ii) (*The cross-correlation property*)

$$\sum_{i=0}^{v-1} x_i y_{i+s} \leq \lambda_c$$

holds for any $X = (x_i), Y = (y_i) \in \mathcal{C}$ with $X \neq Y$ and every integer s,

where all subscripts are taken modulo v. The concept of OOCs can be more conveniently reformulated by using the following set notation. By identifying codewords in $\mathcal{C}$ with k-subsets of $\mathbb{Z}_v$ representing the indices of the nonzero positions, $\mathcal{C}$ can be viewed as a family $\mathcal{F} \subseteq \binom{\mathbb{Z}_v}{k}$ satisfying:

(i) (The auto-correlation property)

$$|X \cap (X + s)| \leq \lambda_a$$

holds for any $X \in \mathcal{F}$ and every $s \in \mathbb{Z}_v \setminus \{0\}$,

(ii) (The cross-correlation property)

$$|X \cap (Y + s)| \leq \lambda_c$$

holds for any $X, Y \in \mathcal{F}$ with $X \neq Y$ and every $s \in \mathbb{Z}_v$.

Example 1.4.1. (1) The set

$$\mathcal{C} = \{(1100100000000), (1010000100000)\}$$

is a $(13, 3, 1, 1)$-OOC with two codewords. In the set notation above, $\mathcal{C}$ can be viewed as

$$\mathcal{F} = \{\{0, 1, 4\}, \{0, 2, 7\}\}.$$

(2) The set

$$\mathcal{C} = \{(11001100000000000), (10100000101000000)\}$$

is a $(17, 4, 2, 1)$-OOC with two codewords. In the set notation above, $\mathcal{C}$ can be viewed as

$$\mathcal{F} = \{\{0, 1, 4, 5\}, \{0, 2, 8, 10\}\}.$$

The objective of a multiple-access communication is to allow the users to share a single common channel and transmit data successfully. Now we briefly mention how to use optical orthogonal codes in an optical CDMA communications system.

When a $(v, k, \lambda_a, \lambda_c)$-OOC $\mathcal{C}$ with m codewords is used in a communication, each codeword in $\mathcal{C}$ is assigned to a transmitter/receiver pair. A transmitter encodes every information bit into a frame of v optical chips, where any chip is an optical time unit which has one of the two signals ON and OFF corresponding to the symbols 1 and 0 of a codeword of the OOC, respectively, in the following way: Let $X = \{x_1, x_2, \ldots, x_k\}$ be the assigned codeword for a particular user pair, where X is the set-notation of a codeword $X \in \mathcal{C}$. When an information bit is **1**, in the corresponding frame, which consists of v optical chips, ON signals are sent at exactly the x_1th, x_2th, ..., and x_kth chips. In the other $v - k$ chips, OFF signals are sent. In other words, the codeword X is used as the signature sequence of the transmitter. On the other hand, if an information bit is **0**, all OFF signals are sent in the corresponding frame.

All m transmitters are allowed to send at any time. Each receiver uses a decoding machine, called a "tap-device," which corresponds to a codeword assigned to each user pair in order to separate transmitted signals at the receiving end. The tap-device corresponding to a user pair, say transmitter A and receiver A', having the codeword $X = \{x_1, x_2, \ldots, x_k\} \in \mathcal{C}$ collects ON signals at intervals of $x_2 - x_1, x_3 - x_2, \ldots, x_k - x_{k-1}, x_1 - x_k$ chips in each time and effectively accumulates the level of the output (the sum of ON signals). The tap-device distinguishes the strength of the accumulated optical signals, and when the strength attains the peak, the syncronization of the user pair is accomplished. Thus, the lower auto-correlation property of the OOC enables to distinguish the peak of signal levels easily, and then the peak enables the receiver to synchronize. (See Figure 1.1, which is a situation that a user pair synchronizes in a communication system applying an OOC of length 7 and weight 3.)

At the same time, the lower cross-correlation property of the OOC is used to avoid mutual interferences from the other user pairs. When more than one user pair transmits simultaneously,

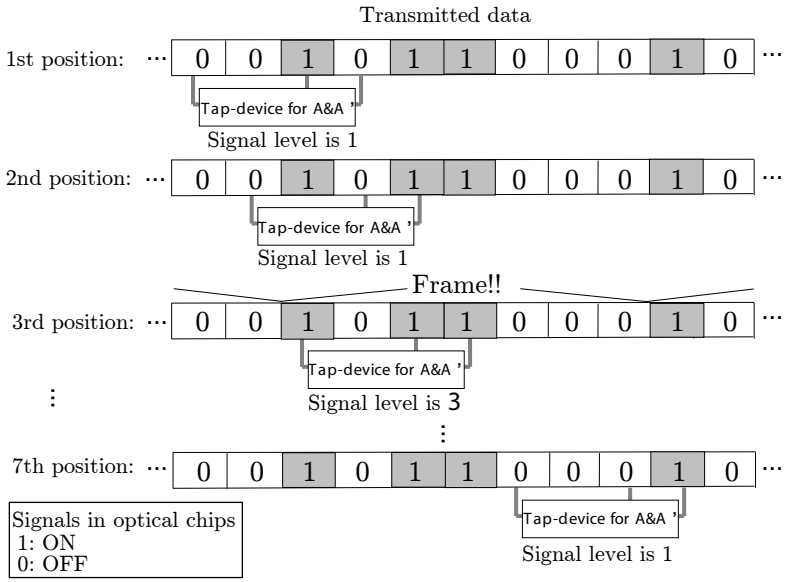

Figure 1.1: A situation that a user pair, say transmitter A and receiver A', tries to synchronize in a communication system applying an OOC of length 7 and weight 3: The codeword $X = \{0, 2, 3\}$ of the OOC is assigned to A&A', and A' use the corresponding tap-device to the codeword X to collect ON signals. In the first and second positions, the tap-device provides the level 1 respectively, but the level 3 in the third position. In this example, the tap-device provides the level 3 exactly once at seven possible positions of tap-devices because of the property $|X \cap (X + s)| \leq 1$ for every $s \not\equiv 0 \,(\mathrm{mod}\, 7)$ (the low auto-correlation property). Hence, the third position enables A' to synchronize, i.e., to know how the sequence of signals is partitioned into frames.

say the transmitters A and B, OFF signals of the signature sequence of the transmitter A (or B respectively) are influenced from ON signals at corresponding chips of that of the transmitter B (or A respectively) and then all signals at those chips are determined as ON. Note that, under the assumption that the synchronization is successfully done, when one transmits the information bit **1** in a frame, then the corresponding tap-device provide a high-level output even if it is influenced from the others, i.e., the information bit **1** is always successfully transmitted. On the other hand, when a user transmits the information bit **0** in a frame, in order to make the receiver recognize that the information bit is **0**, it is important to make the level of outputs in the frame lower and which is successfully done by the low cross-correlation property of the OOC to avoid high influences by the other transmitted frames. (See Figure 1.2, which is a situation that three user pairs communicate simultaneously utilizing an OOC of length 10 and weight 3.) Thus, it is required that values of λ_a and λ_c of the auto- and cross-correlations of OOCs are kept as lower as possible. For more detailed description of the system and for other related ideas, see [42, 102, 103, 82, 83].

OOCs with lower auto- and cross-correlations are required in order to assure a transmission under the condition that there are a given number of active users. Whereas, it is important to find OOCs with a larger number of codewords given parameters v, k, λ_a, and λ_c to increase

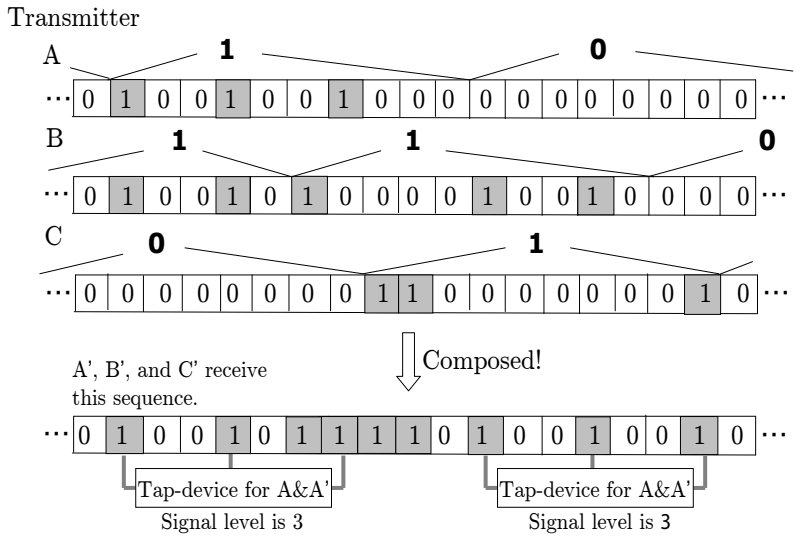

Figure 1.2: A situation that three user pairs communicate simultaneously utilizing an OOC of length 10 and weight 3: The user pairs A&A', B&B', and C&C' use the codewords $\{0,3,6\}$, $\{0,3,5\}$, and $\{0,1,2\}$ of the OOC, respectively. It is assumed that the synchronization is successfully done for every user pair. The transmitter A sends the sequence $\cdots 1001001000000000000\cdots$ of signals to A' by encoding the information bits $\cdots \mathbf{1}\,\mathbf{0}\cdots$ using their codeword as shown in this figure. Similarly, B and C sends sequences of packets to B' and C', respectively. As a result, those three sequences are composed into the sequence $\cdots 10010111101001001000\cdots$, and then all of A', B' and C' receive the same composed sequence. At the receiving end, A' recognizes that the information bits sent by A are $\cdots \mathbf{1}\,\mathbf{1}\cdots$, i.e., the former information bit **1** is successfully transmitted but the latter bit **0** failed to decode, which is caused by the high cross-correlation $\lambda_c = 2$ relative to the weight $k = 3$.

the number of potential users. An OOC with the maximum number of codewords for given v, k, λ_a, and λ_c is called *maximal*. In [53, 118], it was shown that a maximal $(v, k, \lambda_a, \lambda_c)$-OOC is equivalent to a combinatorial structure called a *maximal cyclic* $(\lambda+1)$-$(v, k, 1)$ *difference packing* when $\lambda = \lambda_a = \lambda_c$, and a tight upper bound of the maximum number of codewords of a (v, k, λ, λ)-OOC was given applying the well-known Johnson bound [67] for constant weight error-correcting codes. We denote the maximum number of codewords of $(v, k, \lambda_a, \lambda_c)$-OOCs by $M(v, k, \lambda_a, \lambda_c)$.

The problems to determine $M(v, k, \lambda_a, \lambda_c)$ and to construct maximal OOCs are difficult in general and remained largely unsettled. Nevertheless there are many known results for the case of $\lambda_a = \lambda_c = 1$. In this case, we can find a strong connection between OOCs and difference families. Let $\mathcal{F}$ be a $(v, k, \lambda_a, \lambda_c)$-OOC. Then, by the definitions of the auto- and cross-correlation properties, it is clear that

(i) $\lambda_a = 1$ if and only if any element of $\mathbb{Z}_v$ does not occur repeatedly in ΔX for every $X \in \mathcal{F}$,

(ii) $\lambda_c = 1$ if and only if $\Delta X \cap \Delta Y = \emptyset$ for every $X, Y \in \mathcal{F}$, $X \neq Y$.

By a simple counting argument, it is obvious that

$$M(v,k,1,1) \leq \Big\lfloor \frac{v-1}{k(k-1)} \Big\rfloor. \tag{1.9}$$

We say that a $(v,k,1,1)$-OOC attaining the bound 1.9 is *optimal*. Hence, we immediately see the following consequence:

Lemma 1.4.2. ([118]) The existence of a cyclic scarce $(v,k,1)$-DF with b blocks is equivalent to that of a $(v,k,1,1)$-OOC with b codewords. In particular, a $(nv,n,k,1)$-CDF with $n \leq k(k-1)$ gives a optimal $(nv,k,1,1)$-OOC.

By Lemma 1.4.2, in order to obtain a optimal $(v,k,1,1)$-OOC, we need only to construct a "maximal" cyclic scarce $(v,k,1)$-DF with respect to the number of blocks. As discussed in the previous sections, since there abundantly exist relative difference families, we can obtain many infinite series of optimal $(v,k,1,1)$-OOCs. Some of known results on constructions of $(v,k,1,1)$-OOCs are listed in Table 1.1. For more results on $(v,k,1,1)$-OOCs with small

Table 1.1: Known optimal $(v,k,1,1)$-OOCs

Construction	Parameters	$M(v,k,1,1)$
Projective geometry	$(v,k) = (\frac{q^m-1}{q-1}, q+1)$ q: a prime power	$\frac{q^m-1}{q^2-1}$, d: even $\frac{q^m-q}{q^2-1}$, d: odd
Affine geometry (also [93])	$(v,k) = (q^m-1, q)$ q: a prime power	$\frac{q^{m-1}-1}{q-1}$
[41, 98]	$k=3$, $v \not\equiv 14, 20 \pmod{24}$	$\lfloor \frac{n-1}{6} \rfloor$
[28, 29, 55]	$k=4$, $v \equiv 0, 6, 18, \pmod{24}$	$\lfloor \frac{n-1}{12} \rfloor$
Wilson's construction [110] using cyclotomy	$v = p = k(k-1)m+1$ p: any sufficiently large prime for given k	m

weight not listed in Table 1.1, see [2, 12, 13, 23, 30, 41, 31, 32, 33, 52, 53, 69, 78, 79]. Researches to find OOCs with a large number of codewords have been concentrated on the case when $\lambda_a = \lambda_c$ in many papers. However, it does not mean that a $(v,k,\lambda_a,\lambda_c)$-OOC with $\lambda_a \neq \lambda_c$ is of no interest. The advantage of using OOCs with $\lambda_a > 1$ or $\lambda_c > 1$ is that it enables a larger number of potential users (or equivalently codewords). In this case, there are several results, for example, see [3, 4, 5, 6, 7, 37, 40, 49, 51, 87], but the existence problem remains unsolved in most parts.

1.4.2 Conflict-avoiding codes

In the previous subsection, we considered an optical orthogonal code as an application of difference families. As described in the previous subsection, the low auto- and cross-correlation properties of an optical orthogonal code facilitate the detection of the expected signal in an optical CDMA communication channel. However, an optical orthogonal code with large λ_a and

small λ_c can be used as a "conflict-avoiding code," which can be applied in a collision channel without feedback [75, 57, 84, 85, 96]. A (v, k, λ_c)-*conflict-avoiding code* (CAC) is defined as a family of $(0, 1)$ sequences of length v and Hamming weight k satisfying $\sum_{i=0}^{v-1} x_i y_{i+s} \leq \lambda_c$ for any $X = (x_i), Y = (y_i) \in \mathcal{C}$ with $X \neq Y$ and every integer s, where all subscripts are taken modulo v. In this subsection, we provide a brief explanation how to use CACs in a collision channel without feedback.

In a sort of multiple-access collision channel without feedback, the time axis is partitioned into slots which corresponds to the transmission time for one packet and all users are supposed to have slot synchronization, but no other synchronization is assumed. In a particular slot, if none of the users is sending a packet, then the channel output in that slot is the silence symbol, that is, a null packet. If exactly one user is sending a packet in a particular slot, then the packet is transmitted successfully and the channel output in that slot is this packet value. If more than one user is sending packets in a particular slot simultaneously, then there is a conflict and the channel output in that slot is the unreadable collision symbol, called an *erasure*.

A codeword, say $X = (x_0, x_1, \ldots, x_{v-1})$ of a (v, k, λ_c)-CAC $\mathcal{C}$ with m codewords, is randomly assigned to each user pair, say transmitter A and receiver A', which controls his/her sending of packets in the following manner: By using the codeword $X = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$, the transmitter A sends k packets in each frame consisting of v slots. When the user pair A&A' becomes active (after some period of inactivity), the transmitter A sends a packet or a null packet in the j-th slot $(0 \leq j \leq v-1)$ of a frame according as $x_j = 1$ or $x_j = 0$. The transmitter A continues to use his codeword periodically in this manner until there are no more packets to be sent, and after that A must remain inactive for at least $v-1$ slots. Those (at least $v-1$) silent slots enable the receiver A' to synchronize without any assumption other than slot synchronization, which is a major difference from the synchronizing technique of optical orthogonal codes.

By using the codeword $X = (x_0, x_1, \ldots, x_{v-1}) \in \mathcal{C}$, the transmitter A sends k packets in each frame consisting of v slots. When A is sending a message by using his/her codeword X_i, different message from the other transmitter B may be sent by the codeword $X_j \in \mathcal{C}$ or its cyclic shift since only slot synchronization is assumed. If more than one user sends packets simultaneously in a particular slot, the packets cause a collision which results in an erasure. It is easily checked that a (v, k, λ_c)-CAC with m codewords has the property that at least $\sigma = k - \lambda_c(u-1)$ successful packet transmissions in a frame are guaranteed for each active user, provided that at most u users out of m potential users are active. In order to guarantee for each user that at least one information packets in a frame are survived from collision, the weight k of the CAC have to satisfy $k \geq \lambda_c(u-1)+1$. If there is at least one packet survived from collision, there may be a chance by utilizing an error correcting code as an "inner code" to correct erasures. Let ℓ be the bit length of each slot. An $(k\ell, \sigma\ell, k\ell - \sigma\ell + 1)$ shortened Reed-Solomon (RS) code over $\mathbb{F}_q$ can be used as an inner code for each user to encode his σ information packets into k transmitted packets, since a $(k\ell, \sigma\ell, k\ell - \sigma\ell + 1)$ shortened RS code can correct $k\ell - \sigma\ell$ position erasures where the user's packets suffer from collision. Then the $k - \sigma$ information packets are recovered from the σ survived packets at the receiver. (See Figure 1.3, which is a situation that three user pairs communicate simultaneously applying a CAC of length 13 and weight 3.) We should mention that errors caused by noises in a channel besides erasures due to collisions are not negligible in a practical data transmission and an

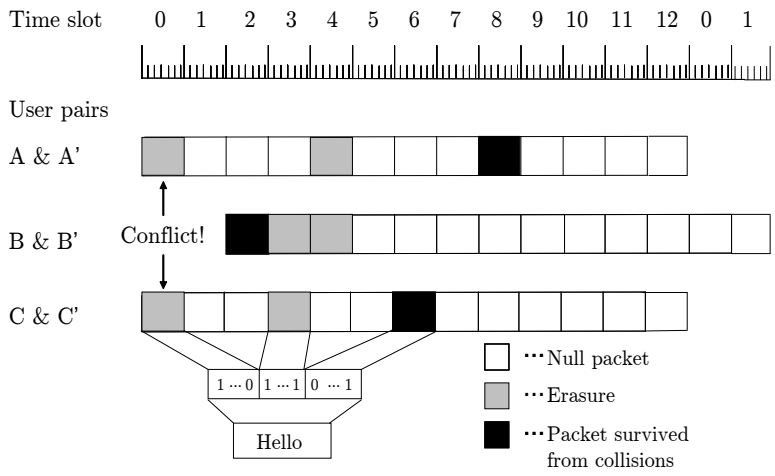

Figure 1.3: A situation that three user pairs communicate simultaneously applying the $(13, 3, 1)$-CAC $\mathcal{F} = \{\{0, 1, 2\}, \{0, 3, 6\}, \{0, 4, 8\}\}$: The transmitter C is sending the message "Hello" to the receiver C', which is translated into a codeword of an inner code and it is partitioned into three packets. The user pairs A&A', B&B', and C&C' use the codewords $\{0, 4, 8\}$, $\{0, 1, 2\}$, and $\{0, 3, 6\}$ of the CAC, respectively. In this example, for each user pair there is at least one packet (exactly one packet in this case) survived from collision since $\lambda_c = 1$ and the number of active users is at most three.

appropriate inner code should be used for error and erasure corrections. In order to use an inner code, every codeword of C should have constant weight k.

Obviously, a CAC can be seen as an OOC without the auto-correlation property, which implies that the maximum size of a CAC should be larger than that of an OOC with the same parameters. Noting that $|X \cap (X + s)| = k$ for $X \in \binom{\mathbb{Z}_v}{k}$ and some $s \in \mathbb{Z}_v \setminus \{0\}$ if and only if $k \mid v$ and $X = \frac{v}{k}\mathbb{Z}_v$, any $(v, k, 1)$-CAC consists of codewords of a $(v, k, k-1, 1)$-OOC and the codeword $X = \frac{v}{k}\mathbb{Z}_v$. In particular, any maximal $(v, k, k-1, 1)$-OOC is also a maximal $(v, k, 1)$-CAC when $k \nmid v$. In the case of $k = 3$ and $\lambda_c = 1$, Levenshtein and Tonchev [74] and Levenshtein [73] obtained the following results, respectively:

Theorem 1.4.3. ([74]) Let v be a positive integer. Then

$$M(v, 3) = \frac{v-2}{4} \quad \text{if } v \equiv 2 \pmod 4$$

holds, where $M(v, 3)$ means the maximum number of codewords of $(v, 3, 1)$-CAC.

Theorem 1.4.4. ([73]) Let v be an odd integer. Then

$$M(v, 3) = \frac{v}{4} + O\left(\frac{v}{\log_2 v}\right).$$

Furthermore, Jimbo et al. [66] obtained the following lower and upper bounds:

Theorem 1.4.5. ([66]) Let $v = 4m$ be a positive integer. Then

$$\frac{v}{6} + O(\log_4 m) \leq M(v, 3) \leq \frac{7}{32}v + \epsilon$$

holds, where ϵ is a non-negative constant depending on the congruence of m modulo 24. Especially, the lower bound is sharp for any v being a power of 2, and the upper bound is sharp for every v such that $m \equiv 2 \pmod 4$.

Thus, there are some results on the existence of maximal $(v, 3, 1)$-CACs (for other results, see [106, 107]). However, as far as the author knows, there are no results in the case when $k > 3$.

1.5 Outline of this thesis

In the remainder of this thesis, we discuss existence problems and constructions of several kinds of difference families and discuss their relations to combinatorial codes, in particular, optical orthogonal codes and conflict-avoiding codes in the following four chapters.

In Chapter 2, we introduce a new type of cyclic difference families, so-called "cyclic δ-support difference families," including ordinary difference families, which is motivated from a certain classification of optical orthogonal codes. In particular, we find a tight upper bound on the number of codewords of $(v, 4, 2, 1)$-OOCs and investigate relations between maximal OOCs and cyclic δ-support difference families. Furthermore, some direct and recursive constructions of $(v, 4, 2, 1)$-OOCs attaining the upper bound is presented. As a consequence, we will obtain many new infinite series of maximal $(v, 4, 2, 1)$-OOCs.

In Chapter 3, we will discuss a relation between (almost) maximal $(v, k, 1)$-CACs ($(v, k, k-1, 1)$-OOCs) and cyclic δ-support difference families. Especially, we give a necessary and sufficient condition for the existence of a special class of cyclic δ-support difference families with small blocksize related to a problem of "perfect packings" and show that such difference families exist infinitely many by investigating the Kronecker density of the set of primes satisfying certain conditions. As consequences, it is shown that there exist infinitely many maximal $(v, k, 1)$-CACs with $\frac{v-1}{2(k-1)}$ codewords for $k = 3, 4$ and 5.

In Chapter 4, strong difference families, difference covers, and their relations to relative difference families are considered. Beginning with fundamental facts on strong difference families and difference covers, we apply some classical approach to construct a lot of new strong difference families and difference covers. Furthermore, we show an asymptotic existence theorem of relative difference families under the assumption of the existence of a strong difference family by generalizing Theorem 1.3.9 for $\lambda \geq 1$. Moreover, we improve Theorem 1.3.9 in the case when $k \leq 5$ and we show that if there exists an (N, k, μ) strong difference family for $k \leq 5$, there is a sufficiently large integer $q_{k,\mu}$ such that there exists an $(N \times \mathbb{F}_q, N \times \{0\}, \lambda = 1)$-DF for any prime power $q \equiv 1 \pmod \mu > q_{k,\mu}$. The results obtained in Chapter 4 also give a partial generalization of Theorem 1.1.3.

Chapter 5 is dedicated to study relative difference families with variable blocksize which is defined as a natural generalization of relative difference families so that blocksizes are variable. In particular, the existence of relative difference families with $G = \mathbb{Z}_{\frac{q^m-1}{n}}$, $N = (\frac{q^m-1}{q-1})\mathbb{Z}_{\frac{q^m-1}{n}}$,

$\lambda = \frac{q^{m-2}(q-1)}{en}$, and whose blocksizes are bounded from lower and upper, is proved using group characters over a finite field. As a corollary, we can find a new large family of optimal optical orthogonal codes whose auto- and cross-correlations are $\lambda_a = 1$ and $\lambda_c = 1$, respectively. It is remarkable that the new series includes $(q^2 - 1, q, 1)$-OOCs ($(q^2 - 1, q, 1)$ difference sets) listed in Table 1.1.

In Chapter 6, we provide concluding remarks and open problems in this thesis.

Chapter 2

Cyclic 8-support $(v, 4)_2$ difference families and $(v, 4, 2, 1)$ optical orthogonal codes

In this chapter, we introduce a new type of difference families which includes difference families treated in Chapter 1 as a special case. The new concept, called "δ-support difference families," is motivated from a certain classification of optical orthogonal codes with $\lambda_c = 1$. As described in Section 1.4.1 of Chapter 1, it is preferred in view of applications to optical CDMA communications that the values λ_a and λ_c of a $(v, k, \lambda_a, \lambda_c)$-OOC are as low as possible. On the other hand, when $\lambda_a > 1$ or $\lambda_c > 1$, in general a maximal $(v, k, \lambda_a, \lambda_c)$-OOC enables a larger number of codewords than maximal $(v, k, 1, 1)$-OOCs though there is a disadvantage such that robustness of communication systems with respect to synchronizations and collisions declines. Thus if we require more codewords, it may worth to consider OOCs with $\lambda_a > 1$ or $\lambda_c > 1$. In this chapter, we consider the case when $\lambda_a = 2$ and $\lambda_c = 1$ and obtain $(v, 4, 2, 1)$-OOCs with a larger number of codewords than $(v, 4, 1, 1)$-OOCs.

In this chapter, we study bounds and constructions of $(v, 4, 2, 1)$-OOCs in relation to δ-support difference families. In Section 2.1, the concept of δ-support difference families is introduced. In Section 2.2, a tight upper bound on $M(v, 4, 2, 1)$, which is the maximum number of codewords of $(v, 4, 2, 1)$-OOCs, is obtained. In Sections 2.3 and 2.4, many series of δ-support relative difference families and "optimal" $(v, 4, 2, 1)$-OOCs attaining the upper bound are constructed via finite fields. A relation between δ-support difference families and "cyclic kite-decompositions" of a complete multipartite graph is discussed and we consequently get a recursive construction of δ-support relative difference families. In Section 2.6, combining all previous results, we obtain many infinite series of optimal $(v, 4, 2, 1)$-OOCs.

2.1 Definition of cyclic δ-support difference families

Given a k-subset $X \in \binom{\mathbb{Z}_v}{k}$, the *support* of the list ΔX of differences of X, denoted by $\mathrm{supp}\Delta X$, is the set of underlying elements in the multiset ΔX. Note that $k-1 \leq |\mathrm{supp}\Delta X| \leq k(k-1)$

for any $X \in \binom{\mathbb{Z}_v}{k}$. Furthermore, we define

$$\mu(X) = \max\{m_a(\Delta X) \,|\, a \in \Delta X\}, \tag{2.1}$$

where $m_a(\Delta X)$ means the multiplicity of the element $a \in \mathbb{Z}_v$ in ΔX. Then, it is easy to see that

$$\mu(X) = \max\{|X \cap (X+s)| \big| s \in \mathbb{Z}_v \setminus \{0\}\}. \tag{2.2}$$

From this correspondence, we have:

Lemma 2.1.1. Every $(v, k, \lambda_a, 1)$-OOC can be viewed as a family $\mathcal{F} \subseteq \binom{\mathbb{Z}_v}{k}$ satisfying the following conditions:

(i) $\lambda_a = \max\{\mu(X) \,|\, X \in \mathcal{F}\}$,

(ii) $\Delta X \cap \Delta Y = \emptyset$ for any $X, Y \in \mathcal{F}$ with $X \neq Y$.

The above conditions (i) and (ii) are corresponding to its auto- and cross-correlation properties, respectively.

Now we introduce new difference families. For positive integers δ and μ with $k-1 \leq \delta \leq k(k-1)$ and $1 \leq \mu \leq k$, let $\mathcal{F}$ be a family of k-subsets (called *blocks*) of $\mathbb{Z}_v$ such that $|\mathrm{supp}\Delta B| = \delta$ and $\mu(B) = \mu$ for every $B \in \mathcal{F}$. We say that $\mathcal{F}$ is a *cyclic δ-support $(v,k)_\mu$ scarce difference family*, shortly denoted as δ-supp $(v,k)_\mu$-CDF, if

$$\Delta B \cap \Delta B' = \emptyset \tag{2.3}$$

holds for any $B, B' \in \mathcal{F}$ with $B \neq B'$. If the number of blocks in $\mathcal{F}$ is maximum for given v, k, μ, δ, we say that the family $\mathcal{F}$ is *maximal*. A cyclic δ-support $(nv,k)_\mu$ scarce difference family $\mathcal{F}$ is called *relative to $v\mathbb{Z}_{nv}$*, denoted by δ-supp $(nv,n,k)_\mu$-CDF, if it satisfies the property

$$\bigcup_{B \in \mathcal{F}} \mathrm{supp}\Delta B = \mathbb{Z}_{nv} \setminus v\mathbb{Z}_{nv}.$$

When $n = 1$, a δ-supp $(v,1,k)_\mu$-CDF is also called a perfect δ-supp $(v,k)_\mu$-CDF. The number of blocks of a δ-supp $(nv,n,k)_\mu$-CDF is equal to $\frac{n(v-1)}{\delta}$ and hence we obviously have the necessary condition $n(v-1) \equiv 0 \pmod{\delta}$. Note that $|\mathrm{supp}\Delta X| = k(k-1)$ iff $\mu(X) = 1$ for any $X \in \binom{\mathbb{Z}_v}{k}$, i.e., $\delta = k(k-1)$ iff $\mu = 1$. By definitions, the following lemma is immediate:

Lemma 2.1.2. Any δ-supp $(nv,n,k)_\mu$-CDF gives an $(nv,k,\mu,1)$-OOC with $n(v-1)/\delta$ codewords.

2.2 Upper bounds for $M(v,4,2,1)$

To get a tight upper bound similar to (1.9) for $(v,k,\lambda_a,1)$-OOCs with $\lambda_a \geq \lambda_c = 1$, we need to know relations between $|\mathrm{supp}\Delta X|$ and $X \in \binom{\mathbb{Z}_v}{k}$.

From now on, we fix the weight k as 3 or 4. For the case of $k = 3$ and $|\mathrm{supp}\Delta X| < 6$ we can easily specify the following correspondence between $|\mathrm{supp}\Delta X|$ and X:

Lemma 2.2.1. For $X \in \binom{\mathbb{Z}_v}{3}$, it holds that

$$|\mathrm{supp}\Delta X| = \begin{cases} 2 & \text{iff } X = (\frac{v}{3})\mathbb{Z}_v, \\ 3 & \text{iff } X \subset (\frac{v}{4})\mathbb{Z}_v, \\ 4 & \text{iff } X = \{0, a, 2a\} \text{ except for the case } |\mathrm{supp}\Delta X| = 2 \text{ and } 3, \\ 5 & \text{iff } X = \{0, a, v/2\} \text{ except for the case } |\mathrm{supp}\Delta X| = 3. \end{cases}$$

Proof: We classify all forms of triples $X \in \binom{\mathbb{Z}_v}{3}$ by $|\mathrm{supp}\Delta X|$. Given $X = \{a_0, a_1, a_2\} \in \binom{\mathbb{Z}_v}{3}$, assume that

$$a_0 = 0 < a_1 < a_2 \leq v - 1$$

and associate X with the sequence $S(X) = (d_0, d_1, d_2)$, where $d_i = a_{i+1} - a_i$, $0 \leq i \leq 2$. Then we have $\Delta X = \{\pm d_0, \pm d_1, \pm d_2\}$ and

$$d_0 + d_1 + d_2 = v. \tag{2.4}$$

Now we suppose that there are repeated elements in ΔX, i.e., $|\mathrm{supp}\Delta X| \leq 5$, and we check all possible forms of $X \in \binom{\mathbb{Z}_v}{3}$ case by case.
Case 1. If $d_0 = v - d_1$, by (2.4), we have $d_2 = 0$, which contradicts to $k = 3$. Hence, this case is impossible.
Case 2. If $d_0 = v - d_2$ or $d_1 = v - d_2$, this is essentially same with Case 1.
Case 3. If $d_0 = d_1$, by (2.4), we have

$$2d_0 + d_2 = v. \tag{2.5}$$

We distinguish four subcases.

Subcase 3-1. If there are no further repeated elements in ΔX, we have $X = \{0, d_0, 2d_0\}$ and $\mathrm{supp}\Delta X = \{\pm d_0, \pm 2d_0\}$.

Subcase 3-2. If $d_0 = v - d_1$, by (2.5), we have $d_2 = 0$, which contradicts to $k = 3$. Hence, this subcase is impossible.

Subcase 3-3. If $d_0 = d_2$, by (2.5), we have $X = (\frac{v}{3})\mathbb{Z}_v$ and $\mathrm{supp}\Delta X = \{\pm v/3\}$.

Subcase 3-4. If $d_0 = v - d_2$, by (2.5), we have $d_1 = 0$, which contradicts to $k = 3$.
Case 4. If $d_0 = d_2$ or $d_1 = d_2$, this is essentially same with Case 3.
Case 5. If $d_0 = v - d_0$, we have $d_0 = v/2$ and

$$d_1 + d_2 = v/2. \tag{2.6}$$

Subcase 5-1. If there are no further repeated elements in ΔX, we have $X = \{0, v/2, v/2 + d_1\}$ and $\mathrm{supp}\Delta X = \{v/2, \pm d_1, v/2 \pm d_1\}$.

Subcase 5-2. If $d_1 = d_2$, by (2.6), we have $X \subseteq (\frac{v}{4})\mathbb{Z}_v$ and $\mathrm{supp}\Delta X = \{v/2, \pm v/4\}$.

Subcase 5-3. In the other cases, it is impossible by (2.6).
Case 6. If $d_1 = v - d_1$ or $d_2 = v - d_2$, we essentially find Case 5 again.

It is easy to see that all possible cases have been examined and the assertion follows. □

From this correspondence, the following lemma for the number $\mu(X)$ of $X \in \binom{\mathbb{Z}_v}{3}$ is shown:

Lemma 2.2.2. For $X \in \binom{\mathbb{Z}_v}{3}$, it holds that

$$\mu(X) = \begin{cases} 3 & \text{iff } |\mathrm{supp}\Delta X| = 2, \\ 2 & \text{iff } |\mathrm{supp}\Delta X| = 3, 4, \text{ or } 5, \\ 1 & \text{iff } |\mathrm{supp}\Delta X| = 6. \end{cases}$$

Proof: It is enough to check that each $X \in \binom{\mathbb{Z}_v}{3}$ of Lemma 2.2.1 has the corresponding $\mu(X)$, since all forms of $X \in \binom{\mathbb{Z}_v}{3}$ are completely classified according to $|\mathrm{supp}\Delta X|$ in Lemma 2.2.1. For example, any $X = \{0, a, 2a\} \in \binom{\mathbb{Z}_v}{3}$ with $|\mathrm{supp}\Delta X| = 4$ has

$$\Delta X = \{\pm a, \pm a, \pm 2a\} \text{ and } \mathrm{supp}\Delta X = \{\pm a, \pm 2a\}.$$

Then, by (2.1) and (2.2), we have $\mu(X) = 2$. By checking the other cases similarly, we easily get the assertion. □

Hence, we have the following upper bound on $M(v, 3, 2, 1)$:

Lemma 2.2.3. Let $v = 4^r m$, where m is not divisible by 4. Then it holds that

$$M(v, 3, 2, 1) \leq \begin{cases} \lfloor (v-1)/4 \rfloor & \text{if } r = 0, \\ v/4 & \text{if } r \geq 1. \end{cases}$$

For example, when $r \geq 1$, since there may be a $(v, 3, 2, 1)$-OOC which contains one codeword X with $|\mathrm{supp}\Delta X| = 3$ and whose every other codeword Y satisfies $|\mathrm{supp}\Delta Y| = 4$, we have

$$M(v, 3, 2, 1) \leq \left\lfloor \frac{v-1-3}{4} + 1 \right\rfloor = \frac{v}{4}.$$

Remark 2.2.4. In general, for any k and $X \in \binom{\mathbb{Z}_v}{k}$ with $|\mathrm{supp}\Delta X| \equiv 1 \pmod 2$, ΔX must contain the element $v/2$ and then v must be divisible by 2. From this fact, any $(v, k, \lambda_a, 1)$-OOC contains at most one codeword $X \in \binom{\mathbb{Z}_v}{k}$ with $|\mathrm{supp}\Delta X| \equiv 1 \pmod 2$.

Similarly, for the case of $k = 4$ and $|\mathrm{supp}\Delta X| < 12$ we have the following correspondence:

Lemma 2.2.5. For $X \in \binom{\mathbb{Z}_v}{4}$, it holds that

$$|\mathrm{supp}\Delta X| = \begin{cases} 3 & \text{iff } X = (\frac{v}{4})\mathbb{Z}_v, \\ 4 & \text{iff } X \subset (\frac{v}{5})\mathbb{Z}_v, \\ 5 & \text{iff } X = \{0, a, v/2, v/2+a\} \text{ or } X \subset (\frac{v}{6})\mathbb{Z}_v \text{ except for } |\mathrm{supp}\Delta X| = 3, \\ 6 & \text{iff } X = \{0, a, 2a, 3a\} \text{ or } X \subset (\frac{v}{7})\mathbb{Z}_v \text{ except for } |\mathrm{supp}\Delta X| = 3, 4 \text{ and } 5, \\ 7 & \text{iff } X = \{0, a, v/2, v-a\},\ X = \{0, a, v/2-a, v/2\}, \text{ or } X \subset (\frac{v}{8})\mathbb{Z}_v \\ & \quad \text{except for } |\mathrm{supp}\Delta X| = 3, 5 \text{ and } 6, \\ 8 & \text{iff } X = \{0, a, a+b, 2a+b\},\ X = \{0, a, v/3, 2v/3\}, \text{ or } X = \{0, a, 2a, 4a\} \\ & \quad \text{except for } |\mathrm{supp}\Delta X| = 3, 4, 5, 6 \text{ and } 7, \\ 9 & \text{iff } X = \{0, a, 2a, v/2\} \text{ or } X = \{0, a, v/2, 3v/4\} \text{ except for} \\ & \quad |\mathrm{supp}\Delta X| = 3, 5 \text{ and } 7, \\ 10 & \text{iff } X = \{0, a, 2a, 2a+b\} \text{ except for } |\mathrm{supp}\Delta X| = 3, 4, 5, 6, 7, 8 \text{ and } 9, \\ 11 & \text{iff } X = \{0, a, b, v/2\} \text{ except for } |\mathrm{supp}\Delta X| = 3, 5, 7 \text{ and } 9. \end{cases}$$

Proof: Similar to the case of $k = 3$, we can assume $a_0 = 0 < a_1 < a_2 < a_3 \leq v - 1$ for $X = \{a_0, a_1, a_2, a_3\} \in \binom{\mathbb{Z}_v}{4}$. We associate X with the sequence $S(X) = (d_0, d_1, d_2, d_3)$, where $d_i = a_{i+1} - a_i$, $0 \leq i \leq 3$. Then we have

$$\Delta X = \{\pm d_0, \pm d_1, \pm d_2, \pm d_3, \pm(d_0 + d_1), \pm(d_1 + d_2)\}$$

and

$$d_0 + d_1 + d_2 + d_3 = v. \tag{2.7}$$

Suppose that there are repeated elements in ΔX, i.e., we have $|\mathrm{supp}\Delta X| \leq 11$, then by checking all possible forms of $X \in \binom{\mathbb{Z}_v}{4}$ case by case, one can easily, though tediously, get the assertion. □

Similarly to Lemma 2.2.2, one can see that the following holds.

Lemma 2.2.6. For $X \in \binom{\mathbb{Z}_v}{4}$, it holds that

$$\mu(X) = \begin{cases} 4 & \text{iff } |\mathrm{supp}\Delta X| = 3 \text{ or } 5 \ (X = \{0, a, v/2, v/2 + a\}), \\ 3 & \text{iff } |\mathrm{supp}\Delta X| = 4,\ 5 \ (X = \{0, v/6, v/3, v/2\},\ X = \{0, v/6, v/3, 2v/3\}), \\ & \quad 6 \ (X = \{0, a, 2a, 3a\}) \text{ or } 8 \ (X = \{\{0, a, v/3, 2v/3\}), \\ 2 & \text{iff } |\mathrm{supp}\Delta X| = 6, 7, 8, 9, 10 \text{ or } 11 \\ & \quad \text{except for } \mu(X) = 3, \\ 1 & \text{iff } |\mathrm{supp}\Delta X| = 12. \end{cases}$$

Then we have the following upper bounds on $M(v, 4, 3, 1)$ and $M(v, 4, 2, 1)$:

Lemma 2.2.7. Let $v = 5^r 6^s m$, where m is not divisible by 5 and 6. Then it holds that

$$M(v, 4, 3, 1) \leq \begin{cases} \lfloor (v+1)/6 \rfloor & \text{if } r \geq 1,\ s = 0, \\ v/6 & \text{if } r = 0,\ s \geq 1, \\ \lfloor (v+2)/6 \rfloor & \text{if } r \geq 1,\ s \geq 1, \\ \lfloor (v-1)/6 \rfloor & \text{if } r = s = 0. \end{cases}$$

Lemma 2.2.8. Let $v = 2^r 7^s m$, where m is not divisible by 2 and 7. Then it holds that

$$M(v, 4, 2, 1) \leq \begin{cases} \lfloor v/8 \rfloor & \text{if } r \geq 1,\ s = 0, \\ \lfloor (v+1)/8 \rfloor & \text{if } r = 0,\ s \geq 1, \\ \lfloor (v+2)/8 \rfloor & \text{if } r \geq 1,\ s \geq 1, \\ \lfloor (v-1)/8 \rfloor & \text{if } r = s = 0. \end{cases}$$

For example, when $r \geq 1$ and $s \geq 1$ in Lemma 2.2.8, since there may be a $(v, 4, 2, 1)$-OOC which contains two codewords X and X' with $|\mathrm{supp}\Delta X| = 6$ and $|\mathrm{supp}\Delta X'| = 7$ and whose every other codeword Y satisfies $|\mathrm{supp}\Delta Y| = 8$, we have

$$M(v, 4, 2, 1) \leq \left\lfloor \frac{v - 1 - 6 - 7}{8} + 2 \right\rfloor = \left\lfloor \frac{v+2}{8} \right\rfloor.$$

We say that a maximal $(v, 4, 2, 1)$-OOC attaining the bound of Lemma 2.2.8 is *optimal*.

2.3 Direct constructions of 8-supp $(np, n, 4)_2$-CDFs

Note that an optimal $(v, 4, 2, 1)$-OOC contains at most two codewords $X \in \binom{\mathbb{Z}_v}{4}$ such that the support size of the list of differences is less than 8. So, to construct such an optimal $(v, 4, 2, 1)$-OOC we mainly use quadruples $X \in \binom{\mathbb{Z}_v}{4}$ such that $|\mathrm{supp}\Delta X| = 8$. Again, we recall that if

$\mu(X) = 2$ and $|\mathrm{supp}\Delta X| = 8$ for $X \in \binom{\mathbb{Z}_v}{4}$, X has either of the forms $X = \{0, a, a+b, 2a+b\}$ or $X = \{0, a, 2a, 4a\}$, where $X = \{0, a, 2a, 4a\}$ has the same support of the list of differences with $X' = \{0, a, 3a, 4a\}$ which is a special case of $X = \{0, a, a+b, 2a+b\}$. Now, we note the following important facts:

(i) If b is in $2\mathbb{Z}_v$, we can take
$$X' = \{\pm\frac{b}{2}, \pm\frac{b+2a}{2}\}$$
instead of X since $X' = X - \frac{b+2a}{2}$, i.e., X' is a translation of X. Conversely, any quadruple $X = \{\pm a, \pm b\} \in \binom{\mathbb{Z}_v}{4}$ can be replaced by $X' = \{0, a', a'+b', 2a'+b'\}$ with $(a', b') = (b-a, 2a)$ since we have $X + b = X'$.

(ii) If $X = \{\pm a, \pm b\} \in \binom{\mathbb{Z}_v}{4}$ and $|\mathrm{supp}\Delta X| = 8$, then $\mu(X) = 2$. In fact, we have $\mu(X) \neq 2$ and $|\mathrm{supp}\Delta X| = 8$ if and only if $X = \{0, a, v/3, 2v/3\}$ by Lemma 2.2.6.

(iii) If a (or b) in $X = \{0, a, a+b, 2a+b\}$ is invertible in $\mathbb{Z}_v$, then X can be written as
$$X = a \cdot \{0, 1, c+1, c+2\} \text{ (or } = b \cdot \{0, c, c+1, 2c+1\}),$$
where $c = ba^{-1}$ (or $= ab^{-1}$, respectively).

By Lemma 2.2.8, it immediately follows:

Lemma 2.3.1. Any 8-supp $(nv, n, 4)_2$-CDF with $n \leq 6$ gives an optimal $(nv, 4, 2, 1)$-OOC.

In this section, we find direct constructions for 8-supp $(np, n, 4)_2$-CDFs in the following cases:

(i) $n = 1$ and any prime $p \equiv 1 \pmod 8$,

(ii) $n = 2$ and any prime $p \equiv 1 \pmod 4$,

(iii) $n = 4$ and any prime $p > 5$,

(iv) $n = 8$ and any prime $p \equiv 1 \pmod 4$ with $p > 5$.

All 8-supp $(np, n, 4)_2$-CDFs obtained in Subsections 2.3.1, 2.3.2, and 2.3.3 generate optimal $(np, 4, 2, 1)$-OOCs by Lemma 2.3.1. In Subsection 2.3.4, we will obtain cyclic 8-supp $(8p, 8, 4)_2$-CDFs corresponding to $(8p, 4, 2, 1)$-OOCs. Though such OOCs are not optimal, it easily leads to optimal ones with the same parameters by adding the single codeword $\{\pm p, \pm 2p\}$ to those.

2.3.1 Perfect 8-supp $(p, 4)_2$-CDFs for primes p

Example 2.3.2. For the prime $p = 17$, the supports of the lists of differences of $X = \{\pm 10, \pm 11\}$ and $Y = 2 \cdot \{\pm 10, \pm 11\}$ defined on $\mathbb{Z}_p$ are given by
$$\mathrm{supp}\Delta X = \{\pm 1, \pm 3, \pm 4, \pm 5\}$$
and
$$\mathrm{supp}\Delta Y = \{\pm 2, \pm 6, \pm 7, \pm 8\},$$
respectively. Thus, $\mathcal{F} = \{X, Y\}$ gives a perfect 8-supp $(17, 4)_2$-CDF.

The following lemma was basically used to construct optimal $(p, k, 1, 1)$-OOCs (or cyclic difference families) for primes p in some papers, for example, [2, 19, 34, 35, 110].

Lemma 2.3.3. Let p be a prime and X be a k-subset of $\mathbb{Z}_p$. If S is a subset of $\mathbb{Z}_p \setminus \{0\}$ such that $\mathrm{supp}\Delta X \cdot S$ has no repeated elements, then $\mathcal{F} = \{X \cdot s \,|\, s \in S\}$ is a $(p, k, \lambda_a, 1)$-OOC with $\lambda_a = \mu(X)$ and with $|S|$ codewords.

The problem of finding a set $S \subset \mathbb{Z}_p$ satisfying the condition of Lemma 2.3.3 and having the maximum possible size is related to a problem of "packings" treated in [19] (see also Chapter 3). In the case when $p = 2es + 1$ and $\mathrm{supp}\Delta X$ has the form $\{1, -1\} \cdot L$, where the elements of L are lying in pairwise distinct cosets of C_0^e, we can take S as a complete system of representatives for the cosets of $\{1, -1\}$ in C_0^e. In this way, Construction 3.3 in [19] corresponds to the case when $\lambda_a = 1$.

In the following theorem, we apply Lemma 2.3.3 to the set X of the fourth roots of unity in $\mathbb{Z}_p$.

Theorem 2.3.4. Let $p \equiv 1 \pmod 8$ be a prime and let 2^e be the largest power of 2 dividing $p-1$. Then there exists a perfect 8-supp $(p, 4)_2$-CDF whose codewords are cosets of the fourth roots of unity in $\mathbb{Z}_p$ if and only if -4 is not a 2^eth power in $\mathbb{Z}_p$.

Proof: Set $p = 8t + 1$ and let $C_0^{2t} = \langle c \rangle$ be the group of fourth roots of unity in $\mathbb{Z}_p$. Note that we have

$$\mathrm{supp}\Delta C_0^{2t} = \pm\{2, 2c, c + 1, c - 1\} = C_0^{2t} \cdot \{c + 1, 2\}.$$

So there exists a perfect 8-supp $(p, 4)_2$-CDFs whose codewords are cosets of C_0^{2t} if and only if there exists a t-subset T of $\mathbb{Z}_p^\times$ such that $\{1, 2/(c+1)\} \cdot T$ is a complete system of representatives for the cosets of C_0^{2t} in $\mathbb{Z}_p^\times$. When we write $2/(c + 1) = \alpha^x$, where α is a primitive root of $\mathbb{Z}_p$, this is equivalent to that there exists a t-subset Y of $\mathbb{Z}_{2t}$ such that $\{0, x\} + Y = \mathbb{Z}_{2t}$. By Corollary 2.7 in [19] (Theorem 3.3.5 in Chapter 3), such a subset Y exists if and only if $2t/\gcd(x, 2t)$ is even and hence if and only if 2^{e-2} is not a divisor of x, that is to say that $2/(c + 1)$ is not a 2^{e-2}th power in $\mathbb{Z}_p$. Observing that $(2/(c + 1))^4 = -4$, the assertion then follows. In fact, we have that

$$\frac{2}{c+1} \in C_0^{2^{e-2}} \text{ iff } \left(\frac{2}{c+1}\right)^{\frac{p-1}{2^{e-2}}} = 1 \text{ iff } (-4)^{\frac{p-1}{2^e}} = 1,$$

i.e., -4 is a 2^eth power in $\mathbb{Z}_p$. □

When the condition $-4 \notin C_0^{2e}$ is satisfied, the 8-supp $(p, 4)_2$-CDF given by Theorem 2.3.4 is explicitly given by

$$\mathcal{F} = \{C_0^{2t} \cdot \alpha^{2xi+j} \,|\, 0 \le i < t/\gcd(x, 2t); 0 \le j < \gcd(x, 2t)\},$$

where $2/(c + 1) = \alpha^x$.

The following are all primes $p < 1000$ satisfying $p \equiv 1 \pmod 8$ and the condition of Theorem 2.3.4:

$$\begin{aligned} p \;=\; & 73, 89, 97, 193, 233, 241, 257, 281, 337, 353, 401, 433, \\ & 449, 577, 601, 617, 641, 673, 769, 881, 929, 937, 977. \end{aligned}$$

In the following theorem, we apply Lemma 2.3.3 to $X = \{\pm c, \pm(c + 2)\}$ with $e = 4$.

Table 2.1: An element $c \in \mathbb{Z}_p^\times$ such that $(1, c, c+1, c+2)$ is a complete system of representatives for the cosets of C_0^4 in $\mathbb{Z}_p^\times$ for each prime $p \equiv 1 \pmod 8$, $41 \le p \le 6577$, except for primes covered by Theorem 2.3.3.

p	c	p	c	p	c	p	c
41	5	1657	21	3121	29	4889	6
113	10	1993	5	3209	10	4969	67
137	23	2113	5	3217	40	5233	37
313	13	2129	28	3313	10	5273	31
409	21	2137	29	3433	18	5393	11
457	10	2153	9	3593	12	5417	6
521	32	2297	5	3761	39	5449	38
569	10	2377	17	3769	40	5641	29
593	9	2521	72	3881	6	5657	24
761	6	2617	10	3929	19	5801	5
809	11	2633	20	4073	31	5849	55
857	6	2713	10	4441	37	5897	6
953	9	2729	22	4649	19	6073	13
1129	11	2777	6	4657	19	6217	10
1201	65	2953	17	4729	29	6329	11
1249	19	3001	69	4793	9	6473	6
1321	13	3089	11	4817	9		

Theorem 2.3.5. There exists a perfect 8-supp $(p, 4)_2$-CDF for every prime $p \equiv 1 \pmod 8$.

Proof: Since Example 2.3.2 shows the existence of a perfect 8-supp $(17, 4)_2$-CDF, we consider the case of $p \ge 41$. Take $X = \{\pm c, \pm(c+2)\}$ with an element $c \in \mathbb{Z}_p$ such that $L = \{1, c, c+1, c+2\}$ is a complete system of representatives for the cosets of C_0^4 in $\mathbb{Z}_p^\times$. Note that for any prime $p \equiv 1 \pmod 8$ with $p \ge 6673$ such an element c always exists in $\mathbb{Z}_p^\times$ by Theorem 1.3.8. The remaining cases $41 \le p \le 6577$ are covered by computer search (see Table 2.1). By noting that

$$\mathrm{supp}\Delta X = \pm 2 \cdot L,$$

if we take a complete system S of representatives for the cosets of $\{1, -1\}$ in C_0^4, we have

$$\pm 2 \cdot L \cdot S = \mathbb{Z}_p^\times.$$

It follows that $\mathcal{F} = \{X \cdot s \mid s \in S\}$ is the desired CDF. □

Note that Theorem 2.3.5 includes Theorem 2.3.4 as an existence theorem, but the construction of Theorem 2.3.4 is more direct than Theorem 2.3.5.

2.3.2 8-supp $(2p, 2, 4)_2$-CDFs for primes p

The following lemma was used to construct optimal $(np, k, 1, 1)$-OOCs for primes p in many papers, for example, [2, 19, 22, 24, 23, 28, 29, 53, 55, 78] (see also Chapter 4).

Lemma 2.3.6. Let p be a prime and X be a k-subset of $\mathbb{Z}_n \times \mathbb{Z}_p$ satisfying $p \nmid n$. Set $\mathrm{supp}\Delta X = \bigcup_{i \in \mathbb{Z}_n} \{i\} \times L_i$, where L_i's are subsets of $\mathbb{Z}_p$, and assume that there exists a subset S of $\mathbb{Z}_p$ such that $L_i \cdot S$ has no repeated elements for each $i \in \mathbb{Z}_n$. Then the family $\mathcal{F} = \{X \cdot (1, s) \mid s \in S\}$ is an $(np, k, \lambda_a, 1)$-OOC with $\lambda_a = \mu(X)$ and $|S|$ codewords.

Lemma 2.3.6 is essentially applied in this and next subsections to construct 8-supp $(np, n, 4)_2$-CDFs for $n = 2, 4$ and 8.

Theorem 2.3.7. There exists an 8-supp $(2p, 2, 4)_2$-CDFs for every prime $p \equiv 1 \pmod 4$.

Proof: Put $p = 4t + 1$ and identify $\mathbb{Z}_{2p}$ with $\mathbb{Z}_2 \times \mathbb{Z}_p$. Consider

$$X = \{\pm(0, 1), \pm(1, c)\} \subset \mathbb{Z}_2 \times \mathbb{Z}_p,$$

where c is a primitive fourth root of unity. Note that we have

$$\mathrm{supp}\Delta X = \bigcup_{i \in \mathbb{Z}_2} \{i\} \times L_i,$$

where $L_0 = 2 \cdot C_0^t$ and $L_1 = (c - 1) \cdot C_0^t$. Now, let S be a complete system of representatives for the cosets of C_0^t in $\mathbb{Z}_p^\times$. Then, we obviously have $L_i \cdot S = \mathbb{Z}_p^\times$ for $i = 1, 2$ and hence, by Lemma 2.3.6, $\mathcal{F} = \{X \cdot (1, s) \,|\, s \in S\}$ is the desired CDF. □

2.3.3 8-supp $(4p, 4, 4)_2$-CDFs for primes p

Example 2.3.8. The set of the eight quadruples

$$\begin{array}{lll} W_h = & (1, h) \cdot \{(0, 0), (1, 1), (0, 6), (1, 7)\} & \text{for } h = 1, 13, \\ X_i = & (1, i) \cdot \{(0, 0), (3, 1), (2, 8), (1, 9)\} & \text{for } i = 1, 13, \\ Y_j = & (1, j) \cdot \{(0, 0), (1, 1), (1, 7), (2, 8)\} & \text{for } j = 2, 8, \\ Z_k = & (1, k) \cdot \{(0, 0), (2, 1), (2, 4), (0, 5)\} & \text{for } k = 3, 10, \end{array}$$

over $\mathbb{Z}_4 \times \mathbb{Z}_{17}$ give an 8-supp $(68, 4, 4)_2$-CDF.

Theorem 2.3.9. There exists an 8-supp $(4p, 4, 4)_2$-CDF for every prime $p > 5$.

Proof: We give two constructions as follows:

(*Construction for non-Fermat prime p's*) Identify $\mathbb{Z}_{4p}$ with $\mathbb{Z}_4 \times \mathbb{Z}_p$. Consider

$$X = \{\pm(0, \alpha^{2^{e-1}} - 1), \pm(1, \alpha^{2^{e-1}} + 1)\},$$

where α is a primitive root of $\mathbb{Z}_p$ and 2^e is the largest power of 2 in $p - 1$. We have:

$$\mathrm{supp}\Delta X = \bigcup_{i \in \mathbb{Z}_4} \{i\} \times L_i,$$

where $L_0 = 2 \cdot \{\pm(\alpha^{2^{e-1}} - 1)\}$, $L_1 = 2 \cdot \{1, \alpha^{2^{e-1}}\}$, $L_2 = 2 \cdot \{\pm(\alpha^{2^{e-1}} + 1)\}$ and $L_3 = -L_1$. Consider the set $S = \{\alpha^{2^e i + j} \,|\, 0 \le i < (p - 1)/2^e; 0 \le j < 2^{e-1}\}$. It is easy to see that $L_i \cdot S = \mathbb{Z}_p^\times$ for $0 \le i \le 3$. Hence, by Lemma 2.3.6, we have that $\mathcal{F} = \{X \cdot (1, s) \,|\, s \in S\}$ is the desired CDF.

(*Construction for primes* $p \equiv 1 \pmod 8$) Take the following four quadruples over $\mathbb{Z}_4 \times \mathbb{Z}_p$:

$$\begin{array}{ll} X_1 = & \{\pm(0, c_1), \pm(1, c_1 + 2\}, \\ X_2 = & \{\pm(1, c_1(c_2 + 1)), \pm(2, (c_1 + 2)(c_2 + 1))\}, \\ X_3 = & \{\pm(0, c_2), \pm(3, c_2 + 2)\}, \text{ and} \\ X_4 = & \{\pm(3, c_2(c_1 + 1)), \pm(2, (c_2 + 2)(c_1 + 1))\} \end{array}$$

such that

$$(c_1, c_1+1, c_1+2) \in C_3^4 \times C_1^4 \times C_0^4$$

and

$$(c_2, c_2+1, c_2+2) \in C_1^4 \times C_2^4 \times C_3^4,$$

where such elements $c_1, c_2 \in \mathbb{Z}_p$ exist for all $p \geq 6673$ by Theorem 1.3.8. Note that there is only one Fermat prime such that $5 < p < 6673$, that is, $p = 257$. In this case, take $c_1 = 13$ and $c_2 = 197$. Then we have

$$\bigcup_{1 \leq i \leq 4} \mathrm{supp}\Delta X_i = \bigcup_{j \in \mathbb{Z}_4} \{j\} \times L_j,$$

where

$$\begin{aligned} L_0 = &\quad \pm 2 \cdot \{c_1, (c_2+1)(c_1+2), c_2, (c_1+1)(c_2+2)\}, \\ L_1 = &\quad L_3 = \pm 2 \cdot \{1, c_1+1, c_2+1, (c_1+1)(c_2+1)\}, \text{ and} \\ L_2 = &\quad \pm 2 \cdot \{c_1+2, c_1(c_2+1), c_2+2, c_2(c_1+1)\}. \end{aligned}$$

The assumptions on the pair (c_1, c_2) imply that each L_i is of the form $\{1, -1\} \cdot L_i'$, where L_i' is a complete system of representatives for the cosets of C_0^4 in $\mathbb{Z}_p^\times$. Thus, if S is a complete system of representatives for the cosets of $\{1, -1\}$ in C_0^4, we obviously have $L_i \cdot S = \mathbb{Z}_p^\times$ for each i and hence, by Lemma 2.3.6, $\mathcal{F} = \{X_i \cdot (1, s) \,|\, 1 \leq i \leq 4,\ s \in S\}$ is the desired CDF.

By combining Example 2.3.8 and the two constructions above, we immediately get the assertion. □

A computer search has shown that there are no 8-supp $(4p, 4, 4)_2$-CDFs for $p = 3$ and 5.

2.3.4 8-supp $(8p, 8, 4)_2$-CDFs for primes p

Example 2.3.10. The set of the twelve quadruples

$$\begin{aligned} W_h = &\quad (1, h) \cdot \{\pm(0,1), \pm(1,3)\} \quad \text{for } h = 1, 3, 9, \\ X_i = &\quad (1, i) \cdot \{\pm(0,2), \pm(3,1)\} \quad \text{for } i = 1, 3, 9, \\ Y_j = &\quad (1, j) \cdot \{\pm(2,1), \pm(1,6)\} \quad \text{for } j = 1, 3, 9, \\ Z_k = &\quad (1, k) \cdot \{\pm(2,2), \pm(3,5)\} \quad \text{for } k = 1, 3, 9, \end{aligned}$$

over $\mathbb{Z}_8 \times \mathbb{Z}_{13}$ give an 8-supp $(104, 8, 4)_2$-CDF.

Theorem 2.3.11. There exists an 8-supp $(8p, 8, 4)_2$-CDF for every prime $p \equiv 1 \pmod 4$ with $p > 5$.

Proof: Since Example 2.3.10 shows the existence of an 8-supp $(8 \cdot 13, 8, 4)_2$-CDF, we consider the case of $p \geq 17$. Take the following four quadruples over $\mathbb{Z}_8 \times \mathbb{Z}_p$:

$$\begin{aligned} X_1 = &\quad \{\pm(0,1), \pm(1,c)\}, \\ X_2 = &\quad \{\pm(0,c+2), \pm(3,c)\}, \\ X_3 = &\quad \{\pm(2, \tfrac{-c+3}{2}), \pm(1, \tfrac{c+1}{2})\}, \text{ and} \\ X_4 = &\quad \{\pm(2, \tfrac{3c+3}{2}), \pm(3, \tfrac{c+1}{2})\} \end{aligned}$$

such that

$$(c+1, c+2) \in C_1^2 \times C_1^2$$

and

$$(2c, c-1, 3(c-3)) \in C_0^2 \times C_0^2 \times C_0^2,$$

where such an element $c \in \mathbb{Z}_p$ exists for all $p \geq 2579$ by Theorem 1.3.8. The remaining cases of $p \leq 2557$ are completed by computer search and listed in Table 2.2. Note that we have

$$\bigcup_{1 \leq i \leq 4} \mathrm{supp}\Delta X_i = \bigcup_{j \in \mathbb{Z}_8} \{j\} \times L_j,$$

where

$$\begin{aligned} L_0 &= \pm 2 \cdot \{1, c+2\}, \\ L_1 &= L_7 = \pm\{c-1, c+1\}, \\ L_2 &= L_6 = \pm\{2c, c+1\}, \\ L_3 &= L_5 = \pm 2 \cdot \{1, c+1\}, \text{ and} \\ L_4 &= \pm\{c-3, 3(c+1)\}. \end{aligned}$$

The assumptions on c imply that each L_i is of the form $\{1, -1\} \cdot \{\ell_i, \ell_i'\}$ where ℓ_i and ℓ_i' are a square and a non-square of $\mathbb{Z}_p$, respectively. Thus, if S is a complete system of representatives for the cosets of $\{1, -1\}$ in C_0^2, we obviously have $L_i \cdot S = \mathbb{Z}_p^\times$ for each i and hence, by Lemma 2.3.6, $\mathcal{F} = \{X_i \cdot (1, s) \,|\, 1 \leq i \leq 4,\ s \in S\}$ is the desired CDF. □

A computer search has shown that there are no 8-supp $(8 \cdot 5, 8, 4)_2$-CDFs.

Remark 2.3.12. For 8-supp $(8p, 8, 4)_2$-CDFs constructed in this section, we have the following comments:

(i) If there exists an 8-supp $(np, n, 4)_2$-CDF $\mathcal{F}$ for a prime p, then it holds that $p \equiv 1 \pmod{8/\gcd(n, 8)}$. In this section, we completely determined the existence of such difference families in the cases of $n = 1, 2$ and 4. In the case of $n = 8$, we determined the existence of 8-supp $(np, n, 4)_2$-CDFs for $p \equiv 1 \pmod 4$ but not for $p \equiv 3 \pmod 4$.

(ii) The construction in Theorem 2.3.4 is similar to those for radical $(p, 4, 1)$ and $(p, 5, 1)$ difference families given in [17] and revisited in [19].

2.4 Further direct constructions of maximal 8-supp $(np, 4)_2$-CDFs

In this section, we obtain further constructions of maximal 8-supp $(np, 4)_2$-CDFs, whose code length np is not covered by the OOCs constructed in the previous section.

Theorem 2.4.1. If $p = 8t + 5$ is a prime, then there exists a maximal 8-supp $(p, 4)_2$-CDF with t blocks consisting of cosets of the fourth roots of unity in $\mathbb{Z}_p$ if and only if -4 is a primitive fourth power in $\mathbb{Z}_p$.

Table 2.2: An element $c \in \mathbb{Z}_p^\times$ such that $(c+1, c+2) \in C_1^2 \times C_1^2$ and $(2c, c-1, 3(c-3)) \in C_0^2 \times C_0^2 \times C_0^2$ for each prime $p \equiv 1 \pmod 4$, $17 \le p \le 2557$.

p	c	p	c	p	c	p	c	p	c
17	9	421	39	941	10	1481	41	2069	21
29	17	433	27	953	9	1489	12	2081	37
37	13	449	36	977	44	1493	11	2089	61
41	10	457	9	997	43	1549	29	2113	12
53	30	461	10	1009	21	1553	9	2129	81
61	6	509	31	1013	45	1597	13	2137	67
73	9	521	22	1021	6	1601	10	2141	10
89	22	541	37	1033	9	1609	27	2153	9
97	12	557	11	1049	26	1613	37	2161	27
101	10	569	57	1061	59	1621	22	2213	30
109	39	577	12	1069	6	1637	45	2221	38
113	32	593	9	1093	41	1657	9	2237	17
137	50	601	27	1097	9	1669	6	2269	30
149	55	613	13	1109	26	1693	17	2273	9
157	20	617	32	1117	42	1697	60	2281	12
173	61	641	37	1129	50	1709	21	2293	13
181	6	653	20	1153	36	1721	50	2297	38
193	9	661	6	1181	31	1733	37	2309	10
197	11	673	9	1193	22	1741	6	2333	50
229	6	677	26	1201	21	1753	12	2341	6
233	9	701	37	1213	22	1777	9	2357	26
241	50	709	22	1217	9	1789	30	2377	50
257	36	733	43	1229	17	1801	21	2381	32
269	31	757	22	1237	45	1861	6	2389	40
277	31	761	10	1249	27	1873	28	2393	9
281	40	769	20	1277	30	1877	11	2417	9
293	11	773	198	1289	20	1889	10	2437	13
313	19	797	26	1297	9	1901	21	2441	10
317	17	809	20	1301	31	1913	9	2473	28
337	9	821	55	1321	12	1933	31	2477	11
349	6	829	6	1361	10	1949	10	2521	21
353	65	853	37	1373	32	1973	45	2549	107
373	32	857	9	1381	40	1993	9	2557	65
389	21	877	13	1409	46	1997	11		
397	50	881	26	1429	77	2017	66		
401	29	929	149	1433	22	2029	6		
409	54	937	9	1453	65	2053	32		

Proof: The proof is quite similar to that of Theorem 3.7. Let $C_0^{2t+1} = \{\pm 1, \pm c\}$ be the subgroup consisting of fourth roots of unity in $\mathbb{Z}_p^\times$. We have:

$$\mathrm{supp}\Delta C_0^{2t+1} = C_0^{2t+1} \cdot \{c+1, 2\}.$$

So, there exists a maximal 8-supp $(p,4)_2$-CDFs with t blocks which are cosets of C_0^{2t+1} if and only if there exists a t-subset T of $\mathbb{Z}_p^\times$ such that $(\{1, 2/(c+1)\} \cdot T) \cup \{1\}$ is a complete system of representatives for the cosets of C_0^{2t+1} in $\mathbb{Z}_p^\times$. When we write $2/(c+1) = \alpha^x$, where α is a primitive root of $\mathbb{Z}_p$, this is equivalent to that there exists a t-subset Y of $\mathbb{Z}_{2t+1}$ such that $(\{0, x\} + Y) = \mathbb{Z}_{2t+1} \setminus \{0\}$. By Corollary 2.7 in [19] such a subset Y exists if and only if $\gcd(x, 2t+1) = 1$. The assertion then easily follows observing that $-4 = \alpha^{4x}$. □

Explicitly, in the case that -4 is a primitive fourth power, the maximal 8-supp $(p,4)_2$-CDFs given by Theorem 2.4.1 is

$$\mathcal{F} = \{C_0^{2t+1} \cdot 2^i \,|\, 0 \le i \le t-1\}.$$

The assumption of Theorem 2.4.1 is satisfied quite frequently. Indeed, the following are all primes $p < 1000$ such that $p \equiv 5 \,(\mathrm{mod}\ 8)$ not satisfying the condition of Theorem 2.4.1:

$$p = 109, 157, 229, 277, 397, 733, 997. \tag{2.8}$$

Theorem 2.4.2. Let $p = 10t \pm 1$ be a prime such that $(\frac{1+\sqrt{5}}{2})^2$ is a primitive square in $\mathbb{Z}_p$. Then there exists a maximal 8-supp $(p,4)_2$-CDF with $\lfloor p/8 \rfloor$ blocks.

Proof: Observe first that the assumption $p \equiv \pm 1 \,(\mathrm{mod}\ 10)$ assures that 5 is a square in $\mathbb{Z}_p$. Consider $X = \{\pm 1, \pm(2+\sqrt{5})\}$. An easy counting shows that :

$$\mathrm{supp}\Delta X = 2 \cdot \{\pm 1, \pm c, \pm c^2, \pm c^3\}$$

holds, where $c = \frac{1+\sqrt{5}}{2}$. Note that the assumption that c^2 is a primitive square assures that either c or $-c$ is a primitive root of $\mathbb{Z}_p$. It is then clear that $\mathcal{F} = \{X \cdot c^{4i} \,|\, 0 \le i < \lfloor p/8 \rfloor\}$ is the desired CDF. □

The following are all primes $p < 1000$ satisfying $p \not\equiv 1 \,(\mathrm{mod}\ 8)$ and the condition of Theorem 2.4.2:

$$\begin{aligned} p \;=\; & 11, 19, 31, 59, 61, 71, 79, 109, 131, 149, 179, 191, 239, 251, 269, 271, 311, 359, 379, 389, \\ & 419, 431, 439, 479, 491, 499, 571, 599, 631, 659, 701, 719, 739, 751, 821, 839, 971. \end{aligned}$$

Theorem 2.4.3. Let $p = 8t + 7$ be a prime such that $(1+\sqrt{2})^2$ is a primitive square in $\mathbb{Z}_p$. Then there exists a maximal 8-supp $(2p,4)_2$-CDF with $2t+1$ blocks.

Proof: The assumption $p \equiv 7 \,(\mathrm{mod}\ 8)$ assures that 2 is a square in $\mathbb{Z}_p$. Consider

$$X = \{\pm(0,1), \pm(1,c)\} \subset \mathbb{Z}_2 \times \mathbb{Z}_p,$$

where $c = 1 + \sqrt{2}$. Then we have

$$\mathrm{supp}\Delta X = \bigcup_{i \in \mathbb{Z}_2} \{i\} \times L_i,$$

where $L_0 = 2 \cdot \{\pm 1, \pm c\}$ and $L_1 = \sqrt{2} \cdot \{\pm 1, \pm c\}$. Note that c or $-c$ is a primitive root of $\mathbb{Z}_p$. Then, $\mathcal{F} = \{X \cdot (1, c^{2i}) \,|\, 0 \le i \le 2t\}$ is the desired OOC. □

The following are all primes $p < 1000$ satisfying the condition of Theorem 2.4.3:

$$\begin{aligned} p \;=\; & 7, 23, 31, 47, 71, 127, 151, 167, 191, 263, 271, 311, 359, \\ & 367, 383, 431, 439, 463, 479, 503, 631, 647, 719, 727, \\ & 743, 823, 839, 863, 887, 911, 919, 967, 983, 991. \end{aligned}$$

Remark 2.4.4. (i) We do not know whether there are infinitely many primes satisfying the condition of each theorem given in this section. However, the constructed maximal 8-supp $(v,4)_2$-CDFs (optimal $(v,4,2,1)$-OOCs) yield new infinite series of maximal (optimal) ones by applying the recursive construction given in the next section.

(ii) We must mention that some other constructions given in [2], in particular Theorem 2.3 and Construction 4.4 for getting a special $(p, 4, 1, 1)$-OOCs, called "good" OOCs, may be adapted to construct maximal 8-supp $(v, 4)_2$-CDFs and optimal $(v, 4, 2, 1)$-OOCs. In fact, we could construct a maximal 8-supp $(p, 4)_2$-CDF for every prime $p \neq 109$ listed in (2.8) (see Table 2.3). The prime $p = 109$ does not require this kind of construction since it is covered by Theorem 4.2.

Table 2.3: This table shows an optimal $(p, 4, 2, 1)$-OOC for each $p = 157, 229, 277, 397, 733,$ and 997. For primes $p = 157, 277, 397, 733,$ and 997, c is a primitive fourth root of unity in $\mathbb{Z}_p$. For the prime $p = 229$, $c = 82$ is the fourth power of the primitive root 112 in $\mathbb{Z}_p$.

p	c	codewords
157	28	$2^i \cdot \langle c \rangle$, $0 \leq i \leq 2$
		$23 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 1$
		$24 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 5$
		$25 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 5$
		$c^i \cdot \{\pm 66, \pm 67\}$, $i = 0, 1$
229	82	$112^i \cdot 19^j \cdot \{\pm 1 \pm c\}$, $0 \leq i \leq 3$, $0 \leq j \leq 6$
277	217	$2^i \cdot \langle c \rangle$, $0 \leq i \leq 8$
		$53 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 10$
		$54 \cdot \langle c \rangle$
		$55 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 10$
		$c^i \cdot \{\pm 111, \pm 112\}$, $i = 0, 1$
397	63	$2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$17 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$18 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$19 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$49 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$127 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$176 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$225 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$92 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 4$
		$c^i \cdot \{\pm 189, \pm 190\}$, $i = 0, 1$
		$c^i \cdot 49 \cdot \{\pm 180, \pm 181\}$, $i = 0, 1$
733	380	$2^i \cdot \langle c \rangle$, $0 \leq i \leq 1$
		$7 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 29$
		$8 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 26$
		$9 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 29$
		$c^i \cdot \{\pm 362, \pm 363\}$, $i = 0, 1$
997	836	$2^i \cdot \langle c \rangle$, $0 \leq i \leq 37$
		$19 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 40$
		$20 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 1$
		$21 \cdot 2^i \cdot \langle c \rangle$, $0 \leq i \leq 40$
		$c^i \cdot \{\pm 488, \pm 489\}$, $i = 0, 1$

2.5 Compositions of 8-supp $(v,4)_2$-CDFs

In this section, we find a nice connection between 8-supp $(v,4)_2$-CDFs and "cyclic kite-decompositions of a complete multipartite graph." As an immediate consequence, we can derive a recursive construction of 8-supp $(v,4)_2$-CDFs.

Let $K=(a_1,a_2,a_3)$-a_4 be the *kite*, that is, the graph consisting of a triangle (a_1,a_2,a_3) with an attached edge (a_3,a_4). A set $\mathcal{F}$ of kites with vertices in $\mathbb{Z}_{nv}$ is called a *cyclic* $(nv,n,K,1)$ *difference family*, briefly $(nv,n,K,1)$-CDF, if the list $\Delta\mathcal{F}$ of differences from $\mathcal{F}$, namely the list of all possible differences $a-b$, where (a,b) is an ordered pair of adjacent vertices of a kite in $\mathcal{F}$, covers all elements of $\mathbb{Z}_{nv}\setminus v\mathbb{Z}_{nv}$ exactly once, while no element in the subgroup $v\mathbb{Z}_{nv}$. (See [25] for the definition of a (nv,n,Γ,λ) difference family, where Γ is an arbitrary graph and λ is an arbitrary positive integer.) As a special case of general results, any $(nv,n,K,1)$-CDF generates a cyclic kite-decomposition of $K_{n\times v}$, the complete n-partite graph whose parts have size v [25].

Let us say that a kite K with vertices in $\mathbb{Z}_{nv}$ is *good* if, up to translations, it is of the form $(a,a+b,0)$-$(2a+b)$ for suitable elements a and b in $\mathbb{Z}_{nv}$. Analogously, let us say that a $(nv,n,K,1)$-CDF is *good* if all its kites are good.

Lemma 2.5.1. The existence of an 8-supp $(nv,n,4)_2$-CDF $\mathcal{F}$ is equivalent to that of a good $(nv,n,K,1)$-CDF.

Proof: We can assume that each codeword of $\mathcal{F}=\{X_i\,|\,1\le i\le t\}$ has the form $X_i=\{0,a_i,a_i+b_i,2a_i+b_i\}$. Now note that $\mathrm{supp}\Delta X_i$ coincides with the list of differences of the good kite $K_i=(a_i,a_i+b_i,0)$-$(2a_i+b_i)$. This implies that $\mathcal{F}'=\{K_i\,|\,1\le i\le t\}$ is a good $(nv,n,K,1)$-CDF. The converse is also true. □

Now we present a recursive construction for 8-supp $(nv,n,4)_2$-CDFs by applying Theorem 3.2 in [25].

A cyclic $(v,K,1)$ *difference matrix*, briefly $(v,K,1)$-CDM, is a $4\times v$ matrix with entries in $\mathbb{Z}_v$ such that the difference between its ith row and its jth row is a permutation of $\mathbb{Z}_v$ whenever a_i and a_j are adjacent in K. Let us say that a $(v,K,1)$-CDM is *good* if it is of the form

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_v \\ a_1+b_1 & a_2+b_2 & \cdots & a_v+b_v \\ 0 & 0 & \cdots & 0 \\ 2a_1+b_1 & 2a_2+b_2 & \cdots & 2a_v+b_v \end{pmatrix}$$

and observe that if $\gcd(v,6)=1$, then

$$\begin{pmatrix} 1 & 2 & \cdots & v \\ 2\cdot 1 & 2\cdot 2 & \cdots & 2\cdot v \\ 0 & 0 & \cdots & 0 \\ 3\cdot 1 & 3\cdot 2 & \cdots & 3\cdot v \end{pmatrix}$$

certainly is a good $(v,K,1)$-CDM.

As a special case of Theorem 3.2 in [25] we can state:

Theorem 2.5.2. If there exist an $(nu, n, K, 1)$-CDF and a $(v, K, 1)$-CDM, then there exists an $(nuv, nv, K, 1)$-CDF.

Now we observe that if we apply the construction given in the proof of Theorem 3.2 in [25] with the additional assumption that both of the $(nu, n, K, 1)$-CDF and the $(v, K, 1)$-CDM are good, the resultant $(nuv, nv, K, 1)$-CDF is also good. Hence, in view of Lemma 2.5.1 we immediately get the following recursive construction.

Theorem 2.5.3. Assume that there exist:

(i) an 8-supp $(nu, n, 4)_2$-CDF $\mathcal{F}$,

(ii) an 8-supp $(nv, 4)_2$-CDF $\mathcal{F}'$ with $\gcd(v, 6) = 1$.

Then there exists an 8-supp $(nuv, 4)_2$-CDF which is maximal if $\mathcal{F}'$ is maximal. Moreover, if $\mathcal{F}'$ is an 8-supp $(nv, n', 4)_2$-CDF for some n' dividing nv, then the obtained family forms an 8-supp $(nuv, n', 4)_2$-CDF.

Proof: By Lemma 2.5.1, $\mathcal{F}$ can be interpreted as a good $(nu, n, K, 1)$-CDF. Composing this difference family with a good $(v, K, 1)$-CDM (existent in view of the assumption $\gcd(v, 6) = 1$) we get a good $(nuv, nv, K, 1)$-CDF and hence, by Lemma 2.5.1 again, an 8-supp $(nuv, nv, 4)_2$-CDF $\mathcal{F}''$. Now, considering that $\mathbb{Z}_{nv}$ is obviously isomorphic to $u\mathbb{Z}_{nuv}$, let us interpret all codewords of $\mathcal{F}'$ as codewords in $u\mathbb{Z}_{nuv}$ and add them to the codewords of $\mathcal{F}''$. In this way we finally get the desired 8-supp $(nuv, 4)_2$-CDF. □

Applying, recursively, Theorem 2.5.3 to all 8-supp $(nv, n, 4)_2$-CDFs obtained in Section 2.3 and a few small perfect 8-supp $(v, 4)_2$-CDFs given in the following, we immediately get our main results in this chapter with respect to 8-supp $(nv, n, 4)_2$-CDFs.

Example 2.5.4. The following are optimal and perfect 8-supp $(v, 4)_2$-CDFs with $v = 9, 25$, and 49:

$(v = 9)$

$$\mathcal{F} = \{\{\pm 1, \pm 2\}\},$$

$(v = 25)$

$$\mathcal{F} = \{\{\pm 2, \pm 3\}, \{\pm 14, \pm 21\}, \{\pm 17, \pm 19\}\},$$

$(v = 49)$

$$\mathcal{F} = \{\{\pm 1, \pm 28\}, \{\pm 4, \pm 5\}, \{\pm 8, \pm 26\}, \{\pm 3, \pm 22\}, \{\pm 7, \pm 30\}, \{\pm 31, \pm 35\}\}.$$

Corollary 2.5.5. There exists an 8-supp $(nv, n, 4)_2$-CDF if one of the following holds:

(i) $\gcd(n, 6) = 1$ and $v = 9^h 25^i 49^j p_1 p_2 \cdots p_r$ where $h \in \{0, 1\}$, i and j are arbitrary non-negative integers, and each p_i is a prime congruent to 1 modulo 8,

(ii) $n = 2n'$ with $\gcd(n', 6) = 1$ and $v = p_1 p_2 \cdots p_r$ where each p_i is a prime congruent to 1 modulo 4,

(iii) $n = 4n'$ with $\gcd(n', 6) = 1$ and v is any positive integer prime to 30,

(iv) $n = 8n'$ with $\gcd(n', 6) = 1$ and $v = p_1 p_2 \cdots p_r$ where each p_i is a prime $\equiv 1 \pmod 4$ greater than 5.

2.6 New infinite series of optimal $(v, 4, 2, 1)$-OOCs

Now we give further maximal 8-supp $(n, 4)_2$-CDFs.

Example 2.6.1. The following are maximal 8-supp $(n, 4)_2$-CDFs for $n \in \{1, 2, 4, 7, 8, 20, 22, 23, 35, 38\}$:

$(n = 1, 2, 4)$

$$\mathcal{F} = \{\emptyset\},$$

$(n = 7)$

$$\mathcal{F} = \{\{0, 1, 3, 6\}\},$$

$(n = 8)$

$$\mathcal{F} = \{\{0, 1, 3, 4\}\},$$

$(n = 20, 22, 23)$

$$\mathcal{F} = \{\{0, 1, 4, 5\}, \{0, 2, 8, 10\}\},$$

$(n = 35)$

$$\mathcal{F} = \{\{0, 1, 3, 4\}, \{0, 5, 17, 22\}, \{0, 6, 14, 20\}, \{0, 9, 16, 25\}\}$$

$(n = 38)$

$$\mathcal{F} = \{\{0, 1, 3, 4\}, \{0, 5, 14, 19\}, \{0, 7, 15, 22\}, \{0, 11, 17, 28\}\}.$$

By applying Theorem 2.5.3 to the 8-supp $(nv, n, 4)_2$-CDFs given in Corollary 2.5.5 and the maximal 8-supp $(nv, 4)_2$-CDFs given in Section 2.4 and in Example 2.6.1, we obtain the following:

Corollary 2.6.2. There exists an optimal $(nv, 4, 2, 1)$-OOC if one of the following holds:

(i) $n \in \{1, 7, 11, 19, 23, 31, 35, 59, 71, 79, 131, 179, 191, 239, 251, 271, 311, 359, 379, 419, 431, 439, 479, 491, 499, 571, 599, 631, 659, 719, 739, 751, 839, 971\}$ or n is a prime such that $n < 1000$ and $n \equiv 5 \pmod 8$, and $v = 9^h 25^i 49^j p_1 p_2 \cdots p_r$ where $h \in \{0, 1\}$, i, j, and r are any non-negative integers and each p_i is a prime such that $p_i \equiv 1 \pmod 8$,

(ii) $n = 2n'$ where $n' \in \{1, 7, 11, 19, 23, 31, 47, 71, 127, 151, 167, 191, 263, 271, 311, 359, 367, 383, 431, 439, 463, 479, 503, 631, 647, 719, 727, 743, 823, 839, 863, 887, 911, 919, 967, 983, 991\}$ and $v = p_1 p_2 \cdots p_r$ where r is any non-negative integer and each p_i is a prime such that $p_i \equiv 1 \pmod 4$,

(iii) $n \in \{4, 20\}$ and v is any positive integer prime to 30,

(iv) $n = 8$ and $v = p_1 p_2 \cdots p_r$ where each p_i is a prime such that $p_i > 5$ and $p_i \equiv 1 \pmod 4$.

Chapter 3

Cyclic $2(k-1)$-support $(v,k)_{k-1}$ difference families and $(v,k,1)$ conflict-avoiding codes

In this chapter, we deal with perfect $2(k-1)$-supp $(v,k)_{k-1}$-CDFs, which yield maximal $(v,k,1)$-CACs and maximal $(v,k,k-1,1)$-OOCs. Though the auto-correlation property of a $(v,k,k-1,1)$-OOC is high, we can use it as a $(v,k,1)$-CAC since it does not require the auto-correlation property as mentioned in Section 1.4.2 of Chapter 1. We describe our main theorems of this chapter in Section 3.1 and discuss a relation between $2(k-1)$-supp $(v,k)_{k-1}$-CDFs and maximal $(v,k,1)$-CACs in Section 3.2. In Section 3.3, by using the concept of "perfect packings," we give a necessary and sufficient condition for the existence of perfect $2(k-1)$-supp $(p,k)_{k-1}$-CDFs, where p is a prime and $k=3,4$, and 5. And in Section 3.4, a recursive construction of perfect $2(k-1)$-supp $(v,k)_{k-1}$-CDFs is presented. Furthermore, in Section 3.5, we prove that primes p satisfying the necessary and sufficient condition given in Section 3.3 exist infinitely many by investigating the Kronecker density.

3.1 Main theorems in this chapter

In this chapter, we obtain the following theorems:

Theorem 3.1.1. There exists a perfect 4-supp $(v,3)_2$-CDF, which yields a maximal $(v,3,1)$-CAC and a maximal $(v,3,2,1)$-OOC, if and only if every prime divisor p_i of $v=p_1p_2\cdots p_r$ satisfies that $2\in\mathbb{Z}_{p_i}$ is not 2^{ℓ_i}th power, where ℓ_i is the highest power of 2 dividing $\frac{p_i-1}{2}$. And such primes p_i exist infinitely many.

Theorem 3.1.2. There exists a perfect 6-supp $(v,4)_3$-CDF, which yields a maximal $(v,4,1)$-CAC and a maximal $(v,4,3,1)$-OOC, if and only if every prime divisor p_i of $v=p_1p_2\cdots p_r$ satisfies that the multiplicative group of $\mathbb{Z}_{p_i}$ contains a subgroup K of index a power of 3, which itself has a subgroup H of index 3, such that $\{1,2,3\}$ is a complete system of representatives for the cosets of H in K. Such primes p_i exist infinitely many.

Theorem 3.1.3. Let v be a positive integer such that $3 \nmid v$. There exists a perfect 8-supp $(v,5)_4$-CDF, which yields a maximal $(v,5,1)$-CAC and a maximal $(v,5,4,1)$-OOC, if and only if every prime divisor p_i of $v = p_1 p_2 \cdots p_r$ satisfies that the multiplicative group of $\mathbb{Z}_{p_i}$ contains a subgroup K of index a power of 2, which itself has a subgroup H of index 4, such that $-1 \in H$ and $\{1,2,3,4\}$ is a complete system of representatives for the cosets of H in K. Such primes p_i exist infinitely many.

3.2 $(v,k,1)$-CACs from perfect $2(k-1)$-supp $(v,k)_{k-1}$-CDFs

The following lemma completely characterizes all k-subsets X of $\mathbb{Z}_v$ such that $\mu(X) = k-1$.

Lemma 3.2.1. Up to translations, any k-subset X of $\mathbb{Z}_v$ for which $\mu(X) = k-1$ has the form $X = \{i \cdot a \,|\, 0 \le i \le r-1\} \cup \{i \cdot a + t_j \,|\, 1 \le i \le d; 1 \le j \le q\}$ where:

(i) a is an element of $\mathbb{Z}_v$ whose order d does not divide k,

(ii) q and r are quotient and remainder, respectively, of the Euclidean division of k by d,

(iii) $1 \le t_1 < t_2 < \cdots < t_q < v/d$.

Proof: Given a nonzero element a of $\mathbb{Z}_v$ and a k-subset X of $\mathbb{Z}_v$, let G be the circulant oriented graph of order v with connection-set $\{a\}$, namely the oriented graph whose vertices are the elements of $\mathbb{Z}_v$, where (i,j) is an arc if and only if $j = i + a$. Then it is obvious that $m_a(\Delta X)$, the multiplicity of a in ΔX, is the number of arcs of $G[X]$, the oriented subgraph of G induced by X.

Let d be the order of a. We see that G has exactly v/d components each of which is an oriented d-cycle. So, the connected components of $G[X]$ are some (possibly none) oriented d-cycles and some (possibly none) oriented paths. Obviously, every connected component that is a d-cycle contributes to the number of arcs of $G[X]$, namely to $m_a(\Delta X)$, with d. It is also obvious that every connected component that is an r-path contributes to $m_a(\Delta X)$ with $r-1$. Thus we see that $m_a(\Delta X) = k - h$ where h is the number of connected components of $G[X]$ which are paths. Hence, $m_a(\Delta X) = k-1$ holds if and only if exactly one connected component of $G[X]$ is an oriented path. Then, the assertion immediately follows. □

By noting that $d \le k-1$ and $ad = 0$ hold if the graph $G[X]$ contains an oriented d-cycle, we have the following:

Corollary 3.2.2. If $\gcd(v,(k-1)!) = 1$, all k-subsets B of $\mathbb{Z}_v$ for which $\mu(X) = k-1$ are, up to translations, multiples of the set $\{0,1,...,k-1\}$.

Given positive integers v and k, to construct $(v,k,1)$-CACs with a large number of codewords, we mainly use $X = a \cdot \{0,1,2,\ldots,k-1\} \in \binom{\mathbb{Z}_v}{k}$ for some $a \in \mathbb{Z}_n$ as codewords. More precisely, we construct $(v,k,1)$-CACs and $(v,k,k-1,1)$-OOCs with $\frac{v-1}{2(k-1)}$ codewords from $2(k-1)$-supp $(v,k)_{k-1}$-CDFs by noting that $|\mathrm{supp}\Delta X| = 2(k-1)$ for $X = a \cdot \{0,1,...,k-1\}$ if $\gcd(v,(2k-2)!) = 1$ and $\gcd(v,a) = 1$. It seems that the resultant CACs and OOCs are almost maximal. Indeed, for the cases when $k = 3$ and 4, such CACs are maximal by Lemmas 2.2.1 and 2.2.5. Furthermore, similar to Lemma 2.2.1, for $k = 5$ $X \in \binom{\mathbb{Z}_v}{k}$ such

that $|\mathrm{supp}\Delta X| \leq 7$ are, up to translations, completely characterized as: $|\mathrm{supp}\Delta X| = \ell$ if and only if $X = (\frac{v}{\ell+1})\mathbb{Z}_v$, where $4 \leq \ell \leq 7$. Hence, $(v, 5, 1)$-CACs obtained from perfect 8-supp $(v, 5)_4$-CDFs are maximal.

We close this section by giving an easy example of perfect $2(k-1)$-supp $(v, k)_{k-1}$-CDFs as follows.

Example 3.2.3. The single block $B = \{0, 1, \ldots, k-1\}$ is a perfect $2(k-1)$-supp $(2k-1, k)_{k-1}$-CDF for any k, which provides a maximal $(2k-1, k, 1)$-CAC.

3.3 Perfect packings

In this section, we treat the problem whether the multiplicative group of $\mathbb{Z}_p$ for a prime $p = de + 1$ is factorizable into $\{1, 2, \ldots, d\} \cdot S$ for a suitable e-set S. This problem is restated in terms of "perfect packing," which is defined below.

Let G be a finite (additive) group and let X and I be subsets of G. Then the family $\{X+i \,|\, i \in I\}$ is called a *packing of* $\mathrm{dev}\, X$ (*packing of the development of* X) if $(X+i) \cap (X+j) = \emptyset$ for every distinct $i, j \in I$. Furthermore, we say that the packing is *perfect* if $|I| = |G|/|X|$, i.e., $\bigcup_{i \in I} X + i = G$. The concept of a packing was introduced in [19, 20] with an application to constructions of radical difference families. From now on, we put $G = \mathbb{Z}_n$. By Corollary 3.2.2, it is obvious that there exists a $2(k-1)$-supp $(p, k)_{k-1}$-CDF for a prime p if and only if there exists a set $\Gamma \subset \mathbb{Z}_p^\times$ with $|\Gamma| = (p-1)/(2k-2)$ satisfying

$$\pm\Gamma \cup \pm 2\Gamma \cup \cdots \cup \pm(k-1)\Gamma = \mathbb{Z}_p^\times. \tag{3.1}$$

Let α be a primitive root of $\mathbb{Z}_p$ and put $X = \log_\alpha(\{1, 2, \ldots, k-1\})$, where $\log_\alpha$ is the logarithm function from $\mathbb{Z}_p^\times$ to $\mathbb{Z}_{p-1}$. Then, the condition (3.1) is equivalent to that the family $\{X + i \,|\, i \in \log_\alpha(\pm\Gamma)\}$ is a perfect packing of $\mathrm{dev}\, X$ over $\mathbb{Z}_{p-1}$, i.e., $\{X + i \,|\, i \in \log_\alpha(\Gamma)\}$ is also a perfect packing of $\mathrm{dev}\, X$ over $\mathbb{Z}_{\frac{p-1}{2}}$. Hence, we get the following:

Lemma 3.3.1. Let $p \equiv 1 \pmod{2k-2}$ be a prime and α be a primitive root of $\mathbb{Z}_p$. Then, there exists a perfect $2(k-1)$-supp $(p, k)_{k-1}$-CDF if and only if there exists a perfect packing of $\mathrm{dev}(\log_\alpha(\{1, 2, \ldots, k-1\}))$ over $\mathbb{Z}_{\frac{p-1}{2}}$.

In [19], the following theorem was given:

Theorem 3.3.2. (Theorem 2.11 in [19]) Let $X \subset \mathbb{Z}_n$ and let $(d_0 = 1, d_1, \ldots, d_{2t}, d_{2t+1} = n)$ be a chain of divisors such that $\prod_{\ell=0}^{t} \frac{d_{2\ell+1}}{d_{2\ell}} = \frac{n}{|X|}$. Suppose that $\max\{\ell : d_\ell \text{ divides } z\}$ is odd for every $z \in \Delta X$. Then $\{X + i \,|\, i \in I\}$ with

$$I = \{\sum_{\ell=0}^{t} d_{2\ell} i_\ell \,|\, 0 \leq i_\ell < \frac{d_{2\ell+1}}{d_{2\ell}}\}$$

is a perfect packing of $\mathrm{dev}\, X$.

By the above theorem, we immediately have the following:

Corollary 3.3.3. Let $p = 2(k-1)m+1$ be a prime and s be a divisor of m. Then, there exists a perfect $2(k-1)$-supp $(p,k)_{k-1}$-CDF if $\{1,2,...,k-1\}$ is a complete system of representatives for the cosets of the group of $s(k-1)$th powers in C_0^s, the group of sth powers.

Proof: Put $X = \log_\alpha(\{1,2,\ldots,k-1\})$ reducing modulo $(k-1)m$, where α is a primitive root of $\mathbb{Z}_p$, and apply Theorem 3.3.2 with $n = (k-1)m$, $t = 1$, $d_1 = s$, and $d_2 = s(k-1)$. □

Example 3.3.4. The first 10 primes $p \geq 2k-1$ satisfying the condition for $s = 1$ in Corollary 3.3.3 for each $3 \leq k \leq 8$, $k \neq 5$, are:

$$\begin{array}{ll}
(k=3) & 5, 13, 29, 37, 53, 61, 101, 109, 149, 157, \\
(k=4) & 7, 37, 139, 163, 181, 241, 313, 337, 349, 379, \\
(k=6) & 11, 421, 701, 2311, 2861, 3181, 3491, 3931, 4621, 5531, \\
(k=7) & 13, 7477, 7933, 8293, 10837, 12637, 15013, 19237, 22573, 29917, \\
(k=8) & 659, 1429, 2087, 3557, 4663, 9689, 12391, 17431, 20749, 21001.
\end{array}$$

Note that there is no prime p satisfying the condition for $s = 1$ in Corollary 3.3.3 when $k = 5$. (The proof is given in the next section, see Example 3.5.13.) Instead, we provide the first ten primes $p \geq 2k-1$ satisfying the condition for the case $s = 2$ in Corollary 3.3.3 when $k = 5$:

$$(k=5)\ \ 97, 1873, 2161, 3457, 6577, 6673, 6961, 7297, 7873, 10273.$$

Now, we concentrate on the cases when $k = 3, 4$, and 5. In [19], the following were proved:

Theorem 3.3.5. (Corollary 2.7 in [19]) Let $n = 2t$ and let $X = \{0, a\} \subset \mathbb{Z}_n$. Then, there exists a subset $I \subset \mathbb{Z}_n$ such that the family $\{X + i \,|\, i \in I\}$ is a perfect packing of $\operatorname{dev} X$ if and only if $\frac{n}{\gcd(a,n)}$ is even.

Theorem 3.3.6. (Theorem 2.8 in [19]) Let $n = 3t$ and let $X = \{0, a, b\} \subset \mathbb{Z}_n$. Then, there exists a subset $I \subset \mathbb{Z}_n$ such that the family $\{X + i \,|\, i \in I\}$ is a perfect packing of $\operatorname{dev} X$ if and only if there is a power of 3 dividing t, which is the highest power of 3 both dividing a, b, and $a - b$.

By applying Lemma 3.3.1 and Theorems 3.3.5 and 3.3.6, we immediately obtain the following theorems:

Theorem 3.3.7. There exists a perfect 4-supp $(p,3)_2$-CDF for a prime $p \equiv 1 \pmod 4$ if and only if $2 \notin C_0^\ell$ for the highest power ℓ of 2 dividing $\frac{p-1}{2}$.

Theorem 3.3.8. There exists a perfect 6-supp $(p,4)_3$-CDF for a prime $p \equiv 1 \pmod 6$ if and only if the multiplicative group of $\mathbb{Z}_p$ contains a subgroup K of index a power of 3, which itself has a subgroup H of index 3, such that $\{1,2,3\}$ is a complete system of representatives for the cosets of H in K.

Next, we consider the case of $k = 5$. To get our desired result, we use the following.

Lemma 3.3.9. (Remark 2.1 in [19]) Let X and I be subsets defined on $\mathbb{Z}_n$. Then the following are equivalent:

(i) The family $\{X + i \,|\, i \in I\}$ is a perfect packing of $\operatorname{dev} X$,

(ii) The family $\{I + x \,|\, x \in X\}$ is a perfect packing of $\operatorname{dev} I$,

(iii) The family $\{X' + i \,|\, i \in I\}$ is a perfect packing of $\operatorname{dev} X'$, where X' is any subset of $\mathbb{Z}_n$ such that $|X| = |X'|$ and $\Delta X = \Delta X'$.

Lemma 3.3.10. Let $n = 4s$ and let $X = \{0, a, 2a, a + b\} \subset \mathbb{Z}_n$. Then, the following are equivalent:

(i) There exists a subset $I \subset \mathbb{Z}_n$ such that $\{X + i \,|\, i \in I\}$ is a perfect packing of $\operatorname{dev} X$.

(ii) There is a power of 2 dividing s, say 2^{r-2} with $r \geq 2$, such that 2^{r-2} and 2^{r-1} are the highest powers of 2 dividing a and b, respectively.

Proof: ((i) $\Rightarrow$ (ii)) Let $X_0 = X$, $X_1 = \{0, a, 2a, a - b\}$, $X_2 = \{a, b, a + b, 2a + b\}$, and $X_3 = \{0, b, b-a, a+b\}$. Then we have $\Delta X_j = \Delta X$ for every j, and hence each $\{I+x \,|\, x \in X_j\}$, $0 \leq j \leq 3$, is a perfect packing of $\operatorname{dev} I$ over $\mathbb{Z}_n$ by Lemma 3.3.9. Therefore, we have

$$\begin{aligned}
\mathbb{Z}_n &= I \dot\cup (I + a) \dot\cup (I + 2a) \dot\cup (I + a + b) && (3.2)\\
&= I \dot\cup (I + a) \dot\cup (I + 2a) \dot\cup (I + a - b) && (3.3)\\
&= (I + a) \dot\cup (I + b) \dot\cup (I + a + b) \dot\cup (I + 2a + b) && (3.4)\\
&= I \dot\cup (I + b) \dot\cup (I + b - a) \dot\cup (I + a + b). && (3.5)
\end{aligned}$$

By (3.2) and (3.3), we get $I + a + b = I + a - b$, i.e., $I = I + 2b$. Furthermore, by (3.2) and (3.4), we have

$$I \dot\cup (I + 2a) = (I + b) \dot\cup (I + 2a + b),$$

while $I \cap (I + b) = \emptyset$ by (3.5), which implies $I = I + 2a + b$. Let $d = \gcd(2a + b, 2b)$, and then it holds that $I = I + dh$ for any $h \in \mathbb{Z}_n$ since $I = I + 2b = I + 2a + b$. Moreover, it is shown have that $d \nmid a, 2a$ and b by (3.2) and (3.5), but $d \,|\, 2b$ and $d \,|\, 4a = 2(2a + b) - 2b$ by the definition of d. If we write $d = 2^r t$ with $2 \nmid t$, then we consequently get that $2^{r-2} \,|\, a$ but $2^{r-1} \nmid a$ and $2^{r-1} \,|\, b$ but $2^r \nmid b$. Finally, we use Corollary 2.4 of [19] which states that a necessary condition in order that $\operatorname{dev} X$ for $X \subset \mathbb{Z}_n$ admits a perfect packing is that $\frac{n}{|X|}$ is divisible by $\gcd(X, n)$. This implies that s is divisible by $\gcd(a, b, a + b, 4s)$, which follows that 2^{r-2} divides s.

((ii) $\Rightarrow$ (i)) Apply Theorem 3.3.2 with $t = 1$, $d_1 = 2^{r-2}$, and $d_2 = 2^r$. □

For the two elements 2 and 3 of $\mathbb{Z}_p^\times$, we denote $2 = \alpha^a$ and $3 = \alpha^{a+b}$, where α is a primitive root of $\mathbb{Z}_p$. Then we have $\log_\alpha(\{1, 2, 3, 4\}) = \{0, a, 2a, a + b\}$. By applying Lemmas 3.3.1 and 3.3.10, we get the following:

Theorem 3.3.11. There exists a perfect 8-supp $(p, 5)_4$-CDF for a prime $p \equiv 1 \pmod 8$ if and only if the multiplicative group of $\mathbb{Z}_p$ contains a subgroup K of index a power of 2, which itself has a subgroup H of index 4, such that $-1 \in H$ and $\{1, 2, 3, 4\}$ is a complete system of representatives for the cosets of H in K.

3.4 Compositions of perfect $2(k-1)$-supp $(v, k)_{k-1}$-CDFs

Theorem 3.4.1. Let v_1, v_2, and k be positive integers such that $k \geq 3$ and $\gcd(v_2, \ell) = 1$ for every ℓ, $1 \leq \ell \leq k-1$. For each $i = 1, 2$, if there exists a perfect $2(k-1)$-supp $(v_i, k)_{k-1}$-CDF

whose blocks are multiples of $\{0, 1, \ldots, k-1\}$, then there also exists a perfect $2(k-1)$-supp $(v_1v_2, k)_{k-1}$-CDF whose blocks are also multiples of $\{0, 1, \ldots, k-1\}$.

Proof: Let $\mathcal{F}_i = \Gamma_i \cdot \{0, 1, \ldots, k-1\}$, $i = 1, 2$, be the perfect $2(k-1)$-supp $(v_i, k)_{k-1}$-CDFs. Let

$$\Gamma_1' = \{a + bv_1 \,|\, a \in \Gamma_1, 0 \le b \le v_2 - 1\} \text{ and } \Gamma_2' = v_1 \cdot \Gamma_2,$$

where each element is reduced modulo v_1v_2. Then the family $\mathcal{F} = \{a \cdot \{0, 1, \ldots, k-1\} \,|\, a \in \Gamma_1' \cup \Gamma_2'\}$ is the desired perfect $2(k-1)$-supp $(v_1v_2, k)_{k-1}$-CDF. We prove that the lists of differences of any two blocks of $\mathcal{F}$ are disjoint. By the definition of Γ_1, any element of $\pm\{1, 2, \ldots, k-1\} \cdot \Gamma_1'$ is not a multiple of v_1. On the other hand, every element of Γ_2 is a multiple of v_1, which implies that

$$(\pm\{1, 2, \ldots, k-1\} \cdot \Gamma_1') \cap (\pm\{1, 2, \ldots, k-1\} \cdot \Gamma_2') = \emptyset.$$

Since it is obvious that the lists of differences of any two blocks from $\{a \cdot \{0, 1, \ldots, k-1\} \,|\, a \in \Gamma_2'\}$ are disjoint, we only show that the list of differences of any two blocks from $\{a \cdot \{0, 1, \ldots, k-1\} \,|\, a \in \Gamma_1'\}$ are disjoint. Assume $\ell(a + bv_1) \equiv \ell'(a' + b'v_1) \pmod{v_1v_2}$ for some $\ell, \ell' \in \pm\{1, 2, \ldots, k-1\}$ and $a + bv_1, a' + b'v_1 \in \Gamma_1'$, then we need to see that $a = a'$ and $b = b'$. By the above assumption, since $(\ell a - \ell' a') + (\ell b - \ell' b')v_1 \equiv 0 \pmod{v_1v_2}$, we have $\ell a \equiv \ell' a' \pmod{v_1}$. By the definition of $\mathcal{F}_1$, $\ell a \equiv \ell' a' \pmod{v_1}$ if and only if $a = a'$ and $\ell = \ell'$. Therefore, we also have $(\ell b - \ell b')v_1 \equiv 0 \pmod{v_1v_2}$, i.e., $\ell(b - b') \equiv 0 \pmod{v_2}$. Then, the assumption that $\gcd(v_2, \ell) = 1$ for every ℓ, $1 \le \ell \le k-1$, implies $b = b'$. □

By applying Theorem 3.4.1, we get the following:

Corollary 3.4.2. Let v and k be positive integers such that $\gcd(v, (k-1)!) = 1$. Then, the following are equivalent:

(i) There exists a perfect $2(k-1)$-supp $(v, k)_{k-1}$-CDF,

(ii) There exists a perfect $2(k-1)$-supp $(p_i, k)_{k-1}$-CDF for every prime divisor p_i of $v = p_1p_2 \cdots p_r$.

Proof: Note that any block of a perfect $2(k-1)$-supp $(v, k)_{k-1}$-CDF with $\gcd(v, (k-1)!) = 1$ is a multiple of $\{0, 1, \ldots, k-1\}$ by Lemma 3.2.2.

((i) ⇒ (ii)) Let $\mathcal{F}$ be the perfect $2(k-1)$-supp $(v, k)_{k-1}$-CDF. Note that $(\frac{v}{p})\mathbb{Z}_v \setminus \{0\} \simeq \mathbb{Z}_p^\times$ for any prime divisor p of v. For any block $B_a = a \cdot \{0, 1, \ldots, k-1\}$ of $\mathcal{F}$, the set ΔB_a intersects with $(\frac{v}{p})\mathbb{Z}_v \setminus \{0\}$, i.e., $a\ell = (\frac{v}{p})t$ for some $\ell \in \pm\{1, 2, \ldots, k-1\}$ and $t \in \mathbb{Z}_v \setminus \{0\}$ iff $a \in (\frac{v}{p})\mathbb{Z}_v \setminus \{0\}$ since $\gcd(v, (k-1)!) = 1$. In other words, the block B_a lies on $(\frac{v}{p})\mathbb{Z}_v \setminus \{0\}$. This implies that there also exists a perfect $2(k-1)$-supp $(p, k)_{k-1}$-CDF.

((ii) ⇒ (i)) Let $\mathcal{F}_i$ be a perfect $2(k-1)$-supp $(p_i, k)_{k-1}$-CDF for each i, $1 \le i \le r$. By applying Theorem 3.4.1 recursively, and noting $p_i \equiv 1 \pmod{2(k-1)}$ and $\gcd(p_i, (k-1)!) = 1$ for each i, we get the desired perfect $2(k-1)$-supp $(v, k)_{k-1}$-CDF. □

By Theorems 3.3.7, 3.3.8, 3.3.11, and Corollary 3.4.2, we have the following corollaries:

Corollary 3.4.3. There exists a perfect 4-supp $(v, 3)_2$-CDF if and only if every prime divisor p_i of $v = p_1p_2 \cdots p_r$ satisfies the condition of Theorem 3.3.7.

Corollary 3.4.4. There exists a perfect 6-supp $(v,4)_3$-CDF if and only if every prime divisor p_i of $v = p_1p_2\cdots p_r$ satisfies the condition of Theorem 3.3.8.

Corollary 3.4.5. Let v be a positive integer such that $3 \nmid v$. Then, there exists a perfect 8-supp $(v,5)_4$-CDF if and only if every prime divisor p_i of $v = p_1p_2\cdots p_r$ satisfies the condition of Theorem 3.3.11.

3.5 The Kronecker density

In this section, we prove that the set of primes p for which there exist perfect $2(k-1)$-supp $(p,k)_{k-1}$-CDFs is infinite for each of $k = 3, 4$, and 5.

3.5.1 Perfect 4-supp $(p,3)_2$-CDFs

For notations and fundamental facts used in the rest of this chapter, we refer to [61, 64]. Let $\zeta_e = \exp(\frac{2\pi\sqrt{-1}}{e})$ and let $\mathfrak{p}$ be a prime ideal in $\mathbb{Q}(\zeta_e)$ not containing e. Now, define the eth power residue symbol by

$$\left(\frac{\xi}{\mathfrak{p}}\right)_e \equiv \begin{cases} 0 & \text{if } \xi \in \mathfrak{p}, \\ \xi^{\frac{N(\mathfrak{p})-1}{e}} \pmod{\mathfrak{p}} & \text{if } \xi \in \mathbb{Z}[\zeta_e] \setminus \mathfrak{p}, \end{cases}$$

where $N(\mathfrak{p})$ means the norm of $\mathfrak{p}$ in $\mathbb{Q}(\zeta_e)/\mathbb{Q}$. Note that $N(\mathfrak{p}) = p$ if $\mathfrak{p}$ is lying over the principal ideal (p) for a prime $p \equiv 1 \pmod{e}$. By this notation, the condition of Theorem 3.3.7 can be immediately reformulated as follows:

Lemma 3.5.1. Let $p \equiv 1 \pmod{2\ell}$ be a rational prime and put $\ell = 2^r$, $r \geq 1$. Then the condition of Theorem 3.3.7 is equivalent to

$$\left(\frac{2}{\mathfrak{p}'}\right)_\ell \neq 1 \text{ and } \left(\frac{-1}{\mathfrak{p}}\right)_{2\ell} = -1, \tag{3.6}$$

where $\mathfrak{p}' \in \mathbb{Q}(\zeta_\ell)$ is a prime ideal lying over (p) and $\mathfrak{p} \in \mathbb{Q}(\zeta_{2\ell})$ is that lying over $\mathfrak{p}'$.

By utilizing the quadratic and quartic reciprocity laws and their supplementary laws, we can completely characterize prime p's admitting the condition for the cases of $r = 1$ and 2 in Lemma 3.5.1.

Example 3.5.2. (i) In the case of $r = 1$, the condition that $p \equiv 1 \pmod 4$ and $\left(\frac{-1}{\mathfrak{p}}\right)_4 = -1$ are equivalent to $p \equiv 5 \pmod 8$. Then, by the supplementary law of quadratic reciprocity [61], that is $\left(\frac{2}{p}\right)_2 \equiv (-1)^{\frac{p^2-1}{8}}$ for an odd prime p, the condition (3.6) is equivalent to $p \equiv 5 \pmod 8$.

(ii) In the case of $r = 2$, the condition that $p \equiv 1 \pmod 8$ and $\left(\frac{-1}{\mathfrak{p}}\right)_8 = -1$ are equivalent to $p \equiv 9 \pmod{16}$. Then, by the supplementary law of quartic reciprocity [61], that is $\left(\frac{2}{(\pi)}\right)_4 \equiv \zeta_4^{\frac{3b}{2}}$ for an integer $\pi = a + b\zeta_4 \in \mathbb{Q}(\zeta_4)$ such that $\pi \equiv 1 \pmod{(1-\zeta_4)^3}$, the condition (3.6) is equivalent to $a \equiv 5 \pmod 8$ and $b \equiv 4 \pmod 8$ for a prime $p = (a + b\zeta_4)(a - b\zeta_4)$.

It seems to be difficult to explicitly characterize primes satisfying the condition of Lemma 3.5.1 for every case of $r > 2$. However, we can show that there are infinitely many such primes for each r and it is possible to estimate the density of those primes $\{p\}$ by calculating the Kronecker density.

Let K be a Galois extension of an algebraic number field F and C be the conjugate class of $\sigma \in G = \mathrm{Gal}(K/F)$, i.e., $C = \{\gamma^{-1}\sigma\gamma \,|\, \gamma \in G\}$. We define a set M_σ of prime ideals in F for a fixed $\sigma \in G$ as follows:

$$M_\sigma = \{\mathfrak{P} \cap F \,|\, \mathfrak{P} \text{ is a prime ideal in } K \text{ such that } \sigma_{\mathfrak{P}} \in C\},$$

where $\sigma_{\mathfrak{P}}$ is a Frobenius substitution with respect to $\mathfrak{P}$ in K/F. The following theorem is well known as Chebotarëv's density theorem [101].

Theorem 3.5.3. The Kronecker density $\delta(M_\sigma)$ of M_σ is equal to $\frac{|C|}{|G|}$, i.e.,

$$\delta(M_\sigma) = \lim_{s \to 1+0} \sum_{\mathfrak{p} \in M_\sigma} \frac{1}{N(\mathfrak{p})^s} / \log \frac{1}{s-1} = \frac{|C|}{|G|}.$$

Especially, if K/F is an abelian extension, there exist infinitely many prime ideals $\mathfrak{p}$ in F such that $\left(\frac{K/F}{\mathfrak{p}}\right) = \sigma$ for each $\sigma \in \mathrm{Gal}(K/F)$, and the Kronecker density of the set of such prime ideals is equal to $\frac{1}{[K:F]}$, where $\left(\frac{K/F}{\mathfrak{p}}\right)$ is the Artin symbol.

Lemma 3.5.4. The degree of the extension $\mathbb{Q}(\zeta_{2^{r_2}}, \sqrt[2^{r_1}]{2})/\mathbb{Q}(\zeta_{2^{r_2}})$ with $1 \leq r_1 \leq r_2$ and $3 \leq r_2$ is equal to 2^{r_1-1}.

Proof: Let $\theta = \sqrt[2^{r_1}]{2}$. Since the extension is cyclic, we can assume

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{2^{r_2}}, \theta)/\mathbb{Q}(\zeta_{2^{r_2}})) = \langle\sigma\rangle \text{ and } \sigma^{2^d} = 1,$$

where $\sigma = (\theta \to \zeta\theta)$, and $\zeta\theta$ is a relative conjugate of θ. Then, since

$$\theta = (\theta)^{\sigma^{2^d}} = \zeta^{2^d}\theta,$$

we have $\zeta^{2^d} = 1$, i.e., $\zeta = \zeta_{2^d}$. Therefore, we also have

$$(\theta^{2^d})^\sigma = (\zeta\theta)^{2^d} = \zeta^{2^d}\theta^{2^d} = \theta^{2^d},$$

i.e., θ^{2^d} is invariant under σ. This implies that $\theta^{2^d} = \sqrt[2^{r_1-d}]{2} \in \mathbb{Q}(\zeta_{2^{r_2}})$. On the other hand, it is obvious that $\sqrt[2^{r_1-d}]{2} \in \mathbb{Q}(\zeta_{2^{r_2}})$ for $r_2 \geq 3$ if and only if $r_1 - d = 1$. Hence, we have $d = r_1 - 1$, i.e., the extension degree is 2^{r_1-1}. □

Now we prove our main theorem by noting the equivalence of the following (i), (ii), and (iii):

(i) A rational prime p which is relatively prime to an integer e splits completely in $\mathbb{Q}(\zeta_e)$,

(ii) A Frobenius substitution σ_p with respect to p in $\mathbb{Q}(\zeta_e)/\mathbb{Q}$ is identical,

(iii) $p \equiv 1 \pmod{e}$.

Furthermore, note that

$$\left(\frac{\alpha}{\mathfrak{p}}\right)_e = 1 \text{ iff } \left(\frac{\mathbb{Q}(\zeta_e, \sqrt[e]{\alpha})/\mathbb{Q}(\zeta_e)}{\mathfrak{p}}\right) = 1. \tag{3.7}$$

Theorem 3.5.5. The Kronecker density of the set of all prime p's such that there exists a perfect 4-supp $(p,3)_2$-CDF is equal to $\frac{5}{12}$, and there exist infinitely many such primes.

Proof: We investigate the Kronecker density D_r of the set of primes satisfying the condition (3.6) of Lemma 3.5.1. In the case of $r = 1$, by Example 3.5.2 (i), the density D_1 of rational prime p's satisfying (3.6) is obviously equal to $\frac{1}{4}$. Therefore, we consider the case $r \geq 2$. Let $\mathfrak{P}$ be a prime ideal in $\mathbb{Q}(\zeta_{2\ell})$ lying over (p) and let

$$\sigma = \left(\frac{\mathbb{Q}(\zeta_{4\ell}, \sqrt[\ell]{2})/\mathbb{Q}(\zeta_{2\ell})}{\mathfrak{P}} \right). \tag{3.8}$$

Then, by (3.7), a necessary and sufficient condition for (3.5.7) is

$$\sigma(\zeta_{4\ell}) = -\zeta_{4\ell} \text{ and } \sigma(\sqrt[\ell]{2}) \neq \sqrt[\ell]{2}. \tag{3.9}$$

Since

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{4\ell}, \sqrt[\ell]{2})/\mathbb{Q}(\zeta_{2\ell})) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{4\ell}, \sqrt[\ell]{2})/\mathbb{Q}(\zeta_{2\ell}, \sqrt[\ell]{2})) \times \mathrm{Gal}(\mathbb{Q}(\zeta_{2\ell}, \sqrt[\ell]{2})/\mathbb{Q}(\zeta_{2\ell}))$$

is abelian, by Lemma 3.5.4, the density A_r of $\{\mathfrak{P}\}$ in $\mathbb{Q}(\zeta_{2\ell})$ satisfying (3.9) is equal to

$$A_r = \frac{[\mathbb{Q}(\zeta_{4\ell}, \sqrt[\ell]{2}) : \mathbb{Q}(\zeta_{2\ell}, \sqrt[\ell]{2})] - 1}{[\mathbb{Q}(\zeta_{4\ell}, \sqrt[\ell]{2}) : \mathbb{Q}(\zeta_{2\ell}, \sqrt[\ell]{2})]} \cdot \frac{[\mathbb{Q}(\zeta_{2\ell}, \sqrt[\ell]{2}) : \mathbb{Q}(\zeta_{2\ell})] - 1}{[\mathbb{Q}(\zeta_{2\ell}, \sqrt[\ell]{2}) : \mathbb{Q}(\zeta_{2\ell})]} = \frac{1}{2} \cdot \frac{2^{r-1} - 1}{2^{r-1}} = \frac{2^{r-1} - 1}{2^r}.$$

Then, it is enough to consider only rational primes which split completely in $\mathbb{Q}(\zeta_{2\ell})$. Hence, the Kronecker density D_r, $r \geq 2$, of the set of such primes is equal to

$$D_r = A_r \cdot \frac{1}{[\mathbb{Q}(\zeta_{2\ell}) : \mathbb{Q}]} = \frac{2^{r-1} - 1}{2^{2r}}.$$

Therefore, the Kronecker density of the set of such primes for all r is in total

$$\sum_{1 \leq r \leq r'} D_r = \frac{1}{4} + \sum_{2 \leq r \leq r'} \frac{2^{r-1} - 1}{2^{2r}} \longrightarrow \frac{5}{12} \quad (\text{as } r' \to \infty),$$

which completes the proof. □

Remark 3.5.6. By Theorem 3.5.5, there exist infinitely many primes satisfying the condition of Lemma 3.5.1 for each $r \geq 2$, and the Kronecker density of those primes is equal to $\frac{2^{r-1}-1}{2^{2r}}$.

3.5.2 Perfect 6-supp $(p,4)_3$-CDFs

The condition of Theorem 3.3.8 can be reformulated as follows:

Lemma 3.5.7. Let $p = 2\ell m + 1$ be a prime, where $\ell = 3^{r'}$, $r' \geq 1$, and $3 \nmid m$. Then, the following are equivalent:

(i) There exists a perfect 6-supp $(p,4)_3$-CDF,

(ii) There exists an integer $r \leq r'$ such that

$$\left(\frac{2}{\mathfrak{p}}\right)_{3^r} = \zeta_3 (= \zeta_{3^r}^{3^{r-1}}) \text{ and } \left(\frac{3}{\mathfrak{p}}\right)_{3^r} = \zeta_3^2 (= \zeta_{3^r}^{2\cdot 3^{r-1}}),$$

or

$$\left(\frac{2}{\mathfrak{p}}\right)_{3^r} = \zeta_3^2 \text{ and } \left(\frac{3}{\mathfrak{p}}\right)_{3^r} = \zeta_3,$$

where $\mathfrak{p} \in \mathbb{Q}(\zeta_{3^r})$ is a prime ideal lying over (p).

(iii) There exists an integer $r \leq r'$ such that

$$\left(\frac{2}{\mathfrak{p}'}\right)_{3^{r-1}} = 1, \left(\frac{6}{\mathfrak{p}}\right)_{3^r} = 1, \text{ and } \left(\frac{2}{\mathfrak{p}}\right)_{3^r} \neq 1, \tag{3.10}$$

where $\mathfrak{p}' \in \mathbb{Q}(\zeta_{3^{r-1}})$ is a prime ideal lying over (p) and $\mathfrak{p} \in \mathbb{Q}(\zeta_{3^r})$ is a prime ideal lying over $\mathfrak{p}'$.

By the cubic reciprocity law and its supplementary law, we can completely characterize prime p's satisfying the condition for the case of $r = 1$ in Lemma 3.5.7.

Example 3.5.8. (Corollary 3.4 of [88]) For the case of $r = 1$ in Lemma 3.5.7, we apply the cubic reciprocity law and its supplementary law [61, 64]. The cubic reciprocity law implies that for a rational integer i prime to 3 and an integer $\pi \in \mathbb{Q}(\zeta_3)$ prime to i and 3 if π is congruent to a rational integer modulo $(1-\zeta_3)^2$, then it holds that

$$\left(\frac{i}{(\pi)}\right)_3 = \left(\frac{\pi}{(i)}\right)_3. \tag{3.11}$$

The supplementary law of cubic reciprocity implies that for an integer $\pi = a + b\zeta_3 \in \mathbb{Q}(\zeta_3)$ prime to 3 if π is congruent to a rational integer modulo 3, then it holds that

$$\left(\frac{3}{(\pi)}\right)_3 = \zeta_3^{\frac{ab}{3}}. \tag{3.12}$$

For a rational prime $p \equiv 1 \pmod 6$, without loss of generality, we can assume that $a \equiv 2 \pmod 3$ and $b \equiv 0 \pmod 3$ for a prime element $\pi = a + b\zeta_3 \in \mathbb{Q}(\zeta_3)$ such that $p = (a+b\zeta_3)(a+\zeta_3^2)$. Then, π satisfies the assumption of the cubic reciprocity law and its supplementary law. Hence, by (3.11), we have

$$\left(\frac{2}{(\pi)}\right)_3 = \left(\frac{\pi}{(2)}\right)_3 = (a+b\zeta_3)^{\frac{N(2)-1}{3}} = a + b\zeta_3 \pmod 2. \tag{3.13}$$

Therefore, by (3.12) and (3.13), the condition for the case of $r = 1$ in Lemma 3.5.7 can be reformulated as

$$\begin{cases} a \equiv 2 \pmod 6, \\ b \equiv 3 \pmod{18}, \end{cases} \text{ or } \begin{cases} a \equiv 5 \pmod 6, \\ b \equiv 15 \pmod{18}, \end{cases}$$

for a prime element $\pi = a + b\zeta_3 \in \mathbb{Q}(\zeta_3)$ such that $p = (a+b\zeta_3)(a+b\zeta_3^2)$.

Similar to the cases of $k = 3$, we can show that there are infinitely many primes satisfying the condition of Lemma 3.5.7 for each $r \geq 1$ and it is possible to estimate the density of those primes $\{p\}$ by calculating the Kronecker density. To get our main theorem, we need the following lemma.

Lemma 3.5.9. The degree of the extension $\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}, \sqrt[3^{r_2}]{3})/\mathbb{Q}(\zeta_{3^r})$ for $1 \leq r_1, r_2 \leq r$ is equal to $3^{r_1+r_2}$.

Proof: Since the extensions $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[3]{3})/\mathbb{Q}$ are not normal, by the Galois theory, we have $\mathbb{Q}(\sqrt[3]{2}) \not\subset \mathbb{Q}(\zeta_{3^r})$ and $\mathbb{Q}(\sqrt[3]{3}) \not\subset \mathbb{Q}(\zeta_{3^r})$, i.e., 2 and 3 are not cubes in $\mathbb{Q}(\zeta_{3^r})$. Then, by the Kummer theory, we have

$$[\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}) : \mathbb{Q}(\zeta_{3^r})] = 3^{r_1} \text{ and } [\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_2}]{3}) : \mathbb{Q}(\zeta_{3^r})] = 3^{r_2}.$$

Next, we prove $K := \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}) \cap \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_2}]{3}) = \mathbb{Q}(\zeta_{3^r})$. Let $\theta_1 = \sqrt[3^{r_1}]{2}$. Since the extension $\mathbb{Q}(\zeta_{3^r}, \theta_1)/K$ is cyclic, we can assume

$$\mathrm{Gal}(\mathbb{Q}(\zeta_{3^r}, \theta_1)/K) = \langle \sigma \rangle \text{ and } \sigma^{3^{d_1}} = 1,$$

where $\sigma = (\theta_1 \to \zeta\theta_1)$, and $\zeta\theta_1$ is a relative conjugate of θ_1. Then, since

$$\theta_1 = (\theta_1)^{\sigma^{3^{d_1}}} = \zeta^{3^{d_1}}\theta_1,$$

we have $\zeta^{3^{d_1}} = 1$. Therefore, we also have

$$(\theta^{3^{d_1}})^{\sigma} = (\zeta\theta_1)^{3^{d_1}} = \zeta^{3^{d_1}}\theta_1^{3^{d_1}} = \theta_1^{3^{d_1}},$$

i.e., $\theta_1^{3^{d_1}}$ is invariant under σ. This implies that $\theta_1^{3^{d_1}} = \sqrt[3^{r_1-d_1}]{2} \in K$. Similarly, by putting $\theta_2 = \sqrt[3^{r_2}]{3}$ and $[\mathbb{Q}(\zeta_{3^r}, \theta_2) : K] = 3^{d_2}$, we have $\sqrt[3^{r_2-d_2}]{3} \in K$. Therefore, it follows that

$$K = \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1-d_1}]{2}) = \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_2-d_2}]{3}),$$

where $r_1 - d_1 = r_2 - d_2$. On the other hand, $\sqrt[3^{r_2-d_2}]{3} \in \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1-d_1}]{2})$ holds iff $r_1 - d_1 = 0$. Hence, we get $K = \mathbb{Q}(\zeta_{3^r})$ and

$$\begin{aligned}
& [\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}, \sqrt[3^{r_2}]{3}) : \mathbb{Q}(\zeta_{3^r})] \\
= \; & [\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}, \sqrt[3^{r_2}]{3}) : \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}) \cap \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_2}]{3})] \\
= \; & [\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}, \sqrt[3^{r_2}]{3}) : \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2})] \cdot [\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}, \sqrt[3^{r_2}]{3}) : \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_2}]{3})] \\
= \; & [\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_1}]{2}) : \mathbb{Q}(\zeta_{3^r})] \cdot [\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r_2}]{3}) : \mathbb{Q}(\zeta_{3^r})] = 3^{r_1+r_2},
\end{aligned}$$

which is the desired assertion. □

Theorem 3.5.10. The Kronecker density of the set of all prime p's such that there exists a perfect 6-supp $(p, 4)_3$-CDF is equal to $\frac{3}{26}$, and there exist infinitely many such primes.

Proof: We investigate the Kronecker density D_r of the set of primes satisfying the condition (3.10) of Lemma 3.5.7. Let $\mathfrak{p} \in \mathbb{Q}(\zeta_{3^r})$ be a prime ideal lying over (p) and $\mathfrak{P} \in \mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r-1}]{2}, \sqrt[3^r]{6})$ be a prime ideal lying over $\mathfrak{p}$, and let

$$\tau = \left(\frac{\mathbb{Q}(\zeta_{3^r}, \sqrt[3^{r-1}]{2}, \sqrt[3^r]{6})/\mathbb{Q}(\zeta_{3^r})}{\mathfrak{p}} \right)$$

and

$$\sigma = \left(\frac{\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^r]{2},\ \sqrt[3^r]{6})/\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^{r-1}]{2},\ \sqrt[3^r]{6})}{\mathfrak{P}} \right).$$

Then, by (3.7), the condition (3.10) can be reformulated as

$$\tau(\sqrt[3^{r-1}]{2}) = \sqrt[3^{r-1}]{2},\ \tau(\sqrt[3^r]{6}) = \sqrt[3^r]{6},\ \text{and}\ \sigma(\sqrt[3^r]{2}) \neq \sqrt[3^r]{2}. \tag{3.14}$$

Since the extensions $\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^{r-1}]{2},\ \sqrt[3^r]{6})/\mathbb{Q}(\zeta_{3^r})$ and $\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^r]{2},\ \sqrt[3^r]{6})/\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^{r-1}]{2},\ \sqrt[3^r]{6})$ are abelian, by Theorem 3.5.3, it is enough to calculate the degrees of the extensions. By noting that $\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^s]{2},\ \sqrt[3^s]{3}) = \mathbb{Q}(\zeta_{3^r},\ \sqrt[3^s]{2},\ \sqrt[3^s]{6})$ for any s and using Lemma 3.5.9, the density A_r of $\{\mathfrak{p}\}$ in $\mathbb{Q}(\zeta_{3^r})$ satisfying (3.14) is equal to

$$\frac{[\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^r]{2},\ \sqrt[3^r]{6}) : \mathbb{Q}(\zeta_{3^r},\ \sqrt[3^{r-1}]{2},\ \sqrt[3^r]{6})] - 1}{[\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^r]{2},\ \sqrt[3^r]{6}) : \mathbb{Q}(\zeta_{3^r},\ \sqrt[3^{r-1}]{2},\ \sqrt[3^r]{6})]} \cdot \frac{1}{[\mathbb{Q}(\zeta_{3^r},\ \sqrt[3^{r-1}]{2},\ \sqrt[3^r]{6}) : \mathbb{Q}(\zeta_{3^r})]} = \frac{2}{3^{2r}}.$$

Then, it is enough to consider only rational primes which split completely in $\mathbb{Q}(\zeta_{3^r})$. Hence, the Kronecker density D_r of the set of such primes is equal to

$$D_r = A_r \cdot \frac{1}{[\mathbb{Q}(\zeta_{3^r}) : \mathbb{Q}]} = \frac{1}{3^{3r-1}}. \tag{3.15}$$

Therefore, the Kronecker density of the set of such primes for all r is in total

$$\sum_{1 \leq r \leq r'} D_r = \sum_{1 \leq r \leq r'} \frac{1}{3^{3r-1}} \longrightarrow \frac{3}{26} \ \ (\text{as } r' \to \infty),$$

which completes the proof. □

Remark 3.5.11. By Theorem 3.5.3 and (3.15), there exist infinitely many primes satisfying the condition of Lemma 3.5.7 for each r, and the Kronecker density of those primes is equal to $\frac{1}{3^{3r-1}}$.

3.5.3 Perfect 8-supp $(p, 5)_4$-CDFs

The condition of Theorem 3.3.11 can be reformulated as follows:

Lemma 3.5.12. Let $p = 2\ell m + 1$ be a prime, where $\ell = 2^{r'}$, $r' \geq 2$, and $2 \nmid m$. Then, the following are equivalent:

(i) There exists a perfect 8-supp $(p, 5)_4$-CDF,

(ii) There exists an integer $r \leq r'$ such that

$$\left(\frac{-1}{\mathfrak{p}}\right)_{2^r} = 1,\ \left(\frac{2}{\mathfrak{p}}\right)_{2^r} = \zeta_4 \text{ and } \left(\frac{3}{\mathfrak{p}}\right)_{2^r} = \zeta_4^3,$$

or

$$\left(\frac{-1}{\mathfrak{p}}\right)_{2^r} = 1,\ \left(\frac{2}{\mathfrak{p}}\right)_{2^r} = \zeta_4^3 \text{ and } \left(\frac{3}{\mathfrak{p}}\right)_{2^r} = \zeta_4,$$

where $\mathfrak{p} \in \mathbb{Q}(\zeta_{2^r})$ is a prime ideal lying over (p),

(iii) There exists an integer $r \leq r'$ such that

$$\left(\frac{-1}{\mathfrak{p}}\right)_{2^r} = 1, \left(\frac{2}{\mathfrak{p}''}\right)_{2^{r-2}} = 1, \left(\frac{6}{\mathfrak{p}}\right)_{2^r} = 1, \text{ and } \left(\frac{2}{\mathfrak{p}'}\right)_{2^{r-1}} \neq 1, \tag{3.16}$$

where $\mathfrak{p}'' \in \mathbb{Q}(\zeta_{2^{r-2}})$, $\mathfrak{p}' \in \mathbb{Q}(\zeta_{2^{r-1}})$, and $\mathfrak{p} \in \mathbb{Q}(\zeta_{2^r})$ are prime ideals lying over (p), $\mathfrak{p}''$, and $\mathfrak{p}'$, respectively.

By applying the supplementary law of the quadratic reciprocity, we can show that there are no primes p satisfying the condition for the case of $r = 2$ in Lemma 3.5.12.

Example 3.5.13. In (3.16), the condition $\left(\frac{-1}{\mathfrak{p}}\right)_{2^2} = 1$ is equivalent to $p \equiv 1 \pmod 8$. On the other hand, by the supplementary law of the quadratic reciprocity, $\left(\frac{2}{p}\right)_2 = 1$ for any prime $p \equiv 1 \pmod 8$. Hence, there are no primes satisfying the condition (3.16) for the case of $r = 2$ in Lemma 3.5.12.

Lemma 3.5.14. The degree of the extension $\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2}, \sqrt[2^{r_2}]{3})/\mathbb{Q}(\zeta_{2^r})$ for $1 \leq r_1, r_2 \leq r$ and $r \geq 3$ is equal to $2^{r_1+r_2-1}$.

Proof: It is well known that $\mathbb{Q}(\sqrt{m}) \subset \mathbb{Q}(\zeta_N)$ for a rational square-free integer m iff $M \mid N$, where

$$M = \begin{cases} |m| & \text{if } m \equiv 1 \pmod 4, \\ 4|m| & \text{if } m \equiv 2, 3 \pmod 4. \end{cases}$$

Hence, we have that $\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\zeta_{2^r})$ for every $r \geq 3$ and $\mathbb{Q}(\sqrt{3}) \not\subset \mathbb{Q}(\zeta_{2^r})$ for any r. Furthermore, the extensions $\mathbb{Q}(\sqrt[2^i]{2})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt[2^i]{3})/\mathbb{Q}$ are not normal when $i \geq 2$, by the Kummer theory, we have

$$[\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2}) : \mathbb{Q}(\zeta_{2^r})] = 2^{r_1-1} \text{ and } [\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_2}]{3}) : \mathbb{Q}(\zeta_{2^r})] = 2^{r_2}.$$

Similar to the proof of Lemma 3.5.9, when we put $\theta_1 = \sqrt[2^{r_1}]{2}$, $\theta_2 = \sqrt[2^{r_2}]{3}$, and $K = \mathbb{Q}(\zeta_{2^r}, \theta_1) \cap \mathbb{Q}(\zeta_{2^r}, \theta_2)$, we have

$$K = \mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1-d_1}]{2}) = \mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_2-d_2}]{3}),$$

where $2^{d_1} = [\mathbb{Q}(\zeta_{2^r}, \theta_1) : K]$, $2^{d_2} = [\mathbb{Q}(\zeta_{2^r}, \theta_2) : K]$, and $r_1 - d_1 - 1 = r_2 - d_2$. On the other hand, $\sqrt[2^{r_1-d_1}]{2} \in \mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_2-d_2}]{3})$ holds iff $r_1 - d_1 = 1$ and $\sqrt[2^{r_1-d_1}]{2} \in \mathbb{Q}(\zeta_{2^r})$. Hence, we get $K = \mathbb{Q}(\zeta_{2^r})$ and

$$\begin{aligned} & [\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2}, \sqrt[2^{r_2}]{3}) : \mathbb{Q}(\zeta_{2^r})] \\ = \; & [\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2}, \sqrt[2^{r_2}]{3}) : \mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2}) \cap \mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_2}]{3})] \\ = \; & [\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2}, \sqrt[2^{r_2}]{3}) : \mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2})] \cdot [\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2}, \sqrt[2^{r_2}]{3}) : \mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_2}]{3})] \\ = \; & [\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_1}]{2}) : \mathbb{Q}(\zeta_{2^r})] \cdot [\mathbb{Q}(\zeta_{2^r}, \sqrt[2^{r_2}]{3}) : \mathbb{Q}(\zeta_{2^r})] = 2^{r_1+r_2-1}, \end{aligned}$$

which is the desired assertion. □

Theorem 3.5.15. The Kronecker density of the set of all prime p's such that there exists a perfect 8-supp $(p, 5)_4$-CDF is equal to $\frac{1}{112}$, and there exist infinitely many such primes.

Proof: We investigate the Kronecker density D_r of the set of primes satisfying the condition (3.16) of Lemma 3.5.12. Since $D_2 = 0$ by Example 3.5.13, we consider the case when $r \geq 3$. Let $\mathfrak{p} \in \mathbb{Q}(\zeta_{2^r})$ be a prime ideal lying over (p) and $\mathfrak{P} \in \mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-1}]{2}, \sqrt[2^r]{6})$ be a prime ideal lying over $\mathfrak{p}$, and let

$$\tau = \left(\frac{\mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-2}]{2}, \sqrt[2^r]{6})/\mathbb{Q}(\zeta_{2^r})}{\mathfrak{p}} \right)$$

and

$$\sigma = \left(\frac{\mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-1}]{2}, \sqrt[2^r]{6})/\mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-2}]{2}, \sqrt[2^r]{6})}{\mathfrak{P}} \right).$$

Then, by (3.7), the condition (3.10) can be reformulated as

$$\tau(\zeta_{2^{r+1}}) = \zeta_{2^{r+1}},\ \tau(\sqrt[2^{r-2}]{2}) = \sqrt[2^{r-2}]{2},\ \tau(\sqrt[2^r]{6}) = \sqrt[2^r]{6},\ \text{and}\ \sigma(\sqrt[2^{r-1}]{2}) \neq \sqrt[2^{r-1}]{2}. \tag{3.17}$$

By noting that $\mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^s]{2}, \sqrt[2^s]{3}) = \mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^s]{2}, \sqrt[2^s]{6})$ for any s and using Lemma 3.5.14, the density A_r, $r \geq 3$, of $\{\mathfrak{p}\}$ in $\mathbb{Q}(\zeta_{2^r})$ satisfying (3.17) is equal to

$$\frac{[\mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-1}]{2}, \sqrt[2^r]{6}) : \mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-2}]{2}, \sqrt[2^r]{6})] - 1}{[\mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-1}]{2}, \sqrt[2^r]{6}) : \mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-2}]{2}, \sqrt[2^r]{6})]} \cdot \frac{1}{[\mathbb{Q}(\zeta_{2^{r+1}}, \sqrt[2^{r-2}]{2}, \sqrt[2^r]{6}) : \mathbb{Q}(\zeta_{2^r})]} = \frac{1}{2^{2r-1}}.$$

Then, it is enough to consider only rational primes which split completely in $\mathbb{Q}(\zeta_{2^r})$. Hence, the Kronecker density D_r, $r \geq 3$, of the set of such primes is equal to

$$D_r = A_r \cdot \frac{1}{[\mathbb{Q}(\zeta_{2^r}) : \mathbb{Q}]} = \frac{1}{2^{3r-2}}. \tag{3.18}$$

Therefore, the Kronecker density of the set of such primes for all $r \geq 3$ is in total

$$\sum_{1 \leq r \leq r'} D_r = \sum_{3 \leq r \leq r'} \frac{1}{2^{3r-2}} \longrightarrow \frac{1}{112} \quad (\text{as } r' \to \infty),$$

which completes the proof. □

Remark 3.5.16. In the above proof, we treated the case of $r = 2$ as an exception. But, it is easy to see $A_2 = 0$ since $[\mathbb{Q}(\zeta_{2^3}, \sqrt{2}, \sqrt[2^2]{6}) : \mathbb{Q}(\zeta_{2^3}, \sqrt[2^2]{6})] = 1$ holds by noting that $\sqrt{2} \in \mathbb{Q}(\zeta_{2^3})$. Furthermore, it is remarkable that by Theorem 3.5.3 and (3.18) there exist infinitely many primes satisfying the condition of Lemma 3.5.12 for each $r \geq 3$, and the Kronecker density of those primes is equal to $\frac{1}{2^{3r-2}}$.

Chapter 4

Strong difference families, difference covers, and relative difference families

In [22], M. Buratti pointed out an insufficiency of systematic treatments of constructions for relative difference families. The concept of strong difference families was introduced to cover such a problem. However, unfortunately, only a few papers related to strong difference families have appeared in the literature in the past ten years. In this chapter, strong difference families, difference covers and their connections to relative difference families and optical orthogonal codes are discussed. Some known results and fundamental facts on strong difference families and difference covers are summarized in Section 4.1. In Sections 4.2, 4.3, and 4.4, existence and non-existence theorems related to strong difference families and difference covers are given. In Section 4.5, we show an asymptotic existence theorem on relative difference families under the assumption that a strong difference family exists.

4.1 Fundamental facts on strong difference families and difference covers

In Section 1.3, we introduced the concept of strong difference families. Now, we again provide its definition. A family $\mathcal{E} = \{A_i \,|\, 1 \leq i \leq m\}$ of multisets, called *blocks*, of size k defined on an abelian group N is called an (N, k, μ) *strong difference family* (SDF) if the multiset $\{b-a \,|\, a, b \in A_i; 1 \leq i \leq m\}$ of differences covers all elements in N exactly μ times. Note that each block is defined as a multiset and all elements including 0 must be covered as differences, which are major differences from the definition of ordinary difference families. With notations of a group ring, we restate the definition of an (N, k, μ)-SDF $\mathcal{E} = \{A_i \,|\, 1 \leq i \leq n\} \subseteq \mathbb{Z}N$ as

$$\sum_{1 \leq i \leq m} A_i A_i^{(-1)} = k\{0\} + \mu N. \tag{4.1}$$

We may also call it as an (n, k, μ)-SDF over N when $|N| = n$. If N is cyclic, an (N, k, μ)-SDF is called *cyclic* and denoted by (n, k, μ)-CSDF. The number of blocks of an (n, k, μ)-SDF is

$n\mu/k(k-1)$, and hence it must be satisfied that $n\mu \equiv 0 \pmod{k(k-1)}$. Furthermore, the element $0 \in N$ is expressed in even ways as differences in any multiset, and then $\mu \equiv 0 \pmod 2$ must hold. When $|\mathcal{E}| = 1$, the uniquely included multiset $D \in \mathcal{E}$ is called an (N, k, μ) *difference cover*. As far as the author knows, only the two papers [24, 25] consciously using these useful concepts have been appeared in the past ten years. In both of the papers, as a topic of graph decompositions, they mainly treated connections between (G, N, Γ, λ)-DFs and (N, Γ, μ)-SDFs where Γ is an arbitrary graph, however, only a few new constructions of (N, k, μ)-SDFs were given. For the formal definitions of (G, N, Γ, λ)-DFs and (N, Γ, μ)-SDFs, see [24, 25]. Note that the special case when Γ is a complete subgraph with k vertices exactly gives the definitions of (G, N, k, λ)-DFs and (N, k, μ)-SDFs. We note that relative difference families and strong difference families can be studied for any finite group but we restrict our study to abelian groups. Some of our results can be extended to non-abelian groups as well.

We give the following summary of known results on cyclic SDFs.

Theorem 4.1.1. There exist cyclic SDFs for the following parameters (n, k, μ):

(i) [9]	$(m(m-1), m^2, m(m+1))$ for any positive integer m,
(ii) [9]	$(m(m+1), m^2, m(m-1))$ for any positive integer m,
(iii) [22]	$(m+1, m^2, m^2(m-1))$ for any positive integer m,
(iv) [22]	$(m, m+1, (m+1)(m+2))$ for any positive integer m,
(v) [22]	$(m, m, m(m-1))$ for any positive integer m,
(vi) [8, 9, 22]	$(p, p, p-1)$ for any odd prime p,
(vii) [8, 9, 22]	$(p, p+1, p+1)$ for any odd prime $p \equiv 3 \pmod 4$,
(viii) [22]	$(p, p+1, 2p+2)$ for any odd prime p,
(ix) [8, 22]	$(p(p+2), p(p+2)+1, p(p+2)+1)$ for any twin primes p and $p+2$,
(x) [8, 9, 22]	$(\frac{q^d-1}{q-1}, q^d, q^d(q-1))$ for any prime power q and any positive integer d.

Theorem 4.1.2. There do not exist cyclic difference covers for the following parameters (n, k, μ):

(i) ([9])	$(n, k, 2)$ for all positive integers n and k excepting $(n, k) = (3, 3)$ and $(6, 4)$,
(ii) ([8, 9])	$(m^2(m \pm 1), m^2, m \mp 1)$ for all positive integers m,
(iii) ([8, 9])	$(\frac{m^2(m+1)}{t}, m^2, t(m-1))$ for all positive integers t and m satisfying $t \mid m+1$.

For individual cyclic SDFs with small k, see [23, 28, 31, 34, 55, 53, 78].

4.2 Strong difference families of order 2

4.2.1 Sums of squares

The following is an immediate generalization of Proposition 2.2 in [22].

Lemma 4.2.1. Let $\mathcal{E}$ be a family of m k-multisets A_i, $1 \le i \le m$, defined on an abelian group N, where we denote the replication number of each element $a \in A_i$ by $c_{i,a}$. Then $\mathcal{E}$ is an (N, k, μ)-SDF if and only if the following holds:

$$\mu = \sum_{i=1}^{m} \sum_{a \in N} c_{i,a}(c_{i,a} - 1) = \sum_{i=1}^{m} \sum_{a \in N} c_{i,a} c_{i,a+b} \text{ for every } b \in N \setminus \{0\}.$$

By Theorem 4.2.1, a necessary and sufficient condition for $\{A_i \mid 1 \le i \le m\}$ defined on $\mathbb{Z}_2$ to be a $(2, k, k(k-1)m/2)$-CSDF is

$$\sum_{i=1}^{m}(c_{i,0}(c_{i,0}-1)+c_{i,1}(c_{i,1}-1))) = \sum_{i=1}^{m} 2c_{i,0}c_{i,1}.$$

Noting that $k = c_{i,0} + c_{i,1}$ for every i, this condition can be immediately reformulated as $\sum_{i=1}^{m}(k-2c_{i,0})^2 = km$. By substituting $x_i = k - 2c_{i,0}$, $1 \le i \le m$, as variables in this equation, we have:

Lemma 4.2.2. There exists a $(2, k, k(k-1)m/2)$-CSDF for given k and m if and only if the equation

$$\sum_{i=1}^{m} x_i^2 = km \tag{4.2}$$

has at least one solution such that every x_i has the same parity with k and satisfies $|x_i| \le k$.

The problem whether u can be expressed as a sum of m squares or not for given positive integers u and m has been studied by many researchers in relation to that of factorizations of integers in an algebraic number field. For this problem, the following solution is known [94, 108].

Theorem 4.2.3. A positive integer u can be expressed as a sum of m squares if and only if

- $(m = 1)$ u is square,
- $(m = 2)$ e_i is even for every $p_i \equiv 3 \pmod 4$ if $u = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ for distinct primes p_i,
- $(m = 3)$ $u \ne 4^a(8b+7)$ for any positive integers $a, b \ge 0$,
- $(m \ge 4)$ u is arbitrary.

4.2.2 Existence of cyclic strong difference families of order 2

From Lemma 4.2.2 and Theorem 4.2.3, to get a complete solution for the existence of $(2, k, k(k-1)m/2)$-CSDFs, it must be known when every x_i has the same parity with k and satisfies $|x_i| \le k$ in (4.2). Note that $x_i^2 \equiv 0 \pmod 4$ if x_i is even, and $x_i^2 \equiv 1 \pmod 8$ otherwise.

First, we give a necessary condition.

Lemma 4.2.4. There do not exist $(2, k, k(k-1)m/2)$-CSDFs for all of the following cases:

- (i) $k \equiv 2 \pmod 4$ and $m \equiv 1 \pmod 2$,
- (ii) $k \equiv 3 \pmod 4$ and $m \equiv 1 \pmod 2$,
- (iii) $k \equiv 5 \pmod 8$ and $m \equiv 1 \pmod 2$,
- (iv) $k \equiv 3 \pmod 4$ and $m \equiv 2 \pmod 4$.

Proof: In Case (i), denote $k = 4\ell+2$ and $m = 2t+1$. Since k is even, all x_i's must be even and we can write the left hand side of (4.2) as $\sum_{i=1}^{2t+1} x_i^2 = 4\sum_{i=1}^{2t+1} w_i^2$, where $w_i = x_i/2$ for all i, $1 \le i \le m$. On the other hand, the right hand side of (4.2) is $(4\ell+2)(2t+1) = 4(2\ell t+\ell+t)+2$, which is impossible. In Case (ii), denote $k = 4\ell + 3$ and $m = 2t + 1$. Since k is odd, all x_i's must be odd and we can write the left hand side of (4.2) as $\sum_{i=1}^{2t+1} x_i^2 = 8(\sum_{i=1}^{2t+1} w_i) + 2t + 1$,

where $w_i = (x_i^2 - 1)/8$ for all i, $1 \leq i \leq m$. On the other hand, the right hand side of (4.2) is $(4\ell + 3)(2t + 1) = 4(2\ell t + \ell + t) + 2t + 3$, which is impossible. The remaining cases can be checked similarly. □

Next, we treat the case of $k \leq 2$.

Lemma 4.2.5. There exists a $(2, k, k(k-1)m/2)$-CSDF for $k \leq 2$ if and only if $m \equiv 0 \pmod{k}$.

Proof: The necessity was given in Lemma 4.2.4, and so we show the sufficiency directly. For the case of $k = 1$, take $x_i = 1$ for all i, $1 \leq i \leq m$, in (4.2). For the case of $k = 2$, take $x_{2i-2} = 0$ and $x_{2i-1} = 2$ for all i, $1 \leq i \leq m/2$. □

In the following, we treat the case of $m \leq 7$.

Lemma 4.2.6. There exists a $(2, k, k(k-1)m/2)$-CSDF for $m \leq 7$ if and only if k satisfies the following:

$(m = 1)$ k is square,
$(m = 2)$ e_i is even for every $p_i \equiv 3 \pmod{4}$ if $k = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ for distinct primes p_i,
$(m = 3)$ $k \not\equiv 2, 3 \pmod{4}$ and $k \neq 4^a(8b + 5)$ for any positive integers $a, b \geq 0$;
$(m = 4)$ k is arbitrary,
$(m = 5)$ $k \equiv 0, 1, 4 \pmod{8}$,
$(m = 6)$ $k \not\equiv 3 \pmod{4}$,
$(m = 7)$ $k \equiv 0, 1, 4 \pmod{8}$.

Proof: Note that if $km \leq k^2$, all x_i's satisfy $|x_i| \leq k$ in the equation (4.2). Furthermore, for the cases of $m = 1, 2$, and 3 except for the cases of Lemma 4.2.4, all x_i's have the same parity with k in the equation (4.2). By these facts, Theorem 4.2.3, Lemmas 4.2.2, and 4.2.4, the assertions for $m = 1, 2$, and 3 follow.

(Case $m = 4$). When $k \geq 4$ is even, it is obvious that all x_i's are even in the equation (4.2). Then, by Theorem 4.2.3 (iv) and $km \leq k^2$, x_i's have a suitable solution. When $k \geq 3$ is odd, put $k = 2\ell + 1$ and $x_4 = 3$. In this case, the equation (4.2) is reformulated as $\sum_{i=1}^{3} x_i^2 = 8(\ell - 1) + 3$ $(\leq k^2)$, and then x_i's are odd and have a suitable solution by Theorem 4.2.3 (iii). The cases of $k = 1$ and 2 are completed by Lemma 4.2.4.

(Case $m = 5$). When $k \equiv 0 \pmod{8}$ with $k \geq 8$, put $k = 8\ell$ and $x_5 = 4$. Then the equation (4.2) is reformulated as $\sum_{i=1}^{4} x_i^2 = 4(10\ell - 4)$ $(\leq k^2)$, and hence this case can be reduced to that of $m = 4$ and k is even. Similarly, when $k \equiv 1 \pmod{8}$ with $k \geq 9$ or $k \equiv 4 \pmod{8}$ with $k \geq 4$, put $x_5 = 3$ or $x_5 = 2$, respectively, and then each of these cases are reduced to Case $m = 4$. Thus, together with Lemmas 4.2.4 and 4.2.5, we obtain the assertion for $m = 5$.

Similar to the case of $m = 5$, we can reduce the cases of $m = 6$ and 7 to that of $m = 4$. In these cases, we give only combinations of (x_5, x_6) and k or (x_5, x_6, x_7) and k.

(Case $m = 6$).

$$(x_5, x_6) = \begin{cases} (2,2) & \text{if } k \equiv 0 \pmod{4} \text{ with } k \geq 4, \\ (3,3) & \text{if } k \equiv 1 \pmod{4} \text{ with } k \geq 5, \\ (2,4) & \text{if } k \equiv 2 \pmod{4} \text{ with } k \geq 6. \end{cases}$$

(Case $m = 7$).

$$(x_5, x_6, x_7) = \begin{cases} (4,4,4) & \text{if } k \equiv 0 \,(\mathrm{mod}\ 8) \text{ with } k \geq 8, \\ (3,3,3) & \text{if } k \equiv 1 \,(\mathrm{mod}\ 8) \text{ with } k \geq 9, \\ (2,2,2) & \text{if } k \equiv 4 \,(\mathrm{mod}\ 8) \text{ with } k \geq 4. \end{cases}$$

□

In the following two lemmas, we use $(2, k, k(k-1)m/2)$-CSDFs of $m = 4, 5$, and 6 given in Lemma 4.2.6.

Lemma 4.2.7. There exists a $(2, k, k(k-1)m/2)$-CSDF for any $m \equiv 1 \,(\mathrm{mod}\ 4)$ with $m \geq 5$, and for any $m \equiv 3 \,(\mathrm{mod}\ 4)$ with $m \geq 11$, except for Case (i), (ii), and (iii) of Lemma 4.2.4.

Proof: When $m \equiv 1 \,(\mathrm{mod}\ 4)$, take $(m-5)/4$ copies of a $(2, k, 2k(k-1))$-CSDF and one $(2, k, 5k(k-1)/2)$-CSDF. When $m \equiv 3 \,(\mathrm{mod}\ 4)$, take $(m-11)/4$ copies of a $(2, k, 2k(k-1))$-, one $(2, k, 5k(k-1)/2)$-CSDF, and one $(2, k, 3k(k-1))$-CSDF. □

Lemma 4.2.8. There exists a $(2, k, k(k-1)m/2)$-CSDF for any even $m \geq 4$, except for Case (iv) of Lemma 4.2.4.

Proof: When $m \equiv 0 \,(\mathrm{mod}\ 4)$, take $m/4$ copies of a $(2, k, 2k(k-1))$-CSDF. When $m \equiv 2 \,(\mathrm{mod}\ 4)$, take $(m-6)/4$ copies of a $(2, k, 2k(k-1))$-CSDF and one $(2, k, 3k(k-1))$-CSDF. □

Combining all lemmas, we immediately get the following:

Theorem 4.2.9. There exists a $(2, k, k(k-1)m/2)$-CSDF if and only if k satisfies the following:

$(m = 1)$	k is square,
$(m = 2)$	e_i is even for every $p_i \equiv 3 \,(\mathrm{mod}\ 4)$ if $k = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ for distinct primes p_i,
$(m = 3)$	$k \not\equiv 2, 3 \,(\mathrm{mod}\ 4)$ and $k \neq 4^a(8b+5)$ for any positive integers $a, b \geq 0$,
$(m \geq 4)$	k is arbitrary when $m \equiv 0 \,(\mathrm{mod}\ 4)$,
	$k \not\equiv 3 \,(\mathrm{mod}\ 4)$ when $m \equiv 2 \,(\mathrm{mod}\ 4)$,
	$k \equiv 0, 1, 4 \,(\mathrm{mod}\ 8)$ when $m \equiv 1 \,(\mathrm{mod}\ 2)$.

In Section 4.5, we can find a nice application of Theorem 4.2.9.

4.3 Difference covers from partial difference sets

A construction of difference covers generated from partial difference sets (and ordinary difference sets) were discussed in [8, 9]. In this section, we try to generalize it. A k-subset (not multiset) D of an abelian group N is called an $(N, k, \lambda_1, \lambda_2)$ *partial difference set* if every non-identity element in D appears in ΔD exactly λ_1 times and every non-identity element not in D exactly λ_2 times. From this definition, using notations of the group ring of Subsection 1.1, the set D is a partial difference set iff

$$DD^{(-1)} = \lambda_2 N + (\lambda_1 - \lambda_2)D + \gamma\{0\}, \tag{4.3}$$

where $\gamma = k - \lambda_2$ if $0 \notin D$ and $\gamma = k - \lambda_1$ if $0 \in D$. Note that D is a partial difference set iff $N - D$ is. In this section, we assume $D = D^{(-1)}$. In this case, it is easy to see that D (containing 0) is a partial difference set iff $D - \{0\}$ is. For further basic properties of partial difference sets, see [77].

Lemma 4.3.1. Let D be an $(n, k, \lambda_1, \lambda_2)$ partial difference set with $0 \in D$ and $D = D^{(-1)}$ over an abelian group N and set $d = \lambda_2 - \lambda_1$. Let s be any integer satisfying

$$4n \mid s(-2d - 4k + d^2 s + 4ks - 4\lambda_1 s), \tag{4.4}$$

If x,y, and z defined by

$$(x, y, z) = \left(y + s, \frac{s(-2d - 4k + d^2 s + 4ks - 4\lambda_1 s)}{4n}, \frac{ds}{2} + x \right) \tag{4.5}$$

are all non-negative, then $D' = x(D - \{0\}) + y(N - D) + z\{0\}$ is an $(N, k' = (d^2 + 4k - 4\lambda_1)s^2/4, \mu)$ difference cover, where $\mu = k'(k' - 1)/n$.

Proof: For the $(N, k, \lambda_1, \lambda_2)$ partial difference set D, let $D' = x(D - \{0\}) + y(N - D) + z\{0\}$. Note that x, y, and z are non-negative integers by the assumption. Then D' is the desired difference cover. Indeed, since D is a partial difference sets, it holds that

$$\begin{aligned}
& D'D'^{(-1)} \\
= \; & (x(D - \{0\}) + y(N - D) + z\{0\})^2 \\
= \; & (x - y)^2 D^2 + y^2 N^2 + (x - z)^2 \{0\}^2 - 2(x - y)(x - z)D\{0\} \\
& -2y(x - z)N\{0\} + 2y(x - y)ND \\
= \; & ((x - y)^2 \lambda_2 + ny^2 - 2y(x - z) + 2ky(x - y))N + ((k - \lambda_1)(x - y)^2 + (x - z)^2)\{0\} \\
& +((x - y)^2(\lambda_1 - \lambda_2) - 2(x - y)(x - z))D \\
= \; & \mu N + k'\{0\},
\end{aligned}$$

where $|D'| = x(k - 1) + y(g - k) + z = s^2(d^2 + 4k - 4\lambda_1)/4$ and $\mu = k'(k' - 1)/n$. □

It is easy to see that the condition of Lemma 4.3.1 is also necessary for $D' = x(D - \{0\}) + y(N - D) + z\{0\}$ to be a difference cover. To ease the expression of this condition, we restrict the parameters of D (containing 0) to the following two types:

$$(n, k, \lambda_1, \lambda_2) = (m^2, r(m - 1) + 1, m + r^2 - 3r + 2, r^2 - r), \tag{4.6}$$

$$(n, k, \lambda_1, \lambda_2) = (m^2, r(m + 1) + 1, -m + r^2 + 3r + 2, r^2 + r). \tag{4.7}$$

The above parameters (4.6) and (4.7) are known as *Latin square type* and *negative Latin square type*, respectively (see [77]). Then, by Lemma 4.3.1, we immediately have the following corollaries:

Corollary 4.3.2. Let D be a Latin square type partial difference set with $D = D^{(-1)}$ having the parameter (4.6) over N, and let u be any integer such that $m \mid u(2r - 1)$. If x, y, and z defined by

$$(x, y, z) = \left(u^2 + 2u - \frac{u(2r - 1)}{m}, u^2 - \frac{u(2r - 1)}{m}, u(2r - m) + u^2 - \frac{u(2r - 1)}{m} \right)$$

are all non-negative, then $D' = x(D - \{0\}) + y(N - D) + z\{0\}$ is an $(N, u^2 m^2, u^2(u^2 m^2 - 1))$ difference cover.

Corollary 4.3.3. Let D be a negative Latin square type partial difference set with $D = D^{(-1)}$ having the parameter (4.7) over N, and let u be any integer such that $m \mid u(2r+1)$. If x, y, and z defined by

$$(x, y, z) = \left(u^2 + 2u - \frac{u(2r+1)}{m}, u^2 - \frac{u(2r+1)}{m}, u(m-2r) + u^2 - \frac{u(2r+1)}{m} \right)$$

are all non-negative, then $D' = x(D - \{0\}) + y(N - D) + z\{0\}$ is an $(N, u^2m^2, u^2(u^2m^2 - 1))$ difference cover.

Example 4.3.4. In [45], Davis found partial difference sets with parameters

$$(p^{2r}, (p^{2r}+1)/2, (p^{2r}+3)/4, (p^{2r}-1)/4) \text{ over } \mathbb{Z}_{p^2}^r$$

for $r \geq 2$, and

$$(p^{4a+4b}, (p^{4a+4b}+1)/2, (p^{4a+4b}+3)/4, (p^{4a+4b}-1)/4) \text{ over } \mathbb{Z}_{p^2}^{4a} \times \mathbb{Z}_{p^2}^{4b},$$

where $a+b$ is a power of 2. By applying Corollary 4.3.2, we have a $(p^{2r}, u^2p^{2r}, u^2(u^2p^{2r}-1))$ difference cover over $\mathbb{Z}_{p^2}^r$ and a $(p^{4a+4b}, u^2p^{4a+4b}, u^2(u^2p^{4a+4b}-1))$ difference cover over $\mathbb{Z}_{p^2}^{4a} \times \mathbb{Z}_{p^2}^{4b}$, where u is an arbitrary integer. This example contains Corollary 3.8 in [9].

Remark 4.3.5. Lemma 4.3.1 provides many new infinite series of difference covers since partial difference sets with the required condition for parameters abundantly exist, see, e.g., [45, 71, 77, 99, 100] and references there in. Note that Lemma 4.3.1 includes Lemma 3.6 in [9].

4.4 Difference covers over a finite field

In this section, we give some classes of new difference covers from finite fields using a classical approach of cyclotomic cosets.

The following is a necessary and sufficient condition for the multiset $yC_\infty + \sum_{0 \leq i \leq e-1} x_i C_i^e$ consisting of cyclotomic coset C_i^e's of index e and $C_\infty = \{0\}$ to be a difference cover.

Lemma 4.4.1. Let $q = ef + 1$ be a prime power. Then, the multiset $D = yC_\infty + \sum_{0 \leq i \leq e-1} x_i C_i^e$ is an $(\mathbb{F}_q, k = y + f\sum_{0 \leq i \leq e-1} x_i, \mu)$ difference cover if and only if the following hold:

(i) $y^2 + f\sum_{0 \leq i \leq e-1} x_i^2 = k + \mu$, and

(ii) when both of f and q are odd,

$$\sum_{0 \leq i < j \leq e-1} x_i x_j((j-\ell, i-\ell)_e + (j-\ell+\frac{e}{2}, i-\ell+\frac{e}{2})_e) + \sum_{0 \leq i \leq e-1} x_i^2 (i-\ell, i-\ell)_e + y(x_\ell + x_{\ell+\frac{e}{2}}) = \mu$$

for every ℓ, $0 \leq \ell \leq e/2 - 1$, or

(ii)' when f or q is even,

$$\sum_{0\le i<j\le e-1} 2x_ix_j(j-\ell,i-\ell)_e + \sum_{0\le i\le e-1} x_i^2(i-\ell,i-\ell)_e + 2yx_\ell = \mu$$

for every ℓ, $0 \le \ell \le e-1$.

Proof: By expanding $DD^{(-1)}$ using Lemma 1.3.3, we easily have

$$\begin{aligned} DD^{(-1)} &= \sum_{0\le\ell\le e-1}\Big(\sum_{0\le i<j\le e-1} x_ix_j((j-\ell,i-\ell)_e+(i-\ell,j-\ell)_e) + \sum_{0\le\ell\le e-1} yx_\ell C_\ell^e \\ &\quad + \sum_{0\le i\le e-1} x_i^2(i-\ell,i-\ell)_e)C_\ell^e + \sum_{0\le\ell\le e-1} yx_\ell C_\ell^{e\,(-1)} + (y^2+f\sum_{0\le i\le e-1} x_i^2)C_\infty. \end{aligned}$$

In the above, if f and q are odd, the coefficient of C_ℓ^e is equal to

$$\sum_{0\le i<j\le e-1} x_ix_j((j-\ell,i-\ell)_e+(j-\ell+\frac{e}{2},i-\ell+\frac{e}{2})_e) + \sum_{0\le i\le e-1} x_i^2(i-\ell,i-\ell)_e + y(x_\ell + x_{\ell+\frac{e}{2}})$$

by Lemma 1.3.2 (ii) and by noting $-1 \in C_{e/2}^e$. Furthermore, the coefficient above is also equal to $C_{\ell+e/2}^e$ since $(i-\ell,i-\ell)_e = (i-\ell+\frac{e}{2},i-\ell+\frac{e}{2})_e$ by Lemma 1.3.2 again. If f or q is even, the coefficient of C_ℓ^e is equal to

$$\sum_{0\le i<j\le e-1} 2x_ix_j(j-\ell,i-\ell)_e + \sum_{0\le i\le e-1} x_i^2(i-\ell,i-\ell)_e + 2yx_\ell$$

by Lemma 1.3.2 and by noting $-1 \in C_0^e$. Then, by the equation (4.1), we get the assertion. □

First, we consider the case of $e = 2$. To this end, we need cyclotomic numbers of order 2, which are given in the following lemma.

Lemma 4.4.2. ([105]) When $e = 2$, it holds that

(i) $(0,0)_2 = (1,0)_2 = (1,1)_2 = (f-1)/2$ and $(0,1)_2 = (f+1)/2$ when f is odd;

(ii) $(0,0)_2 = (f-2)/2$ and $(0,1)_2 = (1,0)_2 = (1,1)_2 = f/2$ when f is even.

Theorem 4.4.3. Let q be a prime power $\equiv 3 \pmod 4$. For any even integers a and b, let

$$k_1 = \frac{q(b^2+qa^2)}{4} \quad \text{and} \quad k_2 = \frac{q(4a+b^2+qa^2)}{4} + 1.$$

Then, there exists a $(q, k_i, k_i(k_i-1)/q)$ difference cover over $\mathbb{F}_q$ for each $i = 1$ and 2.

Proof: Put

$$(x_0,x_1,y) = \left(x_1+b, \frac{a(2+aq)+b(b-2)}{4}, -af + \frac{b+2x_1-a}{2}\right)$$

and

$$(x_0,x_1,y) = \left(x_1+b, \frac{a(2+aq)+b(b-2)}{4}, af + \frac{b+2x_1+a+2}{2}\right),$$

respectively. Then, by using Lemma 4.4.2, one can directly check that the conditions (i) and (ii) in Lemma 4.4.1 are satisfied. □

Theorem 4.4.4. Let q be a prime power $\equiv 1 \pmod 4$. There exist $(q, a^2, a^2(a^2-1)/q)$ and $(q, (a+1)^2, (a+1)^2((a+1)^2-1)/q)$ difference covers over $\mathbb{F}_q$ for any positive integer a such that $q \mid a(a+1)$.

Proof: Put

$$(x_0, x_1, y) = \left(\frac{a(a+1)}{q}, \frac{a(a+1)}{q}, -a + \frac{a(a+1)}{q} \right)$$

and

$$(x_0, x_1, y) = \left(\frac{a(a+1)}{q}, \frac{a(a+1)}{q}, a+1 + \frac{a(a+1)}{q} \right),$$

respectively. Then, by using Lemma 4.4.2, one can directly check that the conditions (i) and (ii)' of Lemma 4.4.1 are satisfied. □

Theorem 4.4.5. Let q be a prime power $\equiv 1 \pmod 4$. There exist a $(q, a^2q, a^2(a^2q-1))$ difference cover over $\mathbb{F}_q$ for any integer a.

Proof: Put $(x_0, x_1, y) = (a^2 \pm a, a^2 \mp a, a^2)$. Then, by using Lemma 4.4.2, one can directly check that the conditions (i) and (ii)' of Lemma 4.4.1 are satisfied. □

Secondly, we treat the case of $e = 3$.

Lemma 4.4.6. ([105]) When $e = 3$, it holds that

$$\begin{aligned}
&(0,0)_3 = (q - 8 + c)/9, \\
&(0,1)_3 = (1,0)_3 = (2,2)_3 = (2q - 4 - c - 9d)/18, \\
&(0,2)_3 = (2,0)_3 = (1,1)_3 = (2q - 4 - c + 9d)/18, \\
&(1,2)_3 = (2,1)_3 = (q + 1 + c)/9,
\end{aligned}$$

where $4q = 4p^r = c^2 + 27d^2$ for a prime p and an integer $c \equiv 1 \pmod 3$ such that

(i) if $p \equiv 2 \pmod 3$, then r is even and $4q = (\pm 2p^{r/2})^2 + 27 \cdot 0^2$;

(ii) if $p \equiv 1 \pmod 3$, then $4q = c^2 + 27d^2$ is the unique representation of $4q$ such that $\gcd(c, p) = 1$; the sign of d is determined by a choice of a primitive root of $\mathbb{F}_q$.

Theorem 4.4.7. Let $q = p^{2r}$ be a prime power, where $p \equiv 2 \pmod 3$. Then, there exist a $(q, q^2u^2, qu^2(q^2u^2-1))$ difference cover over $\mathbb{F}_q$ for any integer u.

Proof: Put $a = p^r$ or $a = -p^r$ depending on whether r is odd or even, respectively, and let

$$(x_0, x_1, x_2, y) = \left(x_2 + 2au, x_0, qu^2 - \frac{u(1+4a)}{3}, qu^2 + \frac{u(-1+q)}{3} \right).$$

Then, by using Lemma 4.4.6 as $c = 2a$ and $d = 0$, one can directly check that the conditions (i) and (ii)' in Lemma 4.4.1 are satisfied. □

It seems that the size k of difference covers obtained in Theorem 4.4.7 is large, but the result is new. Furthermore, in particular when $p = 2$, we can find a good application to relative difference families, see Corollary 4.5.10 in the next section.

Thirdly, we treat the case when $e = 4$ and f is odd, i.e., $q \equiv 5 \pmod 8$.

Lemma 4.4.8. ([105]) When $e = 4$ and f is odd, it holds that

$$\begin{aligned}
&(0,0)_4 = (2,0)_4 = (2,2)_4 = (q-7+2s)/16,\\
&(0,1)_4 = (1,3)_4 = (3,2)_4 = (q+1+2s-8t)/16,\\
&(0,2)_4 = (q+1-6s)/16,\\
&(0,3)_4 = (1,2)_4 = (3,1)_4 = (q+1+2s+8t)/16,\\
&(1,0)_4 = (1,1)_4 = (2,1)_4 = (2,3)_4 = (3,0)_4 = (3,3)_4 = (q-3-2s)/16,
\end{aligned}$$

where $q = p^r = s^2 + 4t^2$ for a prime p and an integer $s \equiv 1 \pmod 4$ such that $\gcd(s,p) = 1$ and the sign of t is determined by the choice of a primitive root of $\mathbb{F}_q$.

Theorem 4.4.9. Let $q = s^2 + 4t^2$ be a prime power $\equiv 5 \pmod 8$, where $s \equiv 1 \pmod 4$ and $\gcd(s,q) = 1$, and u an arbitrary integer. Put

$$k_1 = 1 + (2 + s^2u^2)u^2q \text{ and } k_2 = 1 + (1 + t^2u^2)u^2q.$$

Then, there exists a $(q, k_i, k_i(k_i-1)/q)$ difference cover over $\mathbb{F}_q$ for each $i = 1$ and 2.

Proof: Put

$$(x_0,x_1,x_2,x_3,y) = (u((2-s)u+s^2u^3-2), x_0+2u+2su^2, x_0+4u, x_0+2u+2su^2, x_0+1+2u+su^2)$$

and

$$(x_0,x_1,x_2,x_3,y) = (u(u^3t^2+u(1-t)-1), x_0+2u+2tu^2, x_0+2u, x_0+2tu^2, x_0+1+u+tu^2),$$

respectively. Then, by using Lemma 4.4.8, one can directly check that the conditions (i) and (ii) of Lemma 4.4.1 are satisfied. □

Finaly, we treat the case when $e = 6$, f is odd, and 2 is a cube in $\mathbb{F}_q$.

Lemma 4.4.10. ([105]) Assume that 2 is a cube in $\mathbb{F}_q$. When $e = 6$ and f is odd, it holds that by

$$\begin{aligned}
&(0,0)_6 = (3,0)_6 = (3,3)_6 = (q-11-8s)/36,\\
&(0,1)_6 = (2,5)_6 = (4,3)_6 = (0,2)_6 = (1,4)_6 = (5,3)_6 = (q+1-2s+12t)/36,\\
&(0,3)_6 = (q+1+16s)/36,\\
&(0,4)_6 = (1,3)_6 = (5,2)_6 = (0,5)_6 = (2,3)_6 = (4,1)_6 = (q+1-2s-12t)/36,\\
&(1,0)_6 = (2,2)_6 = (3,1)_6 = (3,4)_6 = (4,0)_6 = (5,5)_6 = (q-5+4s+6t)/36,\\
&(1,1)_6 = (2,0)_6 = (3,2)_6 = (3,5)_6 = (4,4)_6 = (5,0)_6 = (q-5+4s-6t)/36,\\
&(1,2)_6 = (1,5)_6 = (2,4)_6 = (4,2)_6 = (5,1)_6 = (5,4)_6 = (2,1)_6 = (4,5)_6 = (q+1-2s)/36,
\end{aligned}$$

where $q = s^2+3t^2$ with $s \equiv 1 \pmod 3$ such that $\gcd(s,p) = 1$ and the sign of t is determined by the choice of a primitive root of $\mathbb{F}_q$.

The cubic character of $2 \in \mathbb{F}_q$ can be characterized by the following lemma.

Lemma 4.4.11. ([105]) Assume that $q \equiv 1 \pmod 3$ is an odd prime power such that $4q = c^2 + 27d^2$ with $c \equiv 1 \pmod 3$ yielding the cyclotomic numbers for $e = 3$ in Lemma 4.4.6. Then, 2 is a cube in $\mathbb{F}_q$ if and only if c is even.

Theorem 4.4.12. Let $q = s^2 + 3t^2 \equiv 7 \pmod{12}$ be a prime power, where $s \equiv 1 \pmod 3$ and $\gcd(s, q) = 1$, such that 2 is a cube in $\mathbb{F}_q$. Let u be an arbitrary positive integer such that $s \mid 2(1+3ut^2)$ and put $k = (5s^2+12t^2)(1+uq)^2/s^2$. Then, there exists a $(q, k, k(k-1)/q)$ difference cover over $\mathbb{F}_q$.

Proof: Put

$$x_0 = x_2 = x_4 = \frac{(4 + 5us^2 + 12ut^2)(1 + uq)}{s^2},\ x_1 = x_5 = \frac{(4 - 2s + 5us^2 + 12ut^2)(1 + uq)}{s^2},$$
$$x_3 = \frac{(4 + 4s + 5us^2 + 12ut^2)(1 + uq)}{s^2},\ \text{and}\ y = \frac{(4 + (1 + 5u)s^2 + 12ut^2)(1 + uq)}{s^2}.$$

Then, by using Lemma 4.4.10, one can directly check that the conditions (i) and (ii) of Lemma 4.4.1 are satisfied. □

Note that $C_0^6 \cup C_1^6 \cup C_3^6$ forms a difference set if q is a prime power of the form $q = x^2 + 27 \equiv 1 \pmod 6$ [105]. Hence, by using the theorem given in [8, 9], we also get a family of difference covers for $e = 6$.

In the theorems of this section, we calculated only the cases when $e \leq 6$. One may obtain further new series of difference covers over a finite field with more computations using cyclotomic numbers and Jacobi sums, see [11, 70, 77, 105]. Again, most of the resultant difference covers obtained in this section are new and include the results (vi) and (vii) of Theorem 4.1.1.

4.5 Relative difference families and strong difference families

4.5.1 Fundamental relations

Theorem 4.5.1. Let $G = N \times H$ be an abelian group. Let $\sigma : N \times H \to N$ be the projection defined by $\sigma((x, y)) = x$. If there exists a $(G, N \times \{0\}, k, \lambda)$-DF $\mathcal{F}$, then $\sigma(\mathcal{F})$ is an $(N, k, (|H| - 1)\lambda)$-SDF.

Proof: Let $\mathcal{E} = \sigma(\mathcal{F}) = \{\sigma(B) \mid B \in \mathcal{F}\}$. Then, we have

$$\bigcup_{A \in \mathcal{E}} \Delta A = \bigcup_{B \in \mathcal{F}} \Delta\sigma(B) = \bigcup_{B \in \mathcal{F}} \sigma(\Delta B) = \lambda\sigma(N \times (H \setminus \{0\})) = \lambda(|H| - 1)N.$$

□

The following was also given in [24].

Theorem 4.5.2. Let H be any subgroup of an abelian group G. Let $\sigma : G \to N = G/H$ be the canonical homomorphism. If there exists a (G, k, μ)-SDF $\mathcal{F}$, then $\sigma(\mathcal{F})$ is an $(N, k, |H|\mu)$-SDF.

The above is easy, but useful to discuss about non-existence of (nv, n, k, λ)-DFs. The following are nice applications of Theorems 4.5.1 and 4.5.2 using Theorem 4.2.9.

Example 4.5.3. (i) By Theorems 4.5.1 and 4.2.9, $(\mathbb{Z}_2 \times H, \mathbb{Z}_2 \times \{0\}, k, k(k-1)m/2(|H| - 1))$-DFs do not exist for all pairs (k, m) satisfying the converse condition of Theorem 4.2.9, where H is any abelian group satisfying $|H| - 1 \mid k(k-1)m/2$. For example,

consider $(2v, 2, 5, 1)$-CDFs. The admissible v for the existence of $(2v, 2, 5, 1)$-CDFs is $v \equiv 1 \pmod{10}$. On the other hand, $(2v, 2, 5, 1)$-CDFs do not exist for all $v \equiv 11 \pmod{20}$ by taking $H = \mathbb{Z}_v$ with $v = 10u + 1$ and $k = 5$. This also implies the non-existence of optimal $(2v, 5, 1)$-OOCs for all $v \equiv 11 \pmod{20}$ since any optimal $(2v, 5, 1)$-OOC with $v \equiv 1 \pmod{10}$ must be a $(2v, 2, 5, 1)$-DF.

(ii) Consider $(6, 5, 10m)$-CSDFs. By Theorems 4.5.2 and 4.2.9, $(6, 5, 10m)$-CSDFs do not exist for all odd m by taking $H = \mathbb{Z}_3$, $n = 3m$, and $k = 5$, which implies the non-existence of $(6v, 6, 5, 1)$-CDFs for any $v \equiv 11 \pmod{20}$ with $\gcd(v, 3) = 1$ by Theorem 4.5.1.

Next, we discuss about an existence problem of relative difference families via strong difference families. Wilson [110] showed that there exist $(\mathbb{F}_q, \{0\}, k, \lambda)$-DFs for sufficiently large prime power q unconsciously using trivial $(1, k, k(k-1))$-SDFs. After his work, many authors used his method to construct several kinds of combinatorial designs and codes. On the other hand, in [22, 24, 25], it was tried to generalize the theorem of Wilson to $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DFs consciously using (N, k, μ)-SDFs, and indeed many new infinite family of $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DFs were obtained. The following theorems played an important role in [22, 24, 25].

Theorem 4.5.4. Let $\mathcal{E} = \{A_i \,|\, 1 \le i \le n\}$ be an (N, k, μ)-SDF, where $A_i = \sum_{a \in N} c_{i,a} X^a$, $1 \le i \le m$, and let q be a prime power and λ a positive integer such that $\mu \,|\, \lambda(q-1)$. Assume that there exists a set S of $\lambda(q-1)/\mu$ elements of $\mathbb{F}_q^\times$ and m k-subsets

$$L_i = \{x_{i,a,h} \,|\, a \in \mathrm{supp}A_i; 1 \le h \le c_{i,a}\} \subset \mathbb{F}_q,$$

$1 \le i \le m$, such that $S \cdot \Delta_b = \lambda \mathbb{F}_q^\times$ for every $b \in N$, where

$$\Delta_b = \bigcup_{1 \le i \le m} \{x_{i,a,h} - x_{i,a',h'} \,|\, a - a' = b; 1 \le h \le c_{i,a}; 1 \le h' \le c_{i,a'}\},$$

and $\mathrm{supp}A_i$ means the set of underlying elements in the multiset A_i. Then the family $\mathcal{F} = \{B_{i,s} \,|\, 1 \le i \le m; s \in S\}$ with

$$B_{i,s} = \{(a, s x_{i,a,h}) \in N \times \mathbb{F}_q \,|\, a \in \mathrm{supp}A_i, 1 \le h \le c_{i,a}\}$$

is an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF.

Given an ℓ-tuple $(j_1, j_2, \ldots, j_\ell) \in \{0, 1, \ldots, e-1\}^\ell$ and a set $A = \{x_1, x_2, \ldots, x_{\ell\lambda}\}$ of $\ell\lambda$ elements of $\mathbb{F}_q$, if each cyclotomic coset $C_{j_i}^e$, $1 \le i \le \ell$, contains exactly λ elements of A, then we say that A is λ-*transversal* for $C_{j_i}^e$, $1 \le i \le \ell$.

Theorem 4.5.5. Let $\mathcal{E} = \{A_i \,|\, 1 \le i \le m\}$ be an (N, k, μ)-SDF with $\mu = d\lambda$ and $q \equiv 1 \pmod{d}$ be a prime power. If there are m k-subsets L_i's of $\mathbb{F}_q^\times$ such that every Δ_b is λ-transversal for C_i^d, $0 \le i \le d-1$, where Δ_b was defined in Theorem 4.5.4, then there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF.

Proof: We can take $S = C_0^d$ in Theorem 4.5.4, then it is clear that $S \cdot \Delta_b = \lambda \mathbb{F}_q^\times$. □

In the rest of this chapter, we use Theorem 1.3.8.

Remark 4.5.6. By Theorem 1.3.8, we can choose a k-subset $B = \{x_1, x_2, \ldots, x_k\}$ of $\mathbb{F}_q$ such that every element of the set $\{x_i - x_j \,|\, 1 \le i < j \le k\}$ (in general, a complete system of representatives for the cosets of $\{-1, 1\}$ in ΔB) can be distributed into a cyclotomic coset C_i^e specified arbitrarily for any odd prime power $q \equiv 1 \pmod{e}$ with $q \ge \min P(e, k-1, 1)$, where $P(e, \ell, t)$ means the set of all prime powers q satisfying $\lceil r_q(\ell, e)/e^\ell \rceil \ge t$ in Theorem 1.3.8. It is important that the index ℓ of $x_j - x_i \in C_\ell^e$ depends only on ℓ' of $x_i - x_j \in C_{\ell'}^e$. In particular, when q is an odd prime power, $\ell = -\ell'$ if $q \equiv e + 1 \pmod{2e}$, and $\ell = \ell'$ if $q \equiv 1 \pmod{2e}$. When q is a power of 2, it holds that $\ell = \ell'$.

The following two theorems are generalizations of Theorem 5.1 in [25] to any λ, but restricting Γ as a complete graph. Hereafter, we denote the subgroup $\{a \in N \,|\, 2a = 0\}$ of an abelian group N by N_2.

Theorem 4.5.7. If there is an (N, k, μ)-SDF with $\mu = 2d\lambda$, then there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, 2\lambda)$-DF for any prime power $q \equiv 1 \pmod{d}$ with $q \ge \min P(d, k-1, 1)$.

Proof: We see that it can be taken subsets L_i's, $1 \le i \le m$, in Theorem 4.5.4 such that Δ_b is 2λ-transversal for C_i^d, $0 \le i \le d-1$. For $b \in N_2$ and any subsets L_i's, there is a subset H_b such that $\Delta_b = \pm H_b$ since $x \in \Delta_b$ iff $-x \in \Delta_b$. (Note that $H_b = -H_b$ when q is even.) Hence, it is sufficient that H_b is λ-transversal for C_i^d, $0 \le i \le d-1$. Furthermore, for $b \notin N_2$, we have $\Delta_b = -\Delta_{-b}$ since $x \in \Delta_b$ iff $-x \in \Delta_{-b}$. Hence, it is sufficient that either of Δ_b or Δ_{-b} is 2λ-transversal for C_i^d, $0 \le i \le d-1$. By Theorem 1.3.8 and Remark 4.5.6, there are such distributions of differences to cyclotomic cosets for any prime power $q \equiv 1 \pmod{d}$ with $q \ge \min P(d, k-1, 1)$. Then, by Theorem 4.5.5, we get the assertion. □

Theorem 4.5.8. If there is an (N, k, μ)-SDF with $\mu = 2d\lambda$, then there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF for any prime power $q \equiv 2d + 1 \pmod{4d}$ with $q \ge \min P(2d, k-1, 1)$.

Proof: It is enough to consider the case when λ is odd by Theorem 4.5.7. We see that it is possible to take subsets L_i's, $1 \le i \le n$, in Theorem 4.5.4 such that Δ_b is λ-transversal for C_i^{2d}, $0 \le i \le 2d-1$. Note that $-1 \in C_{d-1}^{2d}$ since $q \equiv 2d + 1 \pmod{4d}$. For $b \in N_2$, similar to Theorem 4.5.7, it is sufficient that H_b is λ-transversal for C_i^{2d}, $0 \le i \le d-1$. Furthermore, for $b \notin N_2$, it is sufficient that either of Δ_b or Δ_{-b} is λ-transversal for C_i^{2d}, $0 \le i \le 2d-1$. By Theorem 1.3.8 and Remark 4.5.6, there are such distributions of differences. Then, by Theorem 4.5.5, we get the assertion. □

4.5.2 An improvement on distributions of differences

In this subsection, we improve the statement of the case when λ is odd in Theorem 4.5.8. If there is an (N, k, μ)-SDF with $\mu = 2d\lambda$, then it is clear that there also exists an $(N, k, t\mu)$-SDF for any positive integer t, which also means by Theorem 4.5.8 that there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF for a sufficiently large prime power $q \equiv 2dt + 1 \pmod{4dt}$. Hence, if there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF for any large prime power $q \equiv 1 \pmod{2^s d}$, where s is a fixed positive integer, then there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF for any sufficiently large prime power $q \equiv 1 \pmod{2d}$.

Theorem 4.5.9. Let $\mathcal{E} = \{A_i \,|\, 1 \le i \le m\}$ be an (N, k, μ)-SDF with $\mu = 2d\lambda$, where $A_i = \sum_{a \in N} c_{i,a} X^a$, $1 \le i \le m$, and q a prime power $\equiv 1 \pmod{2^s d}$. Assume that there

exists a family of $2^{s-1}m$ k-subsets

$$L_{i,j} = \{x_{i,j,a,h} \,|\, a \in \mathrm{supp}A_i; 1 \le h \le c_{i,a}\} \text{ for } 1 \le i \le m \text{ and } 1 \le j \le 2^{s-1} \tag{4.8}$$

defined on $\mathbb{F}_q$ such that for every $b \in N$

$$\Delta_b = \bigcup_{1\le i\le m} \bigcup_{1\le j\le 2^{s-1}} \{x_{i,j,a,h} - x_{i,j,a',h'} \,|\, a - a' = b; 1 \le h \le c_{i,a}; 1 \le h' \le c_{i,a'}\} = \pm H_b \tag{4.9}$$

for some $H_b \subset \mathbb{F}_q$ and each H_b is λ-transversal for $C_i^{2^{s-1}d}$, $0 \le i \le 2^{s-1}d - 1$. Let S be a complete system of representatives for the cosets of $\{-1, 1\}$ in $C_0^{2^{s-1}d}$. Then the family

$$\mathcal{F} = \{B_{i,j,s} \,|\, 1 \le i \le m; 1 \le j \le 2^{s-1}; s \in S\}$$

with

$$B_{i,j,s} = \{(a, sx_{i,j,a,h}) \in N \times \mathbb{F}_q \,|\, a \in \mathrm{supp}A_i; 1 \le i \le m; 1 \le j \le 2^{s-1}\}$$

is an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF.

Proof: Note that $-1 \in C_0^{2^{s-1}d}$ by the assumption $q \equiv 1 \pmod{2^s d}$. Then we have

$$\begin{aligned} \Delta\mathcal{F} &= \bigcup_{b\in N} \{b\} \times (S \cdot \Delta_b) = \bigcup_{b\in N} \{b\} \times (\pm S \cdot H_b) \\ &= \bigcup_{b\in N} \{b\} \times (C_0^{2^{s-1}d} \cdot H_b) = \lambda(N \times \mathbb{F}_q^{\times}). \end{aligned}$$

□

When $N = \{0\}$ or $\mathbb{Z}_2^m$, i.e., $N = N_2$, it is obvious that for $s = 1$ and for any choice of sets of (4.8) there exists a set H_b such that $\Delta_b = \pm H_b$ for every $b \in N$. Hence, similar to Theorems 4.5.7 and 4.5.8, by using Theorem 1.3.8 and Remark 4.5.6 we have the following:

Corollary 4.5.10. Let $N = \{0\}$ or $\mathbb{Z}_2^m$. If there is an (N, k, μ)-SDF with $\mu = 2d\lambda$, then there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF for any prime power $q \equiv 1 \pmod{2d}$ with $q \ge \min P(d, k-1, 1)$.

Note that Corollary 4.5.10 was also given in [22].

For (N, k, μ)-SDFs with a special structure, one may be able to find some sets of (4.8) satisfying the condition (4.9). Indeed, in [22], by using special $(N, k, \mu = 2d\lambda)$-SDFs, $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DFs for prime powers $q \equiv 1 \pmod{2d}$ were constructed. But, for general (N, k, μ)-SDFs, it seems to be difficult to know whether there is a distribution of differences satisfying (4.9). We can give partial solutions for this problem.

Lemma 4.5.11. Let $k = 3, 4$, or 5. If there is an (N, k, μ)-SDF $\mathcal{E}$ with $\mu = 2d\lambda$, then there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF for any prime power $q \equiv 1 \pmod{2^{s_k} d}$ with $q \ge \min P(2^{s_k-1}d, \ell_k, t_k)$, where

$$(k, s_k, \ell_k, t_k) = (3, 3, 3, 2), (4, 3, 6, 24 \cdot 47 + 1), \text{ and } (5, 4, 12, 80 \cdot 159 + 1).$$

Remark 4.5.12. In (4.8), if there is a subset $H_{i,b} \subset \mathbb{F}_q$ such that

$$\bigcup_{1 \le j \le 2^s} \{x_{i,j,a,h} - x_{i,j,a',h'} \mid a - a' = b; 1 \le h \le c_{i,a}; 1 \le h' \le c_{i,a'}\} = \pm H_{i,b}, \tag{4.10}$$

then the condition (4.9) is satisfied. Furthermore, in order to verify the condition that each H_b is λ-transversal for $C_\ell^{2^{s-1}d}$, $0 \le \ell \le 2^{s-1}d - 1$, it is sufficient that all elements of $H_{i,b}$ can be distributed to cyclotomic cosets specified arbitrarily for all i.

Proof: For the case of $k = 3$, there are three patterns of $A_i = \{0, a, b\} \in \mathcal{E}$, those are, (i) $a \in N_2$ and $b \notin N_2$, (ii) $a, b, a - b \notin N_2$, and (iii) $a, b \in N_2$. For each pattern, we give $L_{i,j}$'s of (4.8).

(i) For $A_i = \{0, a, b\} \in \mathcal{E}$ with $a \in N_2$ and $b \notin N_2$, take $x_{i,j,a,h}$'s of $L_{i,j}$'s of (4.8) as

$$(x_{i,j,0,1}, x_{i,j,a,h}, x_{i,j,b,h'}) = \begin{cases} (0, -x_1 + x_2, -x_1) & \text{for } j = 1, \\ (0, -x_2 + y_1, y_1) & \text{for } j = 2, \\ (0, x_1 + y_2, x_1) & \text{for } j = 3, \\ (0, -y_1 - y_2, -y_1) & \text{for } j = 4, \end{cases}$$

then $H_{i,b}$'s of (4.10) are

$$H_{i,a} = \{x_1 - x_2, x_2 - y_1, x_1 + y_2, y_1 + y_2\},\ H_{i,b} = \{x_1, y_1\},\ \text{ and }\ H_{i,b-a} = \{x_2, y_2\}.$$

Assume that we want to distribute each element of $H_{i,b}$'s to cyclotomic cosets so that

$$(x_1 - x_2, x_2 - y_1, x_1 + y_2, y_1 + y_2, x_1, y_1, x_2, y_2) \in C_{h_1}^{4d} \times C_{h_2}^{4d} \times \cdots \times C_{h_8}^{4d}$$

holds. Now we choose x_1, x_2, y_1, and y_2 from $\mathbb{F}_q$ in that order. More detailed steps are as follows:

(1) Choose x_1 arbitrarily from $C_{h_5}^{4d}$.

(2) Choose x_2 so that $x_2 \in C_{h_7}^{4d}$ and $x_1 - x_2 \in C_{h_1}^{4d}$, where such x_2 always exists for $q \ge \min P(2^2 d, 2, 1)$ by Theorem 1.3.8.

(3) Choose y_1 so that $y_1 \in C_{h_6}^{4d}$, $x_2 - y_1 \in C_{h_2}^{4d}$, and $x_1 + y_2 \ne y_1 + y_2$, where such y_1 always exists for $q \ge \min P(2^2 d, 2, 2)$ by Theorem 1.3.8. Note that $x_1 + y_2 \ne y_1 + y_2$ means that all elements in $\pm H_{i,b}$'s have pairwise distinct forms after the choice of y_1. This condition is required to use Theorem 1.3.8 in the next step.

(4) Choose y_2 so that $y_2 \in C_{h_8}^{4d}$, $x_1 + y_2 \in C_{h_3}^{4d}$, and $y_1 + y_2 \in C_{h_4}^{4d}$, where such y_2 always exists for $q \ge \min P(2^2 d, 3, 1)$ by Theorem 1.3.8.

Thus, every element in $H_{i,b}$'s can be distributed to arbitrary cyclotomic cosets of $\mathbb{F}_q$ for any prime power $q \equiv 1 \pmod{2^3 d}$ with $q \ge \min P(2^2 d, 3, 2)$. For the patterns (ii) and (iii), we give only the forms of $L_{i,j}$'s of (4.8) and the order of choice of x_i's.

(ii) For $A_i = \{0, a, b\} \in \mathcal{E}$ with $a, b, a - b \notin N_2$, let

$$(x_{i,j,0,1}, x_{i,j,a,h}, x_{i,j,b,h'}) = \begin{cases} (0, x_1, x_2) & \text{for } j = 1, \\ (0, -x_1, -x_2) & \text{for } j = 2, \\ (0, y_1, y_2) & \text{for } j = 3, \\ (0, -y_1, -y_2) & \text{for } j = 4, \end{cases}$$

then we have

$$H_{i,a} = \{x_1, y_1\},\ H_{i,b} = \{x_2, y_2\},\ \text{ and }\ H_{i,b-a} = \{x_2 - x_1, y_2 - y_1\}.$$

We can choose x_1, x_2, y_1, y_2 from $\mathbb{F}_q$ in that order so that all elements in $H_{i,b}$'s are distributed to arbitrary cyclotomic cosets of $\mathbb{F}_q$ for any prime power $q \equiv 1 \pmod{2^3 d}$ with $q \geq \min P(2^2 d, 2, 1)$.

(iii) For $A_i = \{0, a, b\} \in \mathcal{E}$ with $a, b \in N_2$, let

$$(x_{i,j,0,1}, x_{i,j,a,h}, x_{i,j,b,h'}) = \begin{cases} (0, w_1, w_2) & \text{for } j = 1; \\ (0, x_1, x_2) & \text{for } j = 2; \\ (0, y_1, y_2) & \text{for } j = 3; \\ (0, z_1, z_2) & \text{for } j = 4, \end{cases}$$

then we have

$$H_{i,a} = \{w_1, x_1, y_1, z_1\},\ H_{i,b} = \{w_2, x_2, y_2, z_2\},\ \text{ and }\ H_{i,b-a} = \{w_2 - w_1, x_2 - x_1, y_2 - y_1, z_2 - z_1\}.$$

We choose $w_1, w_2, x_1, \cdots, z_2$ in that order so that all elements in $H_{i,b}$'s are distributed to arbitrary cyclotomic cosets of $\mathbb{F}_q$ for any prime power $q \equiv 1 \pmod{2^3 d}$ with $q \geq \min P(2^2 d, 2, 1)$.

Hence, by Theorem 4.5.9 and Remark 4.5.12, there exists an $(N \times \mathbb{F}_q, N \times \{0\}, 3, \lambda)$-DF for any prime power $q \equiv 1 \pmod{2^3 d}$ with $q \geq \min P(2^2 d, 3, 2)$ if there is an (N, k, μ)-SDF with $\mu = 2d\lambda$. For the cases of $k = 4$ and 5, one can see the assertions similarly by using Tables 4.1 and 4.2, respectively. Here, we should remark the following to aid checking the cases of $k = 4$ and 5:

(i) The value ℓ of $P(2^{s_k - 1}, \ell, t)$ is naturally determined when the forms of $L_{i,j}$'s are given and the order of choices of x_i's is determined.

(ii) As described in the step (3) of the pattern (i) for the case of $k = 3$, after the choice of each x_i, all elements in $\pm H_{i,b}$'s must have pairwise distinct forms to use Theorem 1.3.8 in the next step. This condition is obviously satisfied when t of $P(2^{s_k - 1}, \ell, t)$ is greater than the number of equations arose from all pairs of two distinct elements in $\pm H_{i,b}$'s, which is less than or equal to $\binom{k(k-1)2^{s_k - 1}}{2}$. Therefore, we set $t = \binom{k(k-1)2^{s_k - 1}}{2} + 1$, and then we can avoid to consider individual cases.

□

By Theorems 4.5.8 and 4.5.9 and Lemma 4.5.11, we immediately get:

Theorem 4.5.13. Let $k = 3, 4$, or 5. If there is an (N, k, μ)-SDF with $\mu = 2d\lambda$, then there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF for any prime power $q \equiv 1 \pmod{2d}$ with $q \geq \min P(2^{s_k - 1} d, \ell_k, t_k)$, where

$$(k, s_k, \ell_k, t_k) = (3, 3, 3, 2), (4, 3, 6, 24 \cdot 47 + 1),\ \text{ and } (5, 4, 12, 80 \cdot 159 + 1).$$

Remark 4.5.14. In the cases of $k \leq 5$, this method has been implicitly used by many authors [23, 28, 31, 34, 55, 53, 78, 118], which is generalized to Theorem 4.5.13. In order to get $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DFs for all prime powers $q \equiv 1 \pmod{2d}$, Theorem 4.5.13 makes the necessity for individual studies of distributions of differences abolish, and requires only the existence of an (N, k, μ)-SDF and $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DFs for small q's.

Table 4.1: This table gives $x_{i,j,a,h}$'s of (4.8) for each pattern of blocks $A_i = \{0, a, b, c\}$ of any $(n, 4, \lambda)$-SDF. In the column j, the symbols o and e indicate $j = 1, 3$ and $j = 2, 4$, respectively.

a, b, c	j	$(x_{i,j,0,1}, x_{i,j,a,h_1}, x_{i,j,b,h_2}, x_{i,j,c,h_3})$	ℓ
$a, b \in N_2$, $c \notin N_2$	1	$(1, x_1, -1 - y_1 + z_1, -y_1)$	5
	2	$(-1, -x_2, 1 + y_2 - z_1, y_2)$	
	3	$(1 - y_1, 2 + x_2 + y_2, z_2, 2)$	
	4	$(-1 + y_2, -2 - x_1 - y_1, -z_2, -2)$	
order		$y_1 \to y_2 \to x_1 \to x_2 \to z_1 \to z_2$	
$a, b - c \in N_2$, $c \notin N_2$,	1	$(1, -1 - x_1 + y_1, -x_1, z)$	6
	2	$(-1, 1 + x_2 - y_1, x_2, -z)$	
	3	$(1, x_1 + y_2, 2 + x_1, -1 + y_1 + y_2 - z)$	
	4	$(-1, -x_2 - y_2, -2 - x_2, 1 - y_1 - y_2 + z)$	
order		$y_1 \to z \to y_2 \to x_1 \to x_2$	
$a \in N_2, b \notin N_2$, $c, b - c \notin N_2$,	1	$(1, -1 - x_1 + y_1, -x_1, -x_1 + z)$	4
	2	$(-1, 1 + x_2 - y_1, x_2, x_2 - z)$	
	3	$(1, x_1 + y_2, 2 + x_1, -x_2 + z)$	
	4	$(-1, -x_2 - y_2, -2 - x_2, x_1 - z)$	
order		$x_1 \to x_2 \to z \to y_1 \to y_2$	
$a, b, c \in N_2$		$(0, x_j, y_j, z_j)$, $1 \le j \le 4$	3
order		$x_1 \to y_1 \to z_1 \to x_2 \to \cdots \to z_4$	
$a, b, c \notin N_2$, $a - b, b - c, a - c \notin N_2$	o	$(0, x_j, y_j, z_j)$	3
	e	$(0, -x_{j-1}, -y_{j-1}, -z_{j-1})$	
order		$x_1 \to y_1 \to z_1 \to x_3 \to y_3 \to z_3$	

Example 4.5.15. For $k = 4$ and 5, by Theorems 4.2.9, 4.1.1, 4.4.3, 4.4.4, and 4.4.5, there are (n, k, μ)-CSDFs with the following parameters:

$$(n, k, \mu) = (1, 4, 12), (2, 4, 6), (3, 4, 4), (6, 4, 2), (1, 5, 20), (2, 5, 20) \text{ and } (5, 5, 4).$$

Then, by Theorem 4.5.13, there exist $(np, n, k, 1)$-CDFs (or optimal $(np, k, 1)$-OOCs) for the parameters (n, k, μ) and for any sufficiently large prime $p \equiv 1 \pmod{\mu}$.

Table 4.2: This table gives $x_{i,j,a,h}$'s of (4.8) for each pattern of blocks $A_i = \{0, a, b, c, d\}$ of any $(n, 5, \lambda)$-SDF. In the column j, the symbols o and e indicate $j = 1, 3, 5, 7$ and $j = 2, 4, 6, 8$, respectively.

a, b, c, d	j	$(x_{i,j,0,1}, x_{i,j,a,h_1}, x_{i,j,b,h_2}, x_{i,j,c,h_3}, x_{i,j,d,h_4})$	ℓ
$a, b, c \in N_2$, $d \notin N_2$	1	$(1, -1 - v_1 + w_1, x_1, -y_1, -v_1)$	7
	2	$(-1, 1 + v_2 - w_1, -x_2, -y_2, v_2)$	
	3	$(1, v_1 + z_1, 2 + v_1 + v_2 + x_2, 2 - y_3, 2 + v_1)$	
	4	$(-1, -v_2 - z_1, -2 - v_1 - v_2 - x_1, -2 - y_4, -2 - v_2)$	
	5	$(1, -1 + v_2 + w_2, x_3, -v_1 + v_2 + y_1, v_2)$	
	6	$(-1, 1 - v_1 - w_2, -x_4, -v_1 + v_2 + y_2, -v_1)$	
	7	$(1, -v_2 + z_2, 2 - v_1 - v_2 + x_4, 2 + v_1 - v_2 + y_3, 2 - v_2)$	
	8	$(-1, v_1 - z_2, -2 + v_1 + v_2 - x_3, -2 + v_1 - v_2 + y_4, -2 + v_1)$	
order		$v_1 \to v_2 \to w_1 \to w_2 \to x_1 \to x_2 \to x_3 \to x_4 \to y_1 \to y_2 \to y_3 \to y_4 \to z_1 \to z_2$	
$a, b - c \in N_2$, $c, d, c - d \notin N_2$	1	$(-1 - v_1, 1 - w_1, -v_1 - w_1, x_1 - w_1, y_1)$	12
	2	$(1 + v_2, -1 + w_1, v_2 + w_1, -x_1 + w_1, -y_1)$	
	3	$(1 + v_1, 2 - y_2, 3 + v_1 - y_2, -x_1 + w_1, 2 + v_1 + v_2 + y_1)$	
	4	$(-1 - v_2, -2 + y_2, -3 - v_2 + y_2, x_1 - w_1, -2 - v_1 - v_2 - y_1)$	
	5	$(-1 + v_2, 1 - w_2, v_2 - w_2, x_2 - w_2, -1 + v_1 + v_2 - w_2 + y_1 + y_2)$	
	6	$(1 - v_1, -1 + w_2, -v_1 + w_2, -x_2 + w_2, 1 - v_1 - v_2 + w_2 - y_1 - y_2)$	
	7	$(1 - v_2, -w_1 - w_2 + y_2, 1 - v_2 + y_2 - w_1 - w_2, -x_2 + w_2, 1 - w_2 + y_1 + y_2)$	
	8	$(-1 + v_1, w_1 + w_2 - y_2, -1 + v_1 - y_2 + w_1 + w_2, x_2 - w_2, -1 + w_2 - y_1 - y_2)$	
order		$w_2 \to w_1 \to v_1 \to v_2 \to y_2 \to y_1 \to x_1 \to x_2$	
$a, d \in N_2$, $b, c, c - b \notin N_2$	1	$(-1, 1 + v_1 - w_1, v_1 - x_1, v_1, -x_2)$	8
	2	$(3 + v_2 - x_1, 1 - x_1 + w_1, 2, 2 - x_1, -x_2 - 2v_1 - v_2 + x_1)$	
	3	$(-1 - v_2 + x_1, -v_1 - v_2 + x_1 - w_2, 0, -2 - v_1 - v_2 + x_1, x_2 + v_1 - x_1)$	
	4	$(-1 - v_2, -2 + w_2, -2 - v_1 - v_2 + x_1, 0, x_2 + v_1)$	
	5	$(-1, 1 + v_3 - w_3, v_3 - x_3, v_3, -x_4)$	
	6	$(3 + v_4 - x_3, 1 - x_3 + w_3, 2, 2 - x_3, -x_4 - 2v_3 - v_4 + x_3)$	
	7	$(-1 - v_4 + x_3, -v_3 - v_4 + x_3 - w_4, 0, -2 - v_3 - v_4 + x_3, x_4 + v_3 - x_3)$	
	8	$(-1 - v_4, -2 + w_4, -2 - v_3 - v_4 + x_3, 0, x_4 + v_3)$	
order		$v_1 \to v_2 \to x_1 \to x_2 \to w_1 \to w_2 \to v_3 \to v_4 \to x_3 \to x_4 \to w_3 \to w_4$	
$a \in N_2, b, c, d \notin N_2$, $b - c, c - d, b - d \notin N_2$	1	$(1, -1 - v_1 + w_1, x_1 - v_1, -v_1 + y_1, -v_1)$	6
	2	$(-1, 1 + v_2 - w_1, -x_1 + v_2, v_2 - y_1, v_2)$	
	3	$(1, v_1 + z_1, v_1 - x_2, -v_2 + y_1, 2 + v_1)$	
	4	$(-1, -v_2 - z_1, -v_2 + x_2, v_1 - y_1, -2 - v_2)$	
	5	$(1, -1 + v_2 + w_2, v_2 - x_2, v_2 + y_2, v_2)$	
	6	$(-1, 1 - v_1 - w_2, -v_1 + x_2, -v_1 - y_2, -v_1)$	
	7	$(1, -v_2 + z_2, 2 + v_1 - x_1, v_1 + y_2, 2 - v_2)$	
	8	$(-1, v_1 - z_2, -2 - v_2 + x_1, -v_2 - y_2, -2 + v_1)$	
order		$v_1 \to v_2 \to y_1 \to y_2 \to x_1 \to x_2 \to w_1 \to w_2 \to z_1 \to z_2$	
$a, b, d - c \in N_2$, $c \notin N_2$,	1	$(1, -1 - v_1 + w_1, x_1, y_1, -v_1)$	12
	2	$(-1, 1 + v_2 - w_1, -x_2, -y_1, v_2)$	
	3	$(1, v_1 + w_2, 2 + v_1 + v_2 + x_2, -1 + w_1 + w_2 - y_1, 2 + v_1)$	
	4	$(-1, -v_2 - w_2, -2 - v_1 - v_2 - x_1, 1 - w_1 - w_2 + y_1, -2 - v_2)$	
	5	$(1, 5 + v_2 - w_1 - w_2 - w_3 + 2y_1 + 2y_2, -x_1 + y_1 + y_2, y_2, v_2)$	
	6	$(-1, -5 - v_1 + w_1 + w_2 + w_3 - 2y_1 - 2y_2, x_2 - y_1 - y_2, -y_2, -v_1)$	
	7	$(1, -v_2 + w_3, 2 - v_1 - v_2 - x_2 + y_1 + y_2, 5 - w_1 - w_2 + 2y_1 + y_2, 2 - v_2)$	
	8	$(-1, v_1 - w_3, -2 + v_1 + v_2 + x_1 - y_1 - y_2, -5 + w_1 + w_2 - 2y_1 - y_2, -2 + v_1)$	
order		$y_1 \to y_2 \to v_1 \to v_2 \to w_1 \to w_2 \to w_3 \to x_1 \to x_2$	
$a, b, c, d \in N_2$,		$(0, v_j, w_j, x_j, y_j)$, $1 \le j \le 8$	4
order		$v_1 \to w_1 \to x_1 \to y_1 \to v_2 \to \cdots \to y_8$	
$a, b, c, d \notin N_2$, $a - b, a - c, a - d \notin N_2$, $b - c, b - d, c - d \notin N_2$	o	$(0, v_j, w_j, x_j, y_j)$	4
	e	$(0, -v_{j-1}, -w_{j-1}, -x_{j-1}, y_{j-1})$	
order		$v_1 \to w_1 \to x_1 \to y_1 \to v_3 \to \cdots \to y_7$	

Chapter 5

Cyclic relative difference families with variable blocksize

In this chapter, we present a new construction method of optimal optical orthogonal codes with $\lambda_c = 1$ including an already known constructions of OOCs. Our construction is based on the concept of "cyclic relative difference families with variable blocksize."

A family of s k_i-subsets A_i, $1 \leq i \leq s$, of $\mathbb{Z}_{nv}$ is called a *cyclic* $(nv, n, \{k_i \,|\, 1 \leq i \leq s\}, \lambda)$ *relative difference family with variable blocksize*, briefly denoted by $(nv, n, \{k_i \,|\, 1 \leq i \leq s\}, \lambda)$-CDF, if the list

$$\{b - a \,|\, a, b \in A_i; 1 \leq i \leq s\}$$

contains every element of $\mathbb{Z}_{nv} \setminus v\mathbb{Z}_{nv}$ exactly λ times but no element of $v\mathbb{Z}_{nv}$.

We can define relative difference families with variable blocksize in any finite group, but we restrict ourselves to cyclic groups because of our applications. Relative difference families with variable blocksize for $n = 1$ (defined in a general group) were treated in many papers under the motivation for constructing *Hadamard matrices*, for example, see [104, 115, 116]. Recently, Ding [47] showed that there exists a $(\frac{q^m-1}{n}, 1, \{k_i \,|\, 1 \leq i \leq q\}, \frac{q^{m-1}-1}{n})$-CDF for a prime power q and for positive integers m and n such that $\gcd(n, m) = 1$ and $n \,|\, q-1$, where each k_i is bounded as

$$\frac{q^{m-1} - nq^{\frac{m}{2}} - 1}{n} \leq k_i \leq \frac{q^{m-1} + nq^{\frac{m}{2}} - 1}{n} \tag{5.1}$$

for any i. For $n > 1$ a quite general recursive construction of such difference families is known [118, 119]. However, there are only a few known direct constructions for $n > 1$ even if the cyclic case.

Section 5.1 is devoted to providing some fundamental facts on characters over finite fields used in this chapter. In Sections 5.2 and 5.3, we provide a new construction of cyclic relative difference families with variable blocksize by modifying Ding's construction [47] and improve the bound (5.1) given by Ding [47]. Finally, in Section 5.4, we obtain a new infinite series of optimal $(v, k, 1, 1)$-OOCs as a corollary of results in the previous sections.

5.1 Group characters and basic lemmas

For a prime p and a positive integer r, let $q = p^r$. Let $\mathrm{Tr}_{\mathbb{F}_q}$ and $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ denote the absolute trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ and the relative trace from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$, respectively. *An additive character* of $\mathbb{F}_q$ is a nonzero function χ from $\mathbb{F}_q$ to the set of nonzero complex numbers such that $\chi(x+y) = \chi(x)\chi(y)$ for any pair (x, y) of $\mathbb{F}_q$. For each $b \in \mathbb{F}_q$, the function

$$\chi_b(c) = e^{\frac{2\pi\sqrt{-1}\mathrm{Tr}_{\mathbb{F}_q}(bc)}{p}} \text{ for any } c \in \mathbb{F}_q$$

defines an additive character of $\mathbb{F}_q$. χ_0 is called the *trivial* additive character of $\mathbb{F}_q$, which satisfies $\chi_0(c) = 1$ for any $c \in \mathbb{F}_q$. The additive character χ_1 of $\mathbb{F}_q$ is called *canonical*.

A multiplicative character of $\mathbb{F}_q$ is a function λ from $\mathbb{F}_q^\times$ to the set of complex numbers such that $\lambda(xy) = \lambda(x)\lambda(y)$ for $(x, y) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times$. For each $j = 0, 1, \ldots, q-2$, the function λ_j with

$$\lambda_j(\alpha^h) = e^{\frac{2\pi\sqrt{-1}jh}{q-1}} \text{ for } h = 0, 1, \ldots, q-2$$

defines a multiplicative character of $\mathbb{F}_q$, where α is a fixed primitive root of $\mathbb{F}_q$. It is obvious that the multiplicative characters of $\mathbb{F}_q$ form a cyclic group of order $q-1$, called the *character group* of $\mathbb{F}_q$, that is isomorphic to the multiplicative group of $\mathbb{F}_q$. This means that any multiplicative character can be expressed as $\lambda = \lambda_1^j$ for some j. The multiplicative character λ_0 of $\mathbb{F}_q$ is called *trivial*, which satisfies that $\lambda_0(c) = 1$ for $c \in \mathbb{F}_q^\times$. For each character λ, the *conjugate* character $\bar{\lambda}$ is defined by $\bar{\lambda}(x) = \overline{\lambda(x)}$ for all $x \in \mathbb{F}_q^\times$, where $\overline{\lambda(x)}$ means the complex conjugate of $\lambda(x)$. Furthermore, we extend the domain of a multiplicative character to all elements of $\mathbb{F}_q$ as $\lambda_j(0) = 0$ for all $j \neq 0$ and $\lambda_0(0) = 1$.

Let λ be a multiplicative and χ an additive character of $\mathbb{F}_q$. Then the sum $G(\lambda, \chi) = \sum_{c \in \mathbb{F}_q^\times} \lambda(c)\chi(c)$ is called *the Gaussian sum*. It is well known [76] that

$$G(\lambda, \chi) = \begin{cases} q-1 & \text{if } \lambda = \lambda_0,\ \chi = \chi_0, \\ -1 & \text{if } \lambda = \lambda_0,\ \chi \neq \chi_0, \\ 0 & \text{if } \lambda \neq \lambda_0,\ \chi = \chi_0 \end{cases} \tag{5.2}$$

holds. If $\lambda \neq \lambda_0$ and $\chi \neq \chi_0$, it holds that

$$|G(\lambda, \chi)| = q^{1/2}. \tag{5.3}$$

Let χ' be an additive and λ' a multiplicative character in $\mathbb{F}_q$. Then χ' and λ' can be "lifted" to the extension field $\mathbb{F}_{q^m}$ by setting $\chi(\beta) = \chi'(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta))$ for $\beta \in \mathbb{F}_{q^m}$ and $\lambda(\beta) = \lambda'(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta))$ for $\beta \in \mathbb{F}_{q^m}^\times$, where $\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}$ is a relative norm from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$. It is clear that χ is an additive and λ a multiplicative character of $\mathbb{F}_{q^m}$. The following theorem known as Davenport-Hasse Theorem establishes an important relationship between $G(\lambda', \chi')$ in $\mathbb{F}_q$ and $G(\lambda, \chi)$ in $\mathbb{F}_{q^m}$.

Theorem 5.1.1. (Theorem 5.14 in [76]) Let χ' be an additive and λ' a multiplicative character of $\mathbb{F}_q$, not both of them trivial. Suppose that χ' and λ' are lifted to characters χ and λ, respectively, of the extension field $\mathbb{F}_{q^m}$. Then, it holds that

$$G(\lambda, \chi) = (-1)^{m-1} G(\lambda', \chi')^m.$$

Let $\lambda_1, \ldots, \lambda_t$ be multiplicative characters of $\mathbb{F}_q$. Then the sum

$$J(\lambda_1, \ldots, \lambda_t) = \sum_{c_1+\cdots+c_t=1} \lambda_1(c_1) \cdots \lambda_t(c_t)$$

is called a *Jacobi sum* in $\mathbb{F}_q$. The following theorems show relationships between Gaussian sums and Jacobi sums.

Theorem 5.1.2. (Theorem 5.21 in [76]) Let $\lambda_1, \ldots, \lambda_t$ be nontrivial multiplicative characters of $\mathbb{F}_q$ and χ be a nontrivial additive character of $\mathbb{F}_q$. If $\lambda_1 \cdots \lambda_t$ is trivial, then it holds that

$$J(\lambda_1, \ldots, \lambda_t) = -\frac{1}{q} G(\lambda_1, \chi) \cdots G(\lambda_t, \chi). \tag{5.4}$$

Whereas if $\lambda_1 \cdots \lambda_t$ is nontrivial, then

$$J(\lambda_1, \ldots, \lambda_t) = \frac{G(\lambda_1, \chi) \cdots G(\lambda_t, \chi)}{G(\lambda_1 \cdots \lambda_t, \chi)} \tag{5.5}$$

holds.

Theorem 5.1.3. (Theorem 5.27 in [76]) Let λ be a multiplicative character of $\mathbb{F}_q$ of order $n \geq 2$ and χ be a nontrivial additive character of $\mathbb{F}_q$. Then it holds that

$$G(\lambda, \chi)^n = \lambda(-1) q J(\lambda, \lambda) J(\lambda, \lambda^2) \cdots J(\lambda, \lambda^{n-2}).$$

Further basic properties of Gaussian sums and Jacobi sums are referred to [76].

Theorem 5.1.4. (Theorem 5.30 in [76]) Let χ be a nontrivial additive character of $\mathbb{F}_q$, $n \in \mathbb{N}$, and λ be a multiplicative character of order $d = \gcd(n, q-1)$ of $\mathbb{F}_q$. Then,

$$\sum_{c \in \mathbb{F}_q} \chi(ac^n + b) = \chi(b) \sum_{j=1}^{d-1} \bar{\lambda}^j(a) G(\lambda^j, \chi)$$

holds for any $a, b \in \mathbb{F}_q$ with $a \neq 0$.

From now on, we denote the canonical additive characters of $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$ by χ and χ', respectively. The following was proved in Theorem 9 of [47].

Lemma 5.1.5. ([47]) Let n and m be positive integers such that $n \mid q-1$ and $\gcd(n, m) = 1$. Then,

$$\sum_{b \in \mathbb{F}_{q^m}} \sum_{c \in \mathbb{F}_q} \chi(b^n c x) = q^m$$

holds for any $x \in \mathbb{F}_{q^m}^{\times}$.

To prove our main theorem, we use the following:

Lemma 5.1.6. Let λ be a multiplicative character of $\mathbb{F}_{q^m}$ of order n. If $n \mid q-1$ and $\gcd(n, m) = 1$, $\sum_{d \in \mathbb{F}_q^{\times}} \lambda^j(d) = 0$ holds for every $1 \leq j \leq n-1$.

Proof: By the assumptions $q \equiv 1 \pmod{n}$ and $\gcd(n, m) = 1$, it is easy to see that the restriction of λ to the subfield $\mathbb{F}_q$ of $\mathbb{F}_{q^m}$ is also a multiplicative character of order n. Hence, by using (5.2) with $\chi = \chi_0$, we get our assertion. □

Lemma 5.1.7. Let n and m be positive integers such that $n \mid q-1$ and $\gcd(n, m) = 1$. Then

$$\sum_{b\in\mathbb{F}_{q^m}} \sum_{c\in\mathbb{F}_q} \sum_{d\in\mathbb{F}_q} \chi(b^n(c+dx)) = \begin{cases} q^{m+1} & \text{if } x \in \mathbb{F}_q^\times, \\ q^m & \text{if } x \notin \mathbb{F}_q. \end{cases}$$

Proof: If $x \in \mathbb{F}_q^\times$, by Lemma 5.1.5, we have

$$\sum_{b\in\mathbb{F}_{q^m}} \sum_{c\in\mathbb{F}_q} \sum_{d\in\mathbb{F}_q} \chi(b^n(c+dx)) = q \sum_{b\in\mathbb{F}_{q^m}} \sum_{c\in\mathbb{F}_q} \chi(b^n c) = q^{m+1}.$$

If $x \notin \mathbb{F}_q$, it is obvious that $c + dx = 0$ if and only if $(c, d) = (0, 0)$. Then, by Theorem 5.1.4, we have

$$\begin{aligned} \sum_{b\in\mathbb{F}_{q^m}} \sum_{c\in\mathbb{F}_q} \sum_{d\in\mathbb{F}_q} \chi(b^n(c+dx)) &= \sum_{b\in\mathbb{F}_{q^m}} \sum_{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q\setminus\{(0,0)\}} \chi(b^n(c+dx)) + \sum_{b\in\mathbb{F}_{q^m}} \chi(0) \\ &= \sum_{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q\setminus\{(0,0)\}} \sum_{j=1}^{n-1} \bar{\lambda}^j(c+dx) G(\lambda^j, \chi) + q^m. \end{aligned}$$

Noting that $\lambda(0) = 0$ and $\sum_{d\in\mathbb{F}_q^\times} \lambda(d) = 0$ for any nontrivial character λ of $\mathbb{F}_{q^m}$ by Lemma 5.1.6, we have

$$\begin{aligned} \sum_{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q\setminus\{(0,0)\}} \bar{\lambda}^j(c+dx) &= \sum_{c\in\mathbb{F}_q} \sum_{d\in\mathbb{F}_q^\times} \bar{\lambda}^j(c+dx)\bar{\lambda}^j(d)\bar{\lambda}^j(d^{-1}) \\ &= \sum_{c\in\mathbb{F}_q} \sum_{d\in\mathbb{F}_q^\times} \bar{\lambda}^j(d)\bar{\lambda}^j(cd^{-1}+x) \\ &= \sum_{d\in\mathbb{F}_q^\times} \bar{\lambda}^j(d) \sum_{c\in\mathbb{F}_q} \bar{\lambda}^j(c+x) = 0, \end{aligned}$$

which gives our assertion. □

5.2 Construction of cyclic relative difference families with variable blocksize

Let q be a prime power and let n and m be positive integers such that $\gcd(n, m) = 1$ and $n \mid q-1$. Define $D_i = \{a \mid \mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(a) = i; a \in \mathbb{F}_{q^m}\}$ for $i \in \mathbb{F}_q$, and let N be the set of nth powers of $\mathbb{F}_{q^m}^\times$. Let α be a primitive root of $\mathbb{F}_{q^m}$ and let $\log_{\alpha^n} : N \to \mathbb{Z}_{(q^m-1)/n}$ be the logarithm function. For $i \in \mathbb{F}_q$, put

$$E_i = \log_{\alpha^n}(D_i \cap N). \tag{5.6}$$

Let A be a subset of $\mathbb{F}_{q^m}$. A characteristic function of A is a function f_A from $\mathbb{F}_{q^m}$ to $\mathbb{Z}$ defined by

$$f_A(x) = \begin{cases} 1 & \text{if } x \in A, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma 5.2.1. Let $\zeta_p = e^{2\pi\sqrt{-1}/p}$. Then the characteristic function of D_i is given by

$$f_{D_i}(x) = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q}(c(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)-i))}.$$

Proof: If $x \in D_i$, i.e., $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) = i$, we have

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q}(c(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)-i))} = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q}(0)} = 1.$$

If $x \notin D_i$, i.e., $\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x) - i = s \neq 0$, we have

$$\frac{1}{q} \sum_{c \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q}(c(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(x)-i))} = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q}(cs)} = \frac{1}{q} \sum_{c \in \mathbb{F}_q} \chi'(cs) = 0.$$

□

Theorem 5.2.2. Let e be a positive integer such that $\gcd(e, n) = 1$. Let S be the set of eth powers of $\mathbb{F}_q$. Then, the family $\{E_i \mid i \in S\}$ is a $(\frac{q^m-1}{n}, \frac{q-1}{n}, \{k_i \mid 1 \leq i \leq \frac{q-1}{e}\}, \frac{q^{m-2}(q-1)}{en})$-CDF.

Proof: Let ℓ be a fixed nonzero element of $\mathbb{Z}_{(q^m-1)/n}$. Then, it is clear that the number of $a \in \mathbb{Z}_{(q^m-1)/n}$ such that $a \in E_i$ and $b = a - \ell \in E_i$ for all $i \in S$, i.e., ℓ occurs as a difference $a - (a - \ell)$, is given by

$$\sum_{i \in S} \sum_{a=0}^{\frac{q^m-1}{n}-1} f_{D_i}(\alpha^{na}) f_{D_i}(\alpha^{na-n\ell}). \tag{5.7}$$

In this proof, we show the following:

$$\sum_{i \in S} \sum_{a=0}^{\frac{q^m-1}{n}-1} f_{D_i}(\alpha^{na}) f_{D_i}(\alpha^{na-n\ell}) = \begin{cases} 0 & \text{if } \alpha^{-n\ell} \in \mathbb{F}_q, \\ \frac{q^{m-2}(q-1)}{en} & \text{if } \alpha^{-n\ell} \notin \mathbb{F}_q. \end{cases} \tag{5.8}$$

Again, let $\zeta_p = e^{2\pi\sqrt{-1}/p}$. Now, by using Lemma 5.2.1, the left-hand side of (5.8) is equal to

$$\begin{aligned}
& \frac{1}{q^2} \sum_{i \in S} \sum_{a=0}^{\frac{q^m-1}{n}-1} \sum_{c \in \mathbb{F}_q} \sum_{d \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q}(c(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{na})-i))} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q}(d(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{na-n\ell})-i))} \\
= & \frac{1}{q^2} \sum_{i \in S} \sum_{a=0}^{\frac{q^m-1}{n}-1} \sum_{c \in \mathbb{F}_q} \sum_{d \in \mathbb{F}_q} \chi(c\alpha^{na}) \chi'(-ic) \chi(d\alpha^{na-n\ell}) \chi'(-id) \\
= & \frac{1}{q^2} \sum_{i \in S} \sum_{a=0}^{\frac{q^m-1}{n}-1} \sum_{c \in \mathbb{F}_q} \sum_{d \in \mathbb{F}_q} \chi(\alpha^{na}(c + d\alpha^{-n\ell})) \chi'(-i(c+d)) \\
= & \frac{1}{enq^2} \sum_{i \in \mathbb{F}_q^\times} \sum_{b \in \mathbb{F}_{q^m}^\times} \sum_{c \in \mathbb{F}_q} \sum_{d \in \mathbb{F}_q} \chi(b^n(c + d\alpha^{-n\ell})) \chi'(-i^e(c+d))
\end{aligned}$$

$$
\begin{aligned}
&= \frac{1}{enq^2}\sum_{i\in\mathbb{F}_q^\times}\sum_{b\in\mathbb{F}_{q^m}^\times}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d))\\
&\quad+\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q^\times}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(0\cdot(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d))\\
&\quad-\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q^\times}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(0\cdot(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d))\\
&= \frac{1}{enq^2}\sum_{i\in\mathbb{F}_q^\times}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d))\\
&= \frac{1}{enq^2}\sum_{i\in\mathbb{F}_q^\times}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d))\\
&\quad+\frac{1}{enq^2}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(0\cdot(c+d))\\
&\quad-\frac{1}{enq^2}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(0\cdot(c+d))\\
&= \frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d))\\
&\quad-\frac{1}{enq^2}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell})).
\end{aligned}
$$

Note that, by Lemma 5.1.7, we have

$$
\frac{1}{enq^2}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell}))=\begin{cases}\frac{q^{m-1}}{en} & \text{if } \alpha^{-n\ell}\in\mathbb{F}_q^\times,\\ \frac{q^{m-2}}{en} & \text{if } \alpha^{-n\ell}\notin\mathbb{F}_q.\end{cases}
$$

Let

$$
\begin{aligned}
W_\ell &= \{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q \mid c+d\alpha^{-n\ell}=0\},\\
X &= \{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q \mid c+d=0\},\\
Y_\ell &= \{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q \mid c+d\alpha^{-n\ell}=0 \text{ and } c+d=0\},\\
Z_\ell &= \{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q \mid c+d\alpha^{-n\ell}=0 \text{ or } c+d=0\}.
\end{aligned}
$$

Then we have

$$
\begin{aligned}
&\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{(c,d)\in W_\ell}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d))\\
=\ &\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{(c,d)\in W_\ell}\chi'(-i^e(c+d))\\
=\ &\begin{cases}\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{d\in\mathbb{F}_q}\chi'(-i^e d(1-\alpha^{-n\ell})) & \text{if } \alpha^{-n\ell}\in\mathbb{F}_q,\\ \frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\chi'(0) & \text{if } \alpha^{-n\ell}\notin\mathbb{F}_q,\end{cases}
\end{aligned}
$$

$$
\begin{aligned}
&= \begin{cases} \frac{1}{enq^2}\sum_{b\in\mathbb{F}_{q^m}}\sum_{d\in\mathbb{F}_q}\chi'(0) & \text{if } \alpha^{-n\ell}\in\mathbb{F}_q, \\ \frac{q^{m-1}}{en} & \text{if } \alpha^{-n\ell}\notin\mathbb{F}_q, \end{cases} \\
&= \frac{q^{m-1}}{en}
\end{aligned}
$$

since $1-\alpha^{-n\ell}\neq 0$ for any $1\leq \ell < \frac{q^m-1}{n}$. Furthermore, by Lemma 5.1.5, we have

$$
\begin{aligned}
&\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{(c,d)\in X\setminus Y_\ell}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d)) \\
&= \frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{d\in\mathbb{F}_q}\chi(b^n d(-1+\alpha^{-n\ell})) - \frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\chi(0) \\
&= \frac{1}{enq}\sum_{b\in\mathbb{F}_{q^m}}\sum_{d\in\mathbb{F}_q}\chi(b^n d(-1+\alpha^{-n\ell})) - \frac{q^{m-1}}{en} \\
&= 0.
\end{aligned}
$$

Thus, it follows that

$$
\begin{aligned}
&\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d)) \\
&= \frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q\setminus Z_\ell}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d)) + \frac{q^{m-1}}{en}.
\end{aligned}
$$

Now let λ and ϕ be multiplicative characters of order n of $\mathbb{F}_{q^m}$ and of order e of $\mathbb{F}_q$, respectively. Applying Theorem 5.1.4, we get

$$
\begin{aligned}
&\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q\setminus Z_\ell}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d)) \\
&= \frac{1}{enq^2}\sum_{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q\setminus Z_\ell}\sum_{s=1}^{n-1}\sum_{t=1}^{e-1}\bar{\lambda}^s(c+d\alpha^{-n\ell})\bar{\phi}^t(-(c+d))G(\lambda^s,\chi)G(\phi^t,\chi') \\
&= \frac{1}{enq^2}\sum_{s=1}^{n-1}\sum_{t=1}^{e-1}G(\lambda^s,\chi)G(\phi^t,\chi')\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\bar{\lambda}^s(c+d\alpha^{-n\ell})\bar{\phi}^t(-(c+d))
\end{aligned}
$$

since $\bar{\lambda}^s(c+d\alpha^{-n\ell})\bar{\phi}^t(-(c+d))=0$ for all $(c,d)\in Z_\ell$. Especially, we have

$$
\begin{aligned}
&\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\bar{\lambda}^s(c+d\alpha^{-n\ell})\bar{\phi}^t(-(c+d)) \\
&= \sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q^\times}\bar{\lambda}^s(c+d\alpha^{-n\ell})\bar{\phi}^t(-(c+d)) + \sum_{c\in\mathbb{F}_q}\bar{\lambda}^s(c)\bar{\phi}^t(-c) \\
&= \sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q^\times}\bar{\lambda}^s(d)\bar{\lambda}^s(d^{-1})\bar{\phi}^t(d)\bar{\phi}^t(d^{-1})\bar{\lambda}^s(c+d\alpha^{-n\ell})\bar{\phi}^t(-(c+d)) + \sum_{c\in\mathbb{F}_q}\bar{\lambda}^s(c)\bar{\phi}^t(-c)
\end{aligned}
$$

$$= \sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q^\times}\bar{\lambda}^s(d)\bar{\phi}^t(d)\bar{\lambda}^s(cd^{-1}+\alpha^{-n\ell})\bar{\phi}^t(-cd^{-1}-1)+\sum_{c\in\mathbb{F}_q}\bar{\lambda}^s(c)\bar{\phi}^t(-c)$$
$$= (\sum_{d\in\mathbb{F}_q^\times}\bar{\lambda}^s(d)\bar{\phi}^t(d))(\sum_{c\in\mathbb{F}_q}\bar{\lambda}^s(c+\alpha^{-n\ell})\bar{\phi}^t(-c-1))+\sum_{c\in\mathbb{F}_q}\bar{\lambda}^s(c)\bar{\phi}^t(-c).$$

By the assumptions $n\,|\,q-1$ and $\gcd(n,m)=1$, the restriction λ' of λ to $\mathbb{F}_q$ is a multiplicative character of order n. Furthermore, since $\gcd(e,n)=1$, we have

$$\sum_{d\in\mathbb{F}_q^\times}\bar{\lambda}^s(d)\bar{\phi}^t(d)=\sum_{d\in\mathbb{F}_q^\times}\bar{\lambda'}^s(d)\bar{\phi}^t(d)=\sum_{d\in\mathbb{F}_q^\times}\bar{\psi}^{es}(d)\bar{\psi}^{nt}(d)=\sum_{h=0}^{q-2}\zeta_{en}^{-(es+nt)h}=0,$$

where ψ is a multiplicative character of order en of $\mathbb{F}_q$ and ζ_{en} is a primitive enth root of unity. This implies that

$$\frac{1}{enq^2}\sum_{i\in\mathbb{F}_q}\sum_{b\in\mathbb{F}_{q^m}}\sum_{(c,d)\in\mathbb{F}_q\times\mathbb{F}_q\setminus Z_\ell}\chi(b^n(c+d\alpha^{-n\ell}))\chi'(-i^e(c+d))=0. \tag{5.9}$$

Therefore, we get

$$\sum_{i\in S}\sum_{a=0}^{\frac{q^m-1}{n}-1}f_{D_i}(\alpha^{na})f_{D_i}(\alpha^{na-n\ell})=\begin{cases}0 & \text{if } \alpha^{-n\ell}\in\mathbb{F}_q,\\ \frac{q^{m-2}(q-1)}{en} & \text{if } \alpha^{-n\ell}\notin\mathbb{F}_q,\end{cases}$$

which shows our assertion. □

5.3 Improvement of a bound on blocksize

In [47], the following bound for k_i's was given by applying *the theorem of Weil* on additive character sums.

Lemma 5.3.1. ([47]) Let n and m be positive integers such that $n\,|\,q-1$ and $\gcd(n,m)=1$. Put $k_i=|E_i|$ for $i\in\mathbb{F}_q$, where E_i is defined in (5.6). Then,

$$\frac{q^{m-1}-nq^{\frac{m}{2}}-1}{n}\le k_i\le\frac{q^{m-1}+nq^{\frac{m}{2}}-1}{n}$$

holds for any $i\in\mathbb{F}_q$.

Now, we improve the bound of Lemma 5.3.1.

Lemma 5.3.2. Let n, m, and k_i's be the same with Lemma 5.3.1. Then, it holds that $k_0=\frac{q^{m-1}-1}{n}$ and

$$\frac{q^{m-1}-(n-1)q^{\frac{m-1}{2}}}{n}\le k_i\le\frac{q^{m-1}+(n-1)q^{\frac{m-1}{2}}}{n} \tag{5.10}$$

for any $i\in\mathbb{F}_q^\times$.

Proof: The size of each E_i, $i \in \mathbb{F}_q$, is given by

$$\begin{aligned}
&\sum_{a=0}^{\frac{q^m-1}{n}-1} f_{D_i}(\alpha^{na}) \qquad (5.11)\\
&= \frac{1}{q}\sum_{a=0}^{\frac{q^m-1}{n}-1}\sum_{c\in\mathbb{F}_q} \zeta_p^{\mathrm{Tr}_{\mathbb{F}_q}(c(\mathrm{Tr}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\alpha^{na})-i))}\\
&= \frac{1}{q}\sum_{a=0}^{\frac{q^m-1}{n}-1}\sum_{c\in\mathbb{F}_q} \chi(c\alpha^{na})\chi'(-ic)\\
&= \frac{1}{nq}\sum_{b\in\mathbb{F}_{q^m}^\times}\sum_{c\in\mathbb{F}_q}\chi(b^n c)\chi'(-ic) + \frac{1}{nq}\sum_{c\in\mathbb{F}_q}\chi(0)\chi'(-ic) - \frac{1}{nq}\sum_{c\in\mathbb{F}_q}\chi(0)\chi'(-ic).
\end{aligned}$$

When $i = 0$, using Lemma 5.1.5, we have

$$\begin{aligned}
&\frac{1}{nq}\sum_{b\in\mathbb{F}_{q^m}^\times}\sum_{c\in\mathbb{F}_q}\chi(b^n c)\chi'(0) + \frac{1}{nq}\sum_{c\in\mathbb{F}_q}\chi(0)\chi'(0) - \frac{1}{nq}\sum_{c\in\mathbb{F}_q}\chi(0)\chi'(0)\\
&= \frac{1}{nq}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\chi(b^n c) - \frac{1}{n} = \frac{q^{m-1}-1}{n}.
\end{aligned}$$

When $i \neq 0$, using Theorem 5.1.4 and $\frac{1}{nq}\sum_{c\in\mathbb{F}_q}\chi(0)\chi'(-ic) = 0$, we have

$$\begin{aligned}
\sum_{a=0}^{\frac{q^m-1}{n}-1} f_{D_i}(\alpha^{na}) &= \frac{1}{nq}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q}\chi(b^n c)\chi'(-ic)\\
&= \frac{1}{nq}\sum_{b\in\mathbb{F}_{q^m}}\sum_{c\in\mathbb{F}_q^\times}\chi(b^n c)\chi'(-ic) + \frac{q^{m-1}}{n}\\
&= \frac{1}{nq}\sum_{j=1}^{n-1}\sum_{c\in\mathbb{F}_q^\times}\bar{\lambda}^j(c)\chi'(-ic)G(\lambda^j,\chi) + \frac{q^{m-1}}{n}\\
&= \frac{1}{nq}\sum_{j=1}^{n-1}\sum_{c\in\mathbb{F}_q^\times}\lambda'^{-j}(c)\lambda'^{-j}(-i)\lambda'^{j}(-i)\chi'(-ic)G(\lambda^j,\chi) + \frac{q^{m-1}}{n}\\
&= \frac{1}{nq}\sum_{j=1}^{n-1}\lambda'^{j}(-i)\sum_{c\in\mathbb{F}_q^\times}\lambda'^{-j}(-ic)\chi'(-ic)G(\lambda^j,\chi) + \frac{q^{m-1}}{n}, \qquad (5.12)
\end{aligned}$$

where λ is a multiplicative character of $\mathbb{F}_{q^m}$ of order n and λ' is its restriction to $\mathbb{F}_q$. By noting $i \neq 0$, (5.12) is reformulated as

$$\frac{1}{nq}\sum_{j=1}^{n-1}\lambda'^{j}(-i)G(\lambda'^{-j},\chi')G(\lambda^j,\chi) + \frac{q^{m-1}}{n}. \qquad (5.13)$$

Then, by using (5.3), we have

$$\begin{aligned}|\frac{1}{nq}\sum_{j=1}^{n-1}\lambda'^{j}(-i)G(\lambda'^{-j},\chi')G(\lambda^{j},\chi)| &\leq \frac{1}{nq}\sum_{j=1}^{n-1}\left|G(\lambda'^{-j},\chi')G(\lambda^{j},\chi)\right| \\ &= \frac{1}{nq}\sum_{j=1}^{n-1}\left|G(\lambda'^{-j},\chi')\right|\cdot\left|G(\lambda^{j},\chi)\right| = \frac{(n-1)q^{\frac{m-1}{2}}}{n}.\end{aligned}$$

Thus, we get our assertion. □

Corollary 5.3.3. For the family $\{E_i \,|\, i \in S\}$ of Theorem 5.2.2, it holds

$$\sum_{i\in S} k_i = \frac{q^{m-1}(q-1)}{en}.$$

Proof: By (5.13), the sum of k_i's, $i \in S$, is given by the value

$$\begin{aligned}&\frac{1}{nq}\sum_{i\in S}\sum_{j=1}^{n-1}\lambda'^{j}(-i)G(\lambda'^{-j},\chi')G(\lambda^{j},\chi) + |S|\cdot\frac{q^{m-1}}{n} \\ =\ &\frac{1}{enq}\sum_{j=1}^{n-1}G(\lambda'^{-j},\chi')G(\lambda^{j},\chi)\sum_{i\in\mathbb{F}_q^\times}\lambda'^{j}(-i^e) + \frac{q^{m-1}(q-1)}{en}.\end{aligned}$$

Noting that λ'^{ej} is not a trivial character for any j, $1 \leq j \leq n-1$, we have

$$\sum_{i\in\mathbb{F}_q^\times}\lambda'^{j}(-i^e) = \sum_{i\in\mathbb{F}_q^\times}\lambda'^{ej}(-i) = 0,$$

which gives our assertion. □

It is quite hard to calculate the exact values of k_i's in general, however, when n is small, we can provide a useful representation of k_i's in terms of Jacobi sums. From now on, we use the notations in Theorem 5.2.2 and Lemma 5.3.2. The following lemma is necessary to give a representation of k_i's.

Lemma 5.3.4. (Exercise 5.28 in [76]) Let $\lambda_1, \ldots, \lambda_t$ be multiplicative characters of $\mathbb{F}_q$. If $\lambda_1 \cdots \lambda_t$ is trivial and λ_t is nontrivial, then it holds that

$$J(\lambda_1, \ldots, \lambda_t) = -\lambda_t(-1)J(\lambda_1, \ldots, \lambda_{t-1}).$$

Let h, $1 \leq h \leq m-1$, be a unique integer such that $mh \equiv 1 \pmod{n}$. Then,

$$\lambda'^{hj}(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_q}(\beta)) = \lambda'^{hj}(\beta^{\frac{q^m-1}{q-1}}) = \lambda'^{hj}(\alpha^{\ell\cdot\frac{q^m-1}{q-1}}) = \zeta_n^{hj\ell m} = \zeta_n^{j\ell} = \lambda^{j}(\beta)$$

holds for any $\beta = \alpha^\ell \in \mathbb{F}_{q^m}$, where ζ_n is a primitive nth root of unity such that $\lambda(\alpha) = \zeta_n$. This implies that the lifted character of λ'^{hj} is λ^j in $\mathbb{F}_{q^m}$. Hence, by using Theorem 5.1.1 and

(5.4) of Theorem 5.1.2, (5.13) is reformulated as

$$\begin{aligned}
&\frac{1}{nq}\sum_{j=1}^{n-1}\lambda'^{j}(-i)G(\lambda'^{-j},\chi')G(\lambda^{j},\chi)+\frac{q^{m-1}}{n}\\
=\;&\frac{(-1)^{m-1}}{nq}\sum_{j=1}^{n-1}\lambda'^{j}(-i)G(\lambda'^{-j},\chi')G(\lambda'^{hj},\chi')^{m}+\frac{q^{m-1}}{n}\\
=\;&\frac{(-1)^{m}}{n}\sum_{j=1}^{n-1}\lambda'^{j}(-i)J(\lambda'^{-j},\lambda'^{hj},\ldots,\lambda'^{hj})+\frac{q^{m-1}}{n}. \qquad (5.14)
\end{aligned}$$

Furthermore, by Lemmas 5.3.4, (5.14) is reformulated as

$$\begin{aligned}
&\frac{(-1)^{m+1}}{n}\sum_{j=1}^{n-1}\lambda'^{j}(-i)\lambda'^{-j}(-1)J(\lambda'^{hj},\ldots,\lambda'^{hj})+\frac{q^{m-1}}{n}\\
=\;&\frac{(-1)^{m+1}}{n}\sum_{j=1}^{n-1}\lambda'^{j}(i)J(\lambda'^{hj},\ldots,\lambda'^{hj})+\frac{q^{m-1}}{n}. \qquad (5.15)
\end{aligned}$$

Thus, we could represent each size k_i in terms of Jacobi sums. Especially, when $m=ns+1$ ($h=1$) or $ns-1$ ($h=m-1$), by combining (5.5) of Theorem 5.1.2 and Theorem 5.1.3 and by noting $G(\lambda'^{j},\chi')G(\lambda'^{-j},\chi')=\lambda'^{j}(-1)q$, (5.15) is equal to

$$\begin{aligned}
&\frac{(-1)^{m+1}}{n}\sum_{j=1}^{n-1}\lambda'^{j}(i)\frac{G(\lambda'^{hj},\chi')^{m}}{G(\lambda'^{hjm},\chi')}+\frac{q^{m-1}}{n}\\
=\;&\frac{(-1)^{m+1}}{n}\sum_{j=1}^{n-1}\lambda'^{j}(i)\frac{G(\lambda'^{hj},\chi')^{m}}{G(\lambda'^{j},\chi')}+\frac{q^{m-1}}{n}\\
=\;&\begin{cases}\frac{(-1)^{m+1}}{n}\sum_{j=1}^{n-1}\lambda'^{j}(i)G(\lambda'^{j},\chi')^{m-1}+\frac{q^{m-1}}{n} & \text{if } m=ns+1,\\ \frac{(-1)^{m+1}}{nq}\sum_{j=1}^{n-1}\lambda'^{j}(i)\lambda'^{j}(-1)G(\lambda'^{-j},\chi')^{m+1}+\frac{q^{m-1}}{n} & \text{if } m=ns-1,\end{cases}\\
=\;&\begin{cases}\frac{(-1)^{m+1}q^{s}}{n}\sum_{j=1}^{n-1}\lambda'^{j}(i)\lambda'^{sj}(-1)(J(\lambda'^{j},\lambda'^{j})\cdots J(\lambda'^{j},\lambda'^{(n-2)j}))^{s}+\frac{q^{m-1}}{n}\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } m=ns+1,\\ \frac{(-1)^{m+1}q^{s-1}}{n}\sum_{j=1}^{n-1}\lambda'^{j}(i)\lambda'^{-(s-1)j}(-1)(J(\lambda'^{-j},\lambda'^{-j})\cdots J(\lambda'^{-j},\lambda'^{-(n-2)j}))^{s}+\frac{q^{m-1}}{n}\\ \qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad \text{if } m=ns-1.\end{cases}
\end{aligned} \qquad (5.16)$$

Now we provide numerical results for $n=2$ and 3.

(**Case** $n=2$) We can assume that $m=2s+1$ and $h=1$. By Exercise 5.39 in [76], it holds that

$$J(\lambda',\ldots,\lambda')=(-1)^{(m-1)(q-1)/4}q^{(m-1)/2}.$$

Then, by (5.15), we have

$$k_i=\frac{q^{m-1}+\lambda'(i)(-1)^{s(q-1)/2}q^{(m-1)/2}}{2},$$

where $\lambda'(i)(-1)^{s(q-1)/2} = 1$ or -1. Hence, each k_i with $i \neq 0$ of Theorem 5.2.2 is $\frac{q^{m-1}+q^{\frac{m-1}{2}}}{2}$ or $\frac{q^{m-1}-q^{\frac{m-1}{2}}}{2}$.

(**Case** $n = 3$) When $n = 3$, it is known [64, 105] that $J(\lambda', \lambda')$ and $J(\lambda'^2, \lambda'^2)$ are written as $a + b\zeta_3$ and $a + b\zeta_3^2$, respectively, where $\zeta_3 = e^{2\pi i/3}$ and a and b are integers determined by

$$q = p^r = a^2 - ab + b^2,\ a \equiv -1 \,(\mathrm{mod}\ 3),\ b \equiv 0 \,(\mathrm{mod}\ 3),$$

where p is a prime such that

(i) if $p \equiv 2 \pmod 3$, then r is even and $a = \pm p^{r/2}$ and $b = 0$,

(ii) if $p \equiv 1 \pmod 3$, then $q = a^2 - ab + b^2$ is the unique representation of q such that $\gcd(2a - b, p) = 1$.

We can assume that $m = 3s+1$ ($h = 1$) or $m = 3s-1$ ($h = 2$). In the former case, by (5.16), we have

$$\begin{aligned}
k_i &= \frac{(-1)^{m+1}q^s}{3}(\lambda'(i)\lambda'^s(-1)J(\lambda', \lambda')^s + \lambda'^2(i)\lambda'^{2s}(-1)J(\lambda'^2, \lambda'^2)^s) + \frac{q^{m-1}}{3} \\
&= \frac{(-1)^{m+1}q^s}{3}(\lambda'(i)(a + b\zeta_3)^s + \lambda'^2(i)(a + b\zeta_3^2)^s) + \frac{q^{m-1}}{3} \\
&= \begin{cases} \frac{(-1)^{m+1}q^s}{3}((a + b\zeta_3)^s + (a + b\zeta_3^2)^s) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = 1, \\ \frac{(-1)^{m+1}q^s}{3}(\zeta_3(a + b\zeta_3)^s + \zeta_3^2(a + b\zeta_3^2)^s) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = \zeta_3, \\ \frac{(-1)^{m+1}q^s}{3}(\zeta_3^2(a + b\zeta_3)^s + \zeta_3(a + b\zeta_3^2)^s) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = \zeta_3^2, \end{cases} \\
&= \begin{cases} \frac{(-1)^{m+1}q^s}{3}(2\sum_{u\equiv 0 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u - \sum_{u\equiv 1,2 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = 1, \\ \frac{(-1)^{m+1}q^s}{3}(2\sum_{u\equiv 2 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u - \sum_{u\equiv 0,1 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = \zeta_3, \\ \frac{(-1)^{m+1}q^s}{3}(2\sum_{u\equiv 1 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u - \sum_{u\equiv 0,2 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = \zeta_3^2. \end{cases}
\end{aligned}$$

In the latter case, similar to the above, we have

$$\begin{aligned}
k_i &= \frac{(-1)^{m+1}q^{s-1}}{3}(\lambda'(i)\lambda'^{-(s-1)}(-1)J(\lambda'^2, \lambda'^2)^s + \lambda'^2(i)\lambda'^{-2(s-1)}(-1)J(\lambda', \lambda')^s) + \frac{q^{m-1}}{3} \\
&= \begin{cases} \frac{(-1)^{m+1}q^{s-1}}{3}(2\sum_{u\equiv 0 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u - \sum_{u\equiv 1,2 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = 1, \\ \frac{(-1)^{m+1}q^{s-1}}{3}(2\sum_{u\equiv 1 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u - \sum_{u\equiv 0,2 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = \zeta_3, \\ \frac{(-1)^{m+1}q^{s-1}}{3}(2\sum_{u\equiv 2 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u - \sum_{u\equiv 0,1 \,(\mathrm{mod}\ 3)} \binom{s}{u} a^{s-u}b^u) + \frac{q^{m-1}}{3} & \text{if } \lambda'(i) = \zeta_3^2. \end{cases}
\end{aligned}$$

For example, when $m = 3 \cdot 1 - 1 = 2$, we can see that each k_i with $i \neq 0$ is $\frac{q-(2a-b)}{3}$, $\frac{q-(2b-a)}{3}$, or $\frac{q+a+b}{3}$.

Remark 5.3.5. When $n = 4$, we can calculate the exact values of k_i's easily but tediously similar to the case when $n = 3$ since there are only two possible cases of $m = 4s + 1$ and $m = 4s - 1$ and the values of Jacobi sums have been already known (see [64, 115]).

5.4 New series of $(v, k, 1, 1)$-OOCs

In this section, we give a new series of optimal $(v, k, 1, 1)$-OOCs as a corollary of Theorem 5.2.2.

Let $m = 2$ in Theorem 5.2.2. Then, if $q = en + 1$ is a prime power for an odd integer n and a positive integer e such that $\gcd(e, n) = 1$, there exists a $(\frac{q^2-1}{n}, \frac{q-1}{n}, \{k_i \mid 1 \le i \le n\}, 1)$-CDF $\mathcal{F} = \{E_i \mid 1 \le i \le n\}$ satisfying the following properties:

(i) $\frac{q-(n-1)\sqrt{q}}{n} \le k_i \le \frac{q+(n-1)\sqrt{q}}{n}$ for any $1 \le i \le n$,

(ii) $k_i = \frac{q-\sum_{j=1}^{n-1} \lambda'^j(i) J(\lambda'^{hj}, \lambda'^{hj})}{n}$,

(iii) $\sum_{1 \le i \le n} k_i = q$

by using (5.8), (5.15), and Lemma 5.3.3. Now, we can get a $(\frac{q^2-1}{n}, k, 1, 1)$-OOC with n codewords, where $k = \min\{k_i \mid 1 \le i \le n\}$, by removing arbitrary $k_i - k$ elements from $E_i \in \mathcal{F}$ for every i, $1 \le i \le n$. Since $k \ge \lceil \frac{q-(n-1)\sqrt{q}}{n} \rceil$ by Lemma 5.3.2, we have the following:

Corollary 5.4.1. Let q be a prime power and let n be an odd positive integer such that $n \mid q - 1$ and $\gcd(n, \frac{q-1}{n}) = 1$. Then there exists a $(\frac{q^2-1}{n}, k, 1, 1)$-OOC with n codewords, where $k = \lceil \frac{q-(n-1)\sqrt{q}}{n} \rceil$. In particular, if

$$\frac{n(q^2 - n - 1)}{q^{1/2}(q^{1/2} + 1)(q^{1/2} - n)(q^{1/2} - n + 1)} < n + 1, \tag{5.17}$$

the resultant OOC is optimal.

Proof: We can check that the number n of codewords attains the bound (1.9) as follows:

$$\lfloor \frac{v-1}{k(k-1)} \rfloor \le \lfloor \frac{v-1}{k'(k'-1)} \rfloor \le \frac{v-1}{k'(k'-1)} = \frac{n(q^2 - n - 1)}{q^{1/2}(q^{1/2} + 1)(q^{1/2} - n)(q^{1/2} - n + 1)} < n + 1,$$

where $k' = \frac{q-(n-1)\sqrt{q}}{n} \in \mathbb{R}$. □

The bound (5.17) is always satisfied when $n = 1$ or $q^{1/2} \ge 2n^2 - 2$ for $n \ge 3$. Furthermore, it is remarkable that the new series obtained in Corollary 5.4.1 contains a well-known series of $(v, k, 1, 1)$-OOCs with exactly one codeword whose parameters are $v = q^2 - 1$ and $k = q$ (cyclic $(q^2 - 1, q - 1, q, 1)$ relative difference set), where q is a prime power, constructed from points and a line of the affine plane $\mathrm{AG}(2, q)$ (see Table 1.1).

Furthermore, we can get further series of OOCs by applying the following recursive construction given by Yin [119].

Theorem 5.4.2. ([119]) Suppose that the following exist:

(i) an $(nv, n, \{k_i \mid 1 \le i \le s\}, 1)$-CDF,

(ii) a $(u, k_i, 1)$-CDM for every i, $1 \le i \le s$,

(iii) an $(nu, n, \{k'_i \mid 1 \le i \le s'\}, 1)$-CDF.

Then, there exists an $(nuv, n, K_1 \cup K_2, 1)$-CDF with

$$K_1 = \{k_{i,j} \mid 1 \le i \le s; 1 \le j \le u\} \text{ and } K_2 = \{k'_i \mid 1 \le i \le s'\},$$

where $k_{i,j} = k_i$ for all j.

Corollary 5.4.3. Put $q = 2^t$ and let n be an odd positive integer such that $n \mid q-1$ and $\gcd(n, \frac{q-1}{n}) = 1$. If $\gcd(q+1, \lfloor \frac{q+(n-1)\sqrt{q}-n}{n} \rfloor !) = 1$, then there exists a $(\frac{(q-1)(q+1)^u}{n}, \frac{q-1}{n}, K, 1)$-CDF with

$$K = \{k_{i,j} \mid 1 \le i \le n; 1 \le j \le ((q+1)^u - 1)/q\},$$

where $k_{i,j} = k_i$ for all j and

$$\frac{q-(n-1)\sqrt{q}}{n} \le k_i \le \frac{q+(n-1)\sqrt{q}}{n}$$

for every i, $1 \le i \le n$. In particular, there exists a $(\frac{(q-1)(q+1)^u}{n}, k, 1, 1)$-OOC with $n((q+1)^u - 1)/q$ codewords for any $u \ge 1$, where $k = \lceil \frac{q-(n-1)\sqrt{q}}{n} \rceil$, which is optimal if

$$\frac{n((q+1)^u(q-1)-n)}{q^{1/2}(q^{1/2}+1)(q^{1/2}-n)(q^{1/2}-n+1)} < \frac{n((q+1)^u-1)}{q} + 1. \tag{5.18}$$

Proof: By using Theorem 1.2.5 and the assumption that $\gcd(q+1, \lfloor \frac{q+(n-1)\sqrt{q}-n}{n} \rfloor !) = 1$, there is a $(q+1, k_i, 1)$-CDM for every $k_i \le \lfloor \frac{q+(n-1)\sqrt{q}}{n} \rfloor$. Apply Theorem 5.4.2 as $g = g' = \frac{q-1}{n}$ and $u = q+1$ to the $(\frac{q^2-1}{n}, \frac{q-1}{n}, \{k_i \mid 1 \le i \le n\}, 1)$-CDF obtained in Theorem 5.2.2, then we can get a $(\frac{(q-1)(q+1)^2}{n}, \frac{q-1}{n}, K_2, 1)$-CDF with

$$K_2 = \{k_{i,j} \mid 1 \le i \le n; 1 \le j \le q+2\},$$

where $k_{i,j} = k_i$ for all j. By continuing this process, we can obtain the desired $(\frac{(q-1)(q+1)^u}{n}, \frac{q-1}{n}, K_u, 1)$-CDF $\mathcal{F}$ with

$$K_u = \{k_{i,j} \mid 1 \le i \le n; 1 \le j \le ((q+1)^u - 1)/q\},$$

where $k_{i,j} = k_i$ for all j. Furthermore, removing arbitrary $k_{i,j} - k$ elements from each block in $\mathcal{F}$, we also get a $(\frac{(q-1)(q+1)^u}{n}, k, 1, 1)$-OOC. The optimality can be checked similar to Corollary 5.4.1. □

Chapter 6

Further researches and open problems

In Chapter 2, we have discussed bounds and constructions of optimal $(v, 4, 2, 1)$-OOCs and 8-supp $(v, 4)_2$-CDFs. In particular, we showed the existence of an 8-supp $(np, n, 4)_2$-CDF for a prime $p \equiv 1 \pmod{8/\gcd(n, 8)}$ when $n = 1, 2$ and 4. In the case of $n = 8$, we showed that there exists an 8-supp $(np, n, 4)_2$-CDF for $p \equiv 1 \pmod 4$ but not for $p \equiv 3 \pmod 4$. Here, we have the following problem.

Problem 1. Establish whether there exist 8-supp $(8p, 8, 4)_2$-CDFs for all primes $p \equiv 3 \pmod 4$.

By the way, for existence problems of optimal $(v, 4, 1, 1)$-OOCs (maximal 12-supp $(v, 4)_1$-CDFs) it was shown in [28, 29, 55] that there exists an optimal $(v, 4, 1, 1)$-OOC with $\lfloor \frac{v-1}{12} \rfloor$ codewords for every $v \equiv 0, 6, 18 \pmod{24}$ by introducing the concept of a *cyclic n-regular* $(nv, k, 1)$ *difference matrix*, which is a $k \times (nv - n)$ matrix $M = [\sigma_{i,j}]$ such that $\sigma_{i,j} \in \mathbb{Z}_{nv}$ and for every pair $(i, i') \in \mathbb{Z}_{nv} \times \mathbb{Z}_{nv}$ every element of $\mathbb{Z}_{nv} \setminus v\mathbb{Z}_{nv}$ occurs exactly once among the list $\{\sigma_{i,j} - \sigma_{i',j} \mid 1 \le j \le nv - n\}$ of differences. Now, we can define a similar concept, namely a *cyclic n-regular* $(nv, K, 1)$ *difference matrix*, where $K = (a, a + b, 0)$-$(2a + b)$ is a good kite, as a $4 \times (nv - n)$ matrix with entries in $\mathbb{Z}_{nv}$ such that the list of differences between its ith row and jth row cover all elements of $\mathbb{Z}_{nv} \setminus v\mathbb{Z}_{nv}$ whenever $(i, j) \in \{(1, 2), (1, 3), (2, 3), (3, 4)\}$ with the form

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{nv-n} \\ a_1 + b_1 & a_2 + b_2 & \cdots & a_{nv-n} + b_{nv-n} \\ 0 & 0 & \cdots & 0 \\ 2a_1 + b_1 & 2a_2 + b_2 & \cdots & 2a_{nv-n} + b_{nv-n} \end{pmatrix}$$

In order to get a similar result for the case when $\lambda_a = 2$, we need to solve the following problems (see [28, 29, 55]).

Problem 2. Find cyclic n-regular $(nv, K, 1)$ difference matrices, in particular, for the case when n is a multiple of powers of 2 and 3.

Problem 3. Determine the existence of 8-supp $(np, n, 4)_2$-CDFs for every n, in particular, for the case when n is a multiple of powers of 2 and 3.

Here are two additional open questions:

Problem 4. For general k, find a correspondence between $|\mathrm{supp}\Delta X|$ and the form of $X \in \binom{\mathbb{Z}_v}{k}$ similar to Lemma 2.2.5 and provide upper bounds on $M(v, k, 2, 1)$.

Problem 5. Generalize Theorems 2.3.5, 2.3.7, 2.3.9, 2.3.11, and 2.5.3 given in Chapter 2 for general k.

In Chapter 3, we have treated perfect δ-supp $(v, k)_\mu$-CDFs for the case when $(\delta, \mu) = (2(k-1), k-1)$ yielding $(v, k, 1)$-CACs or $(v, k, k-1, 1)$-OOCs. We have mainly discussed about the existence of perfects $2(k-1)$-supp $(p, k)_{k-1}$-CDFs for primes p and $k = 3, 4$, and 5, which is strongly connected to a problem of perfect packings. The hard part in our arguments is to establish whether the set of primes for which there exist perfect $2(k-1)$-supp $(p, k)_{k-1}$-CDFs is infinite. However, for the case when k is small a similar method used in Section 3.5 may be applicable. We give the following open problems related to perfect $2(k-1)$-supp $(p, k)_{k-1}$-CDFs.

Problem 6. Given a positive integer $k \geq 6$, establish whether the set of primes $p \equiv 1 \pmod{2k-2}$ for which there exist perfect $2(k-1)$-support $(p, k)_{k-1}$-CDFs is infinite or not.

One may suspect that there are values of k for which the above set is empty. In fact, given a "large" k, apart from the trivial case of $p = 2k-1$ (see Lemma 3.2.3), the existence of a perfect $2(k-1)$-supp $(p, k)_{k-1}$-CDF seems to be rare. This can be observed from the following results obtained by computer search. For each k such that $9 \leq k \leq 20$, the first prime $p > 2k-1$ for which there exists a perfect $2(k-1)$-supp $(p, k)_{k-1}$-CDF satisfying the condition of Corollary 3.3.3 with $s = 1$ is computed as follows:

$$\begin{aligned}(k, p) \;=\; & (9, 3617), (10, 27127), (11, 3181), (12, 56431), (13, ?), (14, 2578733), (15, 434029), \\ & (16, 4147921), (17, 55903553), (18, 48611161), (19, 74431333), (20, 10134791).\end{aligned}$$

For $k = 13$ and $s = 1$, it was checked by computer that there is no prime $p < 10^9$ for which there exist a $2(k-1)$-supp $(p, k)_{k-1}$-CDF. So, one may wonder whether each element of the set $\{1, 2, \ldots, 12\}$ is never evenly distributed over the cosets of the 12th powers modulo a prime $p \equiv 1 \pmod{24}$ similar to the case when $k = 5$ (see Example 3.5.13). We give three additional open questions in Chapter 3:

Problem 7. Generalize Theorems 3.3.7, 3.3.8, and 3.3.11 for $k \geq 6$, i.e., give necessary and sufficient conditions for the existence of perfect $2(k-1)$-supp $(p, k)_{k-1}$-CDFs for all primes p and every interger $k \geq 6$ in terms of cyclotomic conditions.

Problem 8. Determine the parameter v such that there exist perfect 8-supp $(v, 5)_4$-CDFs when $3 \mid v$.

Problem 9. Provide constructions and existence theorems of $2(k-1)$-supp $(nv, n, k)_{k-1}$-CDF for general $n \geq 2$.

In Chapter 4, some existence and non-existence theorems for strong difference families and difference covers have been presented. Furthermore, relations between these designs and

relative difference families have been investigated. As stated in Theorems 4.5.7, 4.5.8, and 4.5.13, new difference covers and strong difference families give new infinite series of relative difference families. In particular, in order to find a larger class of relative difference families, it is important to find a strong difference family with smaller μ satisfying the congruence $n\mu \equiv 0 \pmod{k(k-1)}$. Note that any difference cover always has minimum μ for given n and k. In this sense, we could get many new and large infinite series of relative difference families and optical orthogonal codes. Here is an open question about relative difference families.

Problem 10. Generalize Lemma 4.5.11 for general $k \geq 6$, i.e., prove that if there is an (N, k, μ)-SDF with $\mu = 2d\lambda$, then there are an integer s and a prime power $q_{k,d}$ such that there exists an $(N \times \mathbb{F}_q, N \times \{0\}, k, \lambda)$-DF for any prime power $q \equiv 1 \pmod{2^s d}$ with $q \geq q_{k,d}$ for any k.

In order to solve Problem 10, we have to find a method to systematically give tables similar to Tables 4.1 and 4.2.

Problem 11. Determine the spectrum of (N, k, μ)'s for which (N, k, μ)-SDFs exist. In particular, for $\mu = 2$ and N is cyclic, when does there exist an $(n, k, 2)$-CSDF?

It was shown in [9] that there does not exist any cyclic $(n, k, 2)$ difference cover except for $(n, k) = (3, 3)$ and $(6, 4)$, which solved Problem 11 for the case when the number of blocks of an (n, k, μ)-CSDF is equal to 1.

Problem 12. Improve the lower bound on q of Lemma 4.5.11.

Moreover, we have the following problem related to Chapter 2.

Problem 13. Provide a similar theorem to Theorem 4.5.13 for 8-supp $(np, n, 4)_2$-CDFs.

In Chapter 5, we constructed cyclic relative difference families with variable blocksize and gave a new construction of optimal $(v, k, 1, 1)$-OOCs from a special case of such difference families. In fact, we could obtain a large new class of optimal OOCs, whose parameters are $v = \frac{q^2-1}{n}$ and $k = \lceil \frac{q-(n-1)\sqrt{q}}{n} \rceil$. Here are some open problems for this result.

Problem 14. Find further constructions of cyclic relative difference families with variable blocksize so that the new series includes $(q^m-1, q-1, q, 1)$-CDFs (optimal $(q^m-1, q, 1)$-OOCs) constructed from $\mathrm{AG}(m, q)$.

Problem 15. Give a tighter bound on blocksize k_i's of Lemma 5.3.2, or explicitly determine the values of k_i's.

Obviously, we can see that the bound of Lemma 5.3.2 is tight when $n = 1$ since we have $k_i = q^{m-1}$, i.e., the obtained family forms a $(q^m - 1, q - 1, q^{m-1}, \frac{q^{m-2}(q-1)}{e})$-CDF. However, when $n > 1$, it seems that the bound (5.10) can be improved. Indeed, the values $\frac{q^{m-1} \pm (n-1)q^{\frac{m-1}{2}}}{n}$ are not integers in general, for example, when m is even and q is square-free. However, in order to solve Problem 15, we should calculate the values of Gaussian sums and Jacobi sums and it seems to be difficult.

Here is an additional problem in Chapter 5.

Problem 16. Find another good subset $S \subseteq \mathbb{F}_q$ such that $\{E_i \mid i \in S\}$ forms a cyclic relative difference family with variable blocksize in Theorem 5.2.2.

Note that in Theorem 5.2.2, we used S as the set of eth powers in $\mathbb{F}_q$ and we mean a "good" subset in the above as a set S such that the value of

$$\frac{1}{q^2}\sum_{i\in S}\sum_{a=0}^{\frac{q^m-1}{n}-1}\sum_{c\in\mathbb{F}_q}\sum_{d\in\mathbb{F}_q}\chi(\alpha^{na}(c+d\alpha^{-n\ell}))\chi'(-i(c+d))$$

can be calculated, where χ and χ' are canonical additive characters of $\mathbb{F}_{q^m}$ and $\mathbb{F}_q$, respectively. Problem 16 is naturally extended as follows:

Problem 17. Find a good (surjective) function f from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ and a good subset $S \subseteq \mathbb{F}_q$ such that $\log_{\alpha^n}\{f^{-1}(i) \cap N \mid i \in S \subseteq \mathbb{F}_q\}$ forms a cyclic relative difference family with variable blocksize, where α is a primitive root in $\mathbb{F}_{q^m}$ and N is the set of nth powers.

List of papers related to this thesis

- K. Momihara, M. Müller, J. Satoh, M. Jimbo, Constant weight conflict-avoiding codes, *SIAM J. Discr. Math.,* **21**, pp. 959–979, (2007).
- K. Momihara, Necessary and sufficient conditions for tight equi-difference conflict avoiding codes of weight three, *Des. Codes Cryptogr.,* **45**, pp. 379–390, (2007).
- K. Momihara, M. Buratti, Bounds and constructions of optimal $(n, 4, 2, 1)$ optical orthogonal codes, *IEEE Trans. Inform. Theory,* **55**, pp. 514–523, (2009).
- K. Momihara, Strong difference families, difference covers, and their applications for relative difference families, *Des. Codes Cryptogr.,* **51**, pp. 253–273, (2009).
- K. Momihara, On cyclic $2(k-1)$-support $(n, k)_{k-1}$ difference families, *Finite Fields Appl.,* **15** pp. 415–427, (2009).

Bibliography

[1] R.J.R. Abel, M. Buratti, Difference families, in *The CRC Handbook of Combinatorial Designs, Second Edition,* C. J. Colbourn and J. H. Dinitz, Eds. Chapman & Hall/CRC, Boca Raton, FL, pp. 392–409, (2006).

[2] R.J.R. Abel, M. Buratti, Some progress on $(v, 4, 1)$ difference families and optical orthogonal codes, *J. Combin. Theory, Ser. A,* **106**, pp. 59–75, (2004).

[3] T.L. Alderson, Optical orthogonal codes and arcs in $\mathrm{PG}(d, q)$, *Finite Fields Appl.,* **13**, pp. 762–768, (2007).

[4] T.L. Alderson, K.E. Mellinger, Constructions of optical orthogonal codes from finite geometry, *SIAM J. Discr. Math.,* **21**, pp. 785–793, (2007).

[5] T.L. Alderson, K.E. Mellinger, Geometric constructions of optimal optical orthogonal codes, *Adv. Math. Commun.,* **2**, pp. 451–467, (2008).

[6] T.L. Alderson, K.E. Mellinger, Classes of optical orthogonal codes from arcs in root subspaces, *Discr. Math.,* **308**, pp. 1093–1101, (2008).

[7] T.L. Alderson, K.E. Mellinger, Families of optimal OOCs with $\lambda = 2$, *IEEE Trans. Inform. Theory,* **54**, pp. 3722–3724, (2008).

[8] K.T. Arasu, S. Sehgal, Cyclic difference covers, *Austral. J. Combin.,* **32**, pp. 213–223, (2005).

[9] K.T. Arasu, A.K. Bhandari, S.L. Ma, S. Sehgal, Regular difference covers, *Kyungpook Math. J.,* **45**, pp. 137–152, (2005).

[10] L.D. Baumert, Cyclic difference sets, *Lecture Notes in Mathematics,* **182**, Springer-Verlag, New York, (1971).

[11] T. Beth, D. Jungnickel, H. Lenz, *Design Theory,* Cambridge University Press, (1999).

[12] I.C.M. Bird, A.D. Keedwell, Design and applications of optical orthogonal codes—a survey, *Bull. Inst. Combin. Appl.,* **11**, pp. 21–44, (1994).

[13] S. Bitan, T. Etzion, Constructions for optimal constant weight cyclically permutable codes and difference families, *IEEE Trans. Inform. Theory,* **41**, pp. 77–87, (1995).

[14] R.C. Bose, On the construction of balanced incomplete block designs, *Ann. Eugen.,* **9**, pp. 353–399, (1939).

[15] A.E. Brower, A. Scrijver, H. Hanani, Group divisible designs with block size 4, *Europ. J. Combin.,* **2**, pp. 323–330, (1981).

[16] M. Buratti, Constructions of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, *Discr. Math.,* **138**, pp. 169–175, (1995).

[17] M. Buratti, Improving two theorems of Bose on difference families, *J. Combin. Des.,* **3**, pp. 15–24, (1995).

[18] M. Buratti, On simple radical difference families, *J. Combin. Des.,* **3**, pp. 161–168, (1995).

[19] M. Buratti, A packing problem and its application to Bose's families, *J. Combin. Des.,* **4**, pp. 457–472, (1996).

[20] M. Buratti, Packing the blocks of a regular structure, *Bull. Inst. Combin. Appl.,* **21**, pp. 49–58, (1997).

[21] M. Buratti, Recursive constructions for difference matrices and relative difference families, *J. Combin. Des.,* **6**, pp. 165–182, (1998).

[22] M. Buratti, Old and new designs via difference multisets and strong difference families, *J. Combin. Des.,* **7**, pp. 406–425, (1999).

[23] M. Buratti, Cyclic designs with block size 4 and related optimal optical orthogonal codes, *Des. Codes Cryptogr.,* **26**, pp. 111–125, (2002).

[24] M. Buratti, L. Gionfriddo, Strong difference families over arbitrary graphs, *J. Combin. Des.,* **16**, pp. 443–461, (2008).

[25] M. Buratti, A. Pasotti, Graph decompositions with the use of difference matrices, *Bull. Inst. Combin. Appl.,* **47**, pp. 23–32, (2006).

[26] M. Buratti, A. Pasotti, Combinatorial designs and the theorem of Weil on multiplicative character sums, *Finite Fields Appl.,* **15**, pp. 332–344, (2009).

[27] M. Buratti, A. Pasotti, Further progress on difference families with block size 4 or 5, preprint.

[28] Y. Chang, R. Fuji-Hara, Y. Miao, Combinatorial constructions of optimal optical orthogonal codes with weight 4, *IEEE Trans. Inform. Theory,* **49**, pp. 1283–1292, (2003).

[29] Y. Chang, Y. Miao, Constructions for optimal optical orthogonal codes, *Discr. Math.,* **261**, pp. 127–139, (2003).

[30] Y. Chang, Some cyclic BIBDs with block size four, *J. Combin. Des.,* **12**, pp. 177–183, (2004).

[31] Y. Chang, L, Ji, Optimal $(4up, 5, 1)$ optical orthogonal codes, *J. Combin. Des.,* **12**, pp. 346–361, (2004).

[32] Y. Chang, J. Yin, Further results on optimal optical orthogonal codes with weight 4, *Discr. Math.,* **279**, pp. 135–151, (2004).

[33] K. Chen, G. Ge, L. Zhu, Starters and related codes, *J. Statis. Plann. Inference,* **86**, pp. 379–395, (2000).

[34] K. Chen, L. Zhu, Existence of $(q, k, 1)$ difference families with q a prime power and $k = 4, 5$, *J. Combin. Des.,* **7**, pp. 21–30, (1997).

[35] K. Chen, L. Zhu, Existence of $(q, 6, 1)$ difference families with q a prime power, *Des. Codes Cryptogr.,* **15**, pp. 167–173, (1998).

[36] K. Chen, R. Wei, L. Zhu, Existence of $(q, 7, 1)$ difference families with q a prime power, *J. Combin. Des.,* **10**, pp. 126–138, (2002).

[37] W. Chu, C.J. Colbourn, Recursive constructions for optimal $(n, 4, 2)$-OOCs, *J. Combin. Des.,* **12**, pp. 333–345, (2004).

[38] W. Chu, C.J. Colbourn, Sequence designs for ultra-wideband impulse radio with optimal correlation properties, *IEEE Trans. Inform. Theory,* **50**, pp. 2402–2407, (2004).

[39] W. Chu, C.J. Colbourn, Optimal frequency-hopping sequences via cyclotomy, *IEEE Trans. Inform. Theory,* **51**, pp. 1139–1141, (2005).

[40] W. Chu, S.W. Golomb, A new recursive construction for optical orthogonal codes, *IEEE Trans. Inform. Theory,* **49**, pp. 3072–3076, (2003).

[41] H. Chung, P.V. Kumar, Optical orthogonal codes—new bounds and an optimal construction, *IEEE Trans. Inform. Theory,* **36**, pp. 866–873, (1990).

[42] F.R.K. Chung, J.A. Salehi, V.K. Wei, Optical orthogonal codes: Design, analysis, and applications, *IEEE Trans. Inform. Theory,* **35**, pp. 595–604, (1989).

[43] M. J. Colbourn, C.J. Colbourn, Recursive constructions for cyclic block designs, *J. Statis. Plann. Inference,* **10**, pp. 97–103, (1984).

[44] C.J. Colbourn, J.H. Dinitz, D.R. Stinson, Applications to communications, cryptography, and networking, *London Math. Soc. Lecture Note, Ser.* 267, pp. 37–100, (1999).

[45] J.A. Davis, Partial difference sets in p-groups, *Arch. Math.,* **63**, pp. 103–110, (1994).

[46] L.E. Dickson, Cyclotomy, higher conguences, and Waring's problem, *Amer. J. Math.,* **57**, pp. 391–424, 463–474, (1935).

[47] C. Ding, Optimal and perfect difference systems of sets, *J. Combin. Theory, Ser. A,* **116**, pp. 109–119, (2009).

[48] C. Ding, T. Helleseth, T. Klove, X. Wang, A generic construction of Cartesian authentication codes, *IEEE Trans. Inform. Theory,* **53**, pp. 2229–2235, (2007).

[49] C. Ding, C. Xing, Several classes of $(2^m - 1, w, 2)$ optical orthogonal codes, *Discr. Appl. Math.,* **128**, pp. 103–120, (2003).

[50] R.A. Fisher, *The Design of Experiments*, Oliver and Boyd, Edinburgh, (1947).

[51] T. Feng, Y. Chang, L. Ji, Constructions for strictly cyclic 3-designs and applications to optimal OOCs with $\lambda = 2$, *J. Combin. Theorey, Ser. A,* **115**, pp. 1527–1551, (2008).

[52] R. Fuji-Hara, Y. Miao, Optical orthogonal codes: their bounds and new optimal constructions *IEEE Trans. Inform. Theory,* **46**, pp. 2396–2406, (2000).

[53] R. Fuji-Hara, Y. Miao, and J. Yin, Optimal $(9v, 4, 1)$ optical orthogonal codes, *SIAM J. Discr. Math.,* **14**, pp. 256–266, (2001).

[54] C.F. Gauss, *Disquisitiones Arithmeticae*, (1801). English translation, Yale, New Haven, (1966). (Reprinted by Springer-Verlag (1986).)

[55] G. Ge, J. Yin, Constructions for optimal $(v, 4, 1)$ optical orthogonal codes, *IEEE Trans. Inform. Theory,* **47**, pp. 2998–3004, (2001).

[56] M. Greig, Some group divisible design constructions, *J. Comb. Math. Comb. Comput.,* **27**, pp. 33-52, (1998).

[57] L. Györfi, I. Vajda, Constructions of protocol sequences for multiple access collision channel without feedback, *IEEE Trans. Inform. Theory,* **39**, pp. 1762–1765, (1993).

[58] H. Hanani, The existence and construction of balanced incomplete block designs, *Ann. Math. Statist.,* **32**, pp. 361-386, (1961).

[59] H. Hanani, On balanced incomplete block designs with block size having five elements, *J. Combin. Theory, Ser. A,* **12**, pp. 184-201, (1972).

[60] H. Hanani, Balanced incomplete block designs and related designs, *Discr. Math.,* **11**, pp. 255-369, (1975).

[61] H. Hasse, *Mathmatische Abhandlungen Band* 1, Walter de Gruyter, Berlin, (1975).

[62] T.J. Healy, Coding and decoding for code division multiple user communication systems, *IEEE Trans. Commun.,* **33**, pp. 310–316, (1985).

[63] J.Y. Hui, Pattern code modulation and optical decoding—a novel code-division multiplexing technique for multifiber network, *IEEE J. Sel. Areas Commum.,* **3**, pp. 916–927, (1985).

[64] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, (1981).

[65] M. Jimbo, S. Kuriki, On a composition of cyclic 2-designs, *Discr. Math.,* **43**, pp. 249–255, (1983).

[66] M. Jimbo, M. Mishima, S. Janiszewski, A.Y. Teymorian, V. Tonchev, On conflict-avoiding codes of length $n = 4m$ for three active users, *IEEE Trans. Inform. Theory,* **53**, pp. 2732–2742, (2007).

[67] S.M. Johnson, A new upper bound for error-correcting codes, *IEEE Trans. Inform. Theory,* **8**, pp. 203–207, (1962).

[68] D. Jungnickel, A. Pott, K.W. Smith, Difference sets, in *The CRC Handbook of Combinatorial Designs, Second Edition,* C. J. Colbourn and J. H. Dinitz, Eds. Chapman & Hall/CRC, Boca Raton, FL, pp. 419–436, (2006).

[69] C. Lam, Y. Miao, $(C_k \oplus G, k, \lambda)$ difference families, *Des. Codes Cryptogr.,* **24**, pp. 291–304, (2001).

[70] H.K. Leung, S.L. Ma, B. Schmidt, New Hadamard matrices of order $4p^2$ obtained from Jacobi sum of order 16, *J. Combin. Theory, Ser. A,* **113**, pp. 822–838, (2006).

[71] K.H. Leung, S.L. Ma, B. Schmidt, Proper partial geometries with Singer groups and pseudogeometric partial difference sets, *J. Combin. Theory, Ser. A,* **115**, pp. 147–177, (2008).

[72] V.I. Levenshtein, Combinatorial problems motivated by comma-free codes, *J. Combin. Des.,* **12**, pp. 184–196, (2004).

[73] V.I. Levenshtein, Conflict-avoiding codes for three active users and cyclic triple systems, *Probl. Inf. Transm.,* **43**, pp. 39–53, (2007).

[74] V.I. Levenshtein, V.D. Tonchev, Optimal conflict-avoiding codes for three active users, *Proc. ISIT, 2005,* pp. 535–537, (2005).

[75] V.I. Levenshtein, A.J.H. Vinck, Perfect (d, k)-codes capable of correcting single peak shifts, *IEEE Trans. Inform. Theory,* **39**, pp. 656–662, (1993).

[76] R. Lidl, H. Niederreiter, *Finite Fields*, Cambridge Univ. Press, (1997).

[77] S.L. Ma, A survey on partial difference sets, *Des, Codes Cryptogr.,* **4**, pp. 221–261, (1994).

[78] S. Ma, Y. Chang, A new class of optimal optical orthogonal codes with weight five, *IEEE Trans. Inform. Theory,* **50**, pp. 1848–1850, (2004).

[79] S. Ma, Y. Chang, Constructions of optimal optical orthogonal codes with weight five, *J. Combin. Des,* **13**, pp. 54–69, (2005).

[80] F.J. MacWilliams, Cyclotomic numbers, coding theory and orthogonal polynomials, *Discr. Math.,* **3**, pp. 133–151, (1972).

[81] F.J. MacWilliams, N.J.A. Sloane, *The Theory of Error-Correcting Codes*, North-Holland Amsterdam, (1978).

[82] S.V. Maric, V.K.N. Lau, Multirate fiber-optic CDMA: System design and performance analysis, *J. Lightwave Technol.,* **16**, pp. 9–17, (1998).

[83] S.V. Maric, O. Moreno, C. Corrada, Multimedia transmission in fiber-optic LAN's using optical CDMA, *J. Lightwave Technol.,* **14**, pp. 2149–2153, (1996).

[84] J.L. Massey, P. Mathys, The collision channel without feedback, *IEEE Trans. Inform. Theory,* **31**, pp. 192–204, (1985).

[85] P. Mathys, A class of codes for a T active users out of N multiple-access, *IEEE Trans. Inform. Theory,* **36**, pp. 1206–1219, (1990).

[86] R.J. McEliece, H. Rumsey, Jr., Euler products, cyclotomy and coding, *J. Number Theory,* **4**, pp. 302–311, (1972).

[87] N. Miyamoto, H. Mizuno, S. Shinohara, Optical orthogonal codes obtained from conics on finite projective planes. *Finite Fields Appl.,* **10**, pp. 405–411, (2004).

[88] K. Momihara, M. Müller, J. Satoh, M. Jimbo, Constant weight conflict-avoiding codes, *SIAM J. Discr. Math.,* **21**, pp. 959–979, (2007).

[89] K. Momihara, Necessary and sufficient conditions for tight equi-difference conflict avoiding codes of weight three, *Des. Codes Cryptogr.,* **45**, pp. 379–390, (2007).

[90] K. Momihara, M. Buratti, Bounds and constructions of optimal $(n, 4, 2, 1)$ optical orthogonal codes, *IEEE Trans. Inform. Theory,* **55**, pp. 514–523, (2009).

[91] K. Momihara, Strong difference families, difference covers, and their applications for relative difference families, *Des. Codes Cryptogr.,* **51**, pp. 253–273, (2009).

[92] K. Momihara, On cyclic $2(k-1)$-support $(n, k)_{k-1}$ difference families, *Finite Fields Appl.,* **15** pp. 415–427, (2009).

[93] O. Moreno, R. Omrani, P.V. Kumar, H. Lu, A generalized Bose-Chowla family of optical orthogonal codes and distinct difference sets. *IEEE Trans. Inform. Theory,* **53**, pp. 1907–1910, (2007).

[94] C.J. Moreno, S.S. Wagstaff, *Sums of squares of integers,* Chapman & Hall/CRC; 1-st editioin, (2005).

[95] E. Netto, Zur theorie der triplesysteme, *Math. Ann.* **442**, pp. 143–152, (1893).

[96] Q.A. Nguyen, L. Györfi, J.L. Massey, Constructions of binary constant weight cyclic codes and cyclically permutable codes, *IEEE Trans. Inform. Theory,* **38**, pp. 940–949, (1992).

[97] W. Ogata, K. Kurosawa, D.R. Stinson, H. Saido, New combinatorial designs and their applications to authentication codes and secret sharing schemes, *Discr. Math.,* **279**, pp. 383-405, (2004).

[98] R. Peltesohn, Eine Losung der beiden Heffterschen Differenzenprobleme, *Compos. Math.,* **6**, pp.251–257, (1938).

[99] J. Polhill, New negative Latin square type partial difference sets in nonelementary abelian 2-groups and 3-groups, *Des. Codes Cryptogr.,* **46**, pp. 365–377, (2008).

[100] D.K. Ray-Chaudhuri, Y.Q. Chen, Q. Xiang, Constructions of partial difference sets and relative difference sets using Galois rings II, *J. Combin. Theory, Ser. A,* **76**, pp. 179–196, (1996).

[101] P. Ribenboim, *Classical theory of algebraic numbers*, Springer-Verlag, New York, (2001).

[102] J.A. Salehi, Code division multiple-access techniques in optical fiber networks, Part I: Fundamental principles, *IEEE Trans. Commun.,* **37**, pp. 824–833, (1989).

[103] J.A. Salehi, C.A. Brackett, Code division multiple access techniques in optical fiber networks, Part II: Systems performance analysis, *IEEE Trans. Commun.,* **37**, pp. 834–842, (1989).

[104] E. Spence, Hadamard matrices from relative difference sets, *J. Combin. Theory Ser. A,* **19**, pp. 287–300, (1975).

[105] T. Storer, *Cyclotomy and difference sets*, Lectures in advanced mathematics, Markham publishing company, (1967).

[106] V.D. Tonchev, *Tables of Conflict-Avoiding Codes*, [Online]. Available: http://www.math.mtu.edu/~tonchev/CAC.html

[107] B.S. Tsybakov, A.R. Rubinov, Some constructions of conflict-avoiding codes, *Probl. Inf. Transm.,* **38**, pp. 268–279, (2002).

[108] W.D. Wallis, *Combinatorial Designs,* Monographs and textbooks in pure and applied mathematics, Ser. 118, Marcel dekker, inc. New York, pp. 46–54, (1988).

[109] W.D. Wallis, A.P. Street, J.S. Wallis, *Combinatorics: Room Squares, Sum-Free Sets, Hadamard Matrices,* Springer-Verlag, Berlin-Heidelberg, New York, (1972).

[110] R.M. Wilson, Cyclotomy and difference families in elementary abelian groups, *J. Number Theory,* **4**, pp. 17–47, (1972).

[111] R.M. Wilson, An existence theorem for pairwise balanced designs, I: Composition theorems and morphisms, *J. Combin. Theory, Ser. A,* **13**, pp. 220–245, (1972).

[112] R.M. Wilson, An existence theorem for pairwise balanced designs, II: The structure of PBD-closed set and the existence conjecture, *J. Combin. Theory, Ser. A,* **13**, pp. 246–273, (1972).

[113] R.M. Wilson, An existence theorem for pairwise balanced designs, III: Proof of the existence conjecture, *J. Combin. Theory, Ser. A,* **18**, pp. 71–79, (1975).

[114] M. Xia, T. Xia, J. Seberry, A new family of supplementary difference sets and Hadamard matrices, *Des. Codes Cryptogr.,* **35**, pp. 283–291, (1996).

[115] M. Yamada, Supplementary difference sets and Jacobi sums, *Discr. Math.,* **103**, pp. 75–90, (1992).

[116] M. Yamada, Supplementary difference sets constructed from $(q+1)$st cyclotomic classes in GF(q^2), *Australas. J. Combin.,* **39**, pp. 73–87, (2007).

[117] F. Yates, Incomplete randomized blocks, *Ann. Eugen.,* **7**, pp. 121–140, (1936).

[118] J. Yin, Some combinatorial constructions for optical orthogonal codes, *Discr. Math.,* **185**, pp. 201–219, (1998).

[119] J. Yin, A general construction for optimal cyclic packing designs, *J. Combin. Theory, Ser. A,* **97**, pp. 272–284, (2002).