STRONGLY REGULAR GRAPHS, ASSOCIATION SCHEMES AND GAUSS SUMS

by

Fan Wu

A dissertation submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Doctor of Philosophy in Mathematics

Winter 2014

ProQuest LLC.
789 East Eisenhower Parkway
P.O. Box 1346
Ann Arbor, MI 48106 - 1346

STRONGLY REGULAR GRAPHS, ASSOCIATION SCHEMES AND GAUSS SUMS

by

Fan Wu

Approved: ______________________________

John Pelesko, Ph.D.
Chair of the Department of Mathematics

Approved: ______________________________

George H. Watson, Ph.D.
Dean of the College of Art and Science

Approved: ______________________________

James G. Richards, Ph.D.
Vice Provost for Graduate and Professional Education

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: ______________________________

Qing Xiang, Ph.D.
Professor in charge of dissertation

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: ______________________________

Sebastian Cioabă, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: ______________________________

Felix Lazebnik, Ph.D.
Member of dissertation committee

I certify that I have read this dissertation and that in my opinion it meets the academic and professional standard required by the University as a dissertation for the degree of Doctor of Philosophy.

Signed: ______________________________

David B. Saunders, Ph.D.
Member of dissertation committee

ACKNOWLEDGEMENTS

This dissertation was written under the guidance of my advisor, Dr. Qing Xiang. I am grateful to Dr. Qing Xiang, for his generous help during the past four and half years at the University of Delaware. He taught me difference sets, classical groups, algebraic number theory, coding theory and p-adic analysis. Dr. Qing Xiang sets a good example for me as a mathematician.

I also want to thank my committee members, Dr. Sebastian Cioabă, Dr. Felix Lazebnik and Dr. B. David Saunders. They spent a lot of their precious time reading my thesis and providing many comments and suggestions that greatly improved my dissertation.

Dr. Lazebnik taught me two graduate level classes in combinatorics in my first year at the University of Delaware. He spent a lot of time patiently explaining basic ideas of combinatorics to me. I also want to thank Dr. Robert Coulter. In the spring semester of 2011, Dr. Lazebnik, Dr. Coulter and I worked on the classification of planar functions over $\mathbb{F}_{p^3}$ together. Our weekly discussions during that semester led to some progress on this problem. From them, I learnt a lot about polynomials over finite fields.

Dr. Cioabă taught me algebraic graph theory. He is a terrific teacher. From his classes, I acquired a lot of background material on strongly regular graphs. I took two courses given by Dr. Saunders, algorithms and computer algebra, from which I learned relationships between mathematics and computer science.

I would like to thank the late Dr. Wenbo Li. He taught me many basic materials in probability. He left us suddenly, but his enthusiasm for mathematics will influence me forever.

I must give my special thanks to Dr. Tao Feng. As one of my best friends, he promoted the study of Gauss sums, Jacobi sums and finite fields. He taught me how to program with MAGMA. Meantime, I benefited much from the frequent discussions with him, which helped me understand the results in [25]. Moreover, his enthusiasm in basketball pushed me to go to gym regularly.

I want to thank Dr. Shaofang Hong, who was my M. S. advisor at Sichuan University. He taught me number theory and coding theory. We worked on a problem about a certain type of Gauss sums together.

Thank all the staff members in the department of mathematical sciences, especially Debora See. Her work made my life at the University of Delaware much easier.

I would like to thank my colleagues, friends and classmates at the University of Delaware, especially Dr. Jiyou Li, Dr. Brian Kronenthal and Dr. Steven Senger. While I was writing up the dissertation, they spent many hours helping me correct language mistakes in the manuscript. Their efforts greatly increased the quality of the thesis. In the past four years at the University of Delaware, I received a lot of help and encouragements from my friends. Thank you for your understanding and support.

Last but not the least, I would like to thank my parents, who are my heroes. They have put up with many “ridiculous” ideas of me for many years, and they never received anything back from me. Even though they do not understand the mathematics I am doing, I believe that I can achieve nothing in mathematics without their unconditional trust, love and support.

TABLE OF CONTENTS

Chapter

LIST OF TABLES

LIST OF FIGURES

ABSTRACT

Gauss sums play an important role in the construction of strongly regular Cayley graphs and association schemes. Compared with other approaches to the constructions of strongly regular graphs, the method using Gauss sums requires a lot of background knowledge from algebra and number theory. In [50], Schmidt and White provided a conjecture on cyclotomic strongly regular graphs which contains 11 sporadic examples of cyclotomic strongly regular graphs. We first generalize one of their sporadic examples to an infinite family of strongly regular graphs by using a union of cyclotomic classes. We do so by first deriving expressions for the (restricted) eigenvalues of Cayley graphs without evaluating Gauss sums explicitly, and then giving conditions that determined candidate Cayley graphs be strongly regular.

A. V. Ivanov's conjecture on amorphic association schemes was first disproved by Van Dam. Before the work of this dissertation, only finitely many counterexamples were known. In the dissertation, we shall give 15 infinite families of counter examples to Ivanov's conjecture. Moreover, our families of association schemes are pseudocyclic. We shall prove this fact by using the properties of Gauss sums of the index 2.

Chapter 1

INTRODUCTION

This dissertation consists of two results. The first main result is to give sufficient and necessary conditions that determine certain Cayley graphs, which come from cyclotomy, to be strongly regular. The significance of this result lies not only in generalizing Example 5 in Table I below, but also in giving an approach to constructing strongly regular Cayley graphs without evaluating Gauss sums of high indices explicitly.

The second main result is the construction of infinite families of counterexamples to A. V. Ivanov's false conjecture about amorphic association schemes. Since association schemes can be viewed as generalizations of strongly regular graphs, we begin by introducing basic terminology in graph theory.

An *graph* $\Gamma(V,\ E)$ consists of a set V of *vertices*, a set E of *edges*, and a mapping associating to each edge $e \in E$ an unordered pair $x,\ y$ of vertices called the *endpoints* of e. We call $v := |V|$ as the *order* of the graph. We say an edge is *incident* with its endpoints. If $E = \emptyset$, we say $\Gamma(V,\ E)$ is *edgeless*. We call the number edges which are incident with a vertex x the *valency* of x. If two endpoints of an edge are same, this edge is called a *loop*. A graph is called *simple*, if it does not contain loops and no two distinct edges have exactly the same pair of endpoints. If an ordered pair of vertices is associated to each edge of a graph, we have a *directed graph*, otherwise, the graph is called *undirected*. For a simple and undirected graph $\Gamma(V,\ E)$, the elements of E can be identified with elements of some subset of $V \times V$. In this dissertation, we assume graphs to be simple, undirected and not edgeless.

In a graph $\Gamma(V,\ E)$ of order v, label the vertices by $\{1,\ \ldots,\ v\}$. The *adjacency matrix* A of Γ is defined by $A = (a_{ij})$, where $a_{ij} = 1$, when vertex i and vertex j are adjacent, and $a_{ij} = 0$ otherwise. Thus, A is a symmetric 0-1 matrix with diagonal entries all being zeros. It is well known that all eigenvalues of the matrix A are real and it has exactly v linearly independent eigenvectors. The eigenvalues (eigenvectors) of A are called the *eigenvalues* (*eigenvectors*) of Γ.

We call two graphs $\Gamma(V_1,\ E_1)$ and $\Gamma(V_2,\ E_2)$ *isomorphic* if there exists a bijection σ from V_1 to V_2 such that $\sigma(x)\sigma(y) \in E_2$ if and only if $xy \in E_1$. Furthermore, we say an isomorphism σ is an *automorphism*, if $V_1 = V_2$ and $E_1 = E_2$. It is easy to see that all automorphisms of a graph form a subgroup of the permutation group of the vertex set. We call this group the *automorphism group* of the graph $S(V)$. Usually, we do not distinguish between two isomorphic graphs, since in graph theory isomorphic graphs share exactly the same graph theoretic properties. In the following, we call the graphs "new", if they are not isomorphic to known examples.

We call two vertices x and y of the graph G are *adjacent*, if $xy \in E(G)$. Let $N(x)$ be the set of vertices adjacent with x. Then, $N(x)$ is called the *neighborhood* of x and $|N(x)|$, denoted as $d(x)$, is called the *valency* of x. We call a graph *regular* of valency k, if all of its vertices have the same valency k. We call a regular graph of order v and valency $v-1$ a *complete graph.* As examples, we introduce simple closed paths. A *walk of length* n in a graph G is a sequence $v_0, e_0, v_1, \ldots, v_{n-1}, e_{n-1}, v_n$, where v_i and v_{i+1} are two endpoints of the edge e_i, $0 \leq i \leq n-1$. A walk is called a *simple closed path*, denoted by C_n, if $v_0, \ldots, v_{n-1}$ are distinct points, $e_0, \ldots, e_{n-1}$ are distinct edges and $v_0 = v_n$. It is easy to see that C_n, $n \geq 1$, are regular graphs. A straightforward conclusion is that for a regular graph Γ of valency k, k is an eigenvalue of Γ, and the all-one vector $\mathbf{1}$ is an eigenvector with respect to k.

In graph theory, regular graphs occupy an important position. In this dissertation, we concern ourselves with a special type of regular graphs, strongly regular graphs. A *strongly regular graph srg* (v, k, λ, μ) is a graph with v vertices that is regular of valency k and that has the following properties:

(1) Any two adjacent vertices x and y have exactly λ common neighbors.

(2) Any two non-adjacent vertices x and y have exactly μ common neighbors.

We call nonnegative integers v, k, λ and μ the *parameters* of a strongly regular graph. The triangle C_3, quadrangle C_4, pentagon C_5 are examples of strongly regular graphs. Moreover, the Petersen graph is an example of strongly regular graphs, srg $(10, 3, 0, 1)$. In Brouwer and Haemers' book [14], we see that there are many more examples of strongly regular graphs that have been constructed. A natural question is to construct more new strongly regular graphs. This is the main topic of our first research project in this dissertation.

Strongly regular graphs have been studied extensively since their introduction by Bose [12] in 1963. Given a set of parameters v, k, λ and μ, the following three types of questions are important in the theory of strongly regular graphs:

(1) Construct strongly regular graphs with the above parameters if possible.

(2) Show the graphs obtained are new.

(3) Show the non-existence of strongly regular graphs with the above parameters if one cannot construct them.

For the third item, we refer the reader to Brouwer and Van Lint's paper [16], which contains a detailed survey on the non-existence problem. This dissertation is only concerned with the first two questions.

Clearly, two strongly regular graphs with different parameters (v, k, λ, μ) are non-isomorphic to each other. Thus, it is straightforward to show two strongly regular graphs are non-isomorphic, if they have different sets of parameters. Then, we focus on the first problem above. An important approach in the theory of strongly regular graph is to investigate the eigenvalues of graphs. An eigenvalue of a graph is called as an *restricted eigenvalue*, if it has a eigenvector that is not a multiple of the all-one vector. In Chapter 3, we shall prove the a candidate regular graph to be strongly regular by showing that it has exactly two restricted eigenvalues. In Chapter 2, we shall introduce some effective methods to fulfill this task.

Regular graphs can be constructed through many approaches. An effective method is by the Cayley graph construction. An automorphism group G of a set V *acts regularly* on V, if only the identity element of G fixes any point. A Cayley graph $\Gamma(V,\ E)$ is defined as a graph which admits an automorphism group G (written additively) acting regularly on the vertex set V. Let P be any point (we call it *base point*) of V, then the regularity of G acting on V allows us to identify the elements of V with the elements of G. Let D be a subset of G such that 0 does not belong to D and $-D = D$. The *Cayley graph* $\mathrm{Cay}(G,\ D)$ *generated by the connection set* D is the graph with the vertex set G and the edge set E, which is identified with the set $\{(x,\ y) \mid x - y \in D \text{ and } x,\ y \in G\}$. It is straightforward that the graphs we obtain in this way are regular. (See Theorem 2.2.9.)

The Cayley graph construction has two main benefits as follows. First, the Cayley graph construction provides a unified method to construct regular graphs in various groups. Furthermore, compared with other types of construction, a strongly regular graph with finite parameters by the Cayley graph construction are easier to be generalized to an infinite family of strongly regular graphs. With the assistance of computers, we search a general pattern of D in an infinite family of groups, and then prove the pattern gives a infinite family of strongly regular graphs. The subfield and semi-primitive cyclotomic strongly regular graphs, which will be defined after a couple of lines, are typical results obtained through this approach. Moreover, the Cayley graph construction was successfully used in a series of papers [25, 27, 28]. Our first main result, published in [53], was also obtained using this type of construction.

The second benefit of the Cayley graph construction is that eigenvalues of Cayley graphs are relatively easy to compute. In fact, the eigenvalues of a Cayley graph are given by character sums. (See Theorem 2.2.9) Let p be a prime, f be a positive integer and $q = p^f$. Let $\mathbb{F}_q$ be finite field of order q and $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$. Let D be a subset of $\mathbb{F}_q^*$ such that $-D = D$. A Cayley graph $\mathrm{Cay}(\mathbb{F}_{p^f}, D)$ with the *connection set* D is a graph whose vertex set is $\mathbb{F}_{p^f}$ and any two vertices are adjacent if and only if their difference belongs to D. A subtle construction of D is crucial to our research project. By the means of cyclotomy, we point out the connection between eigenvalues of Cayley graphs and Gauss sums (Gauss sums will be introduced in Section 2.1).

Let γ be a primitive element of $\mathbb{F}_q$. Let N be a positive integer that divides $q-1$ such that $1 < N < q-1$. Let $C_0 = \langle \gamma^N \rangle \leq \mathbb{F}_q^*$. Then, we have $[\mathbb{F}_q^* : C_0] = N$, $|C_0| = \frac{q-1}{N}$ and the sets C_0, $C_1 = \gamma C_0$, $\ldots$, $C_{N-1} = \gamma^{N-1} C_0$ are called the *cyclotomic classes* of order N of $\mathbb{F}_q$. The class C_0 is also called the N^{th} *power residues*. If we set D to be one or a union of cyclotomic classes, the eigenvalues of Cayley graphs are determined by the values of Gauss sums. The advantage of this construction lies in that powerful tools from algebra and number theory (such as Stickelberger's theorem, see [9], Chapter 10) can be consequently applied to this problem. In the dissertation, our connection set D is a union of cyclotomic classes. Before the formal introduction of our result, we summarize recent progress about the case when D is a single class.

If D is a single class, it is easy to see that $\mathrm{Cay}(\mathbb{F}_q, C_i) \cong \mathrm{Cay}(\mathbb{F}_q, C_0)$, $1 \leq i \leq N-1$. Without loss of generality, we set $D = C_0$. Thus, D is a subgroup of $\mathbb{F}_q^*$. If $\mathrm{Cay}(\mathbb{F}_q, D)$ is strongly regular, then we speak of a *cyclotomic strongly regular graph*. A straightforward result is that $\mathrm{Cay}(\mathbb{F}_q,\ D)$ is strongly regular if D is the multiplicative group of a subfield of $\mathbb{F}_{p^f}$. (See Section 2.4) Such cyclotomic strongly regular graphs are called *subfield examples*. Next, if there exists a positive integer t such that $-1 \equiv p^t \pmod{N}$, then it can be shown that $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph. (For the proof of this fact, see [8].) Such cyclotomic strongly regular graphs are called *semiprimitive examples*. It is natural to ask: Can we classify and characterize all cyclotomic strongly regular graphs? Schmidt and White [50] proposed a conjectural classification of cyclotomic strongly regular graphs.

Conjecture 1.0.1. (Conjecture 4.4, [50]) *Let p be a prime, f a positive integer, and $q = p^f$. Let $N > 1$ be a divisor of $(q-1)/(p-1)$. Assume that D is the subgroup of $\mathbb{F}_q^*$ of index N such that $-D = D$. If Cay$(\mathbb{F}_q,\ D)$ is a strongly regular graph, then one of the following holds:*

(1) (subfield case) $D = \mathbb{F}_{p^e}^*$ for some integer $e \geq 1$, $e|f$.

(2) (semi-primitive case) There exists a positive integer t such that $-1 \equiv p^t \pmod{N}$.

(3) (exceptional case) Cay$(\mathbb{F}_{p^f}, D)$ is one of the 11 sporadic examples appearing in the

following table:

N	p	f	$[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle]$
11	3	5	2
19	5	9	2
35	3	12	2
37	7	9	4
43	11	7	6
67	17	33	2
107	3	53	2
133	5	18	6
163	41	81	2
323	3	144	2
499	5	249	2

Table 1.1: Sporadic examples of $\mathrm{Cay}(\mathbb{F}_{p^f}, D)$

Conjecture 1.0.1 as a whole remains open, while partial results can be found in [1, 50]. In [50], Schmidt and White gave a proof of Conjecture 1.0.1 for the case where $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = 2$. (See Theorem 5.4, [50]) Their proof depends on the generalized Riemann hypothesis. According to a personal conversation with Bernhard Schmidt at Caltech in March 2012, this is the most recent progress about this conjecture. We should remark that this conjecture is closely related to subdifference sets of Singer difference sets. (See [50]).

In [50], the authors gave sufficient and necessary conditions for irreducible cyclic codes to have two nonzero weights (Theorem 3.1, [50]). By their theorem, it is straightforward to show subfield and semi-primitive irreducible cyclic codes have exactly two nonzero weights. Two-weight linear codes are closely related to strongly regular Cayley graphs, projective two-intersection sets in finite geometry, and partial difference sets. (See, for instance, [14, 17, 40].) Thus, Schmidt and White's results actually gave the conditions that determine a candidate Cayley graph to be subfield or semi-primitive example, when the connection set is a single cyclotomic class.

Compared with the constructions of strongly regular graphs by using a single cyclotomic class of finite fields, unions of cyclotomic classes give us more examples. In fact, some sporadic examples of such strongly regular graphs have been found:
(1) (De Lange [21]) Let $q = 2^{12}$ and $N = 45$. Then, the connection set $D = C_0 \cup C_5 \cup C_{10}$ gives a strongly regular graph, while $\mathrm{Cay}(\mathbb{F}_q, C_0)$ is not.
(2) (Ikuta and Munemasa [32]) Let $q = 2^{21}$ and $N = 49$. Then, the connection set $D = C_0 \cup C_3 \cup C_6 \cup C_9 \cup C_{12}$ gives a strongly regular graph, while $\mathrm{Cay}(\mathbb{F}_q, C_0)$ is not.
(3) (De Lange [21]) Let $q = 2^{12}$ and $N = 45$. Then, the connection set $D = C_0 \cup C_1 \cup C_2 \cup C_3 \cup C_4 \cup C_5 \cup C_6$ gives a strongly regular graph, while $\mathrm{Cay}(\mathbb{F}_q, C_0)$ is not.
The above examples solidify our confidence in constructing strongly regular graphs using unions of cyclotomic classes.

Our first main result was contained in [53]. It is not the first time that this method was successfully used. A sequence of papers [25, 28] greatly contributed to this topic. Feng and Xiang in [25] extended the above three examples into infinite families and, what is more, they obtained nine more infinite families of strongly regular graphs. They succeeded in generalizing index 2 examples in Table I. Soon after, Ge, Xiang and Yuan in [28] generalized the index 4 example in Table I. Since their results require some technical terminology that has not been defined, we postpone sketching them to Chapter 3.

The first main task of this dissertation is to generalize one index 6 example in Table I to an infinite family using a union of cyclotomic classes. In fact, by our main theorem (Theorem 3.0.10), we shall obtain 2 more infinite families of strongly regular graphs. The constructions in [25, 27, 28] rely on explicit determination of index 2 and 4 Gauss sums. A major obstacle is the determination of Gauss sums of high index.

However, after studying [28] closely, we realized that in order to construct strongly regular Cayley graphs by using methods similar to those in [25, 27, 28], one does not need to evaluate Gauss sums of high indices explicitly; it suffices to know which subfield (of the cyclotomic field) the Gauss sums belong to.

We should remark that Koji Momihara gave a recursive construction of strongly regular Cayley graphs in [44], generalizing all but the first sporadic example in the statement of the Schmidt-White conjecture (Conjecture 1.0.1) into infinite families. His construction is useful and elegant, but is different from our method.

In this dissertation, we first generalize the construction of [28] to the index w case, where $w \geq 2$ is even. We shall show that the Cayley graphs defined in Chapter 3 have at most $w+1$ restricted eigenvalues. See Theorem 3.0.9. Furthermore, we shall give necessary and sufficient conditions for the candidate Cayley graphs to be strongly regular. The statements and proofs of the two conclusions constitute the main content of Chapter 3. After the proofs, we shall describe the three infinite families of strongly regular graphs obtained by using the results of Chapter 3.

As generalizations of regular graphs, a *d-class association scheme* can be viewed as d regular graphs defined on the same vertex set, whose union is a complete graph and they are interrelated in a specific way. The simplest association schemes are the schemes with one class, which contains no interesting information. The next simplest case, the symmetric schemes with two classes, can be seen to be equivalent to strongly regular graphs. We refer the reader to [3, 5, 14, 15, 29] for more examples of association schemes.

The Bose-Mesner algebra of an association scheme, was introduced in [10], is a powerful tool in the theory of association scheme. Let $A_0,\ A_1,\ \dots,\ A_d$ be the adjacency matrices of the regular graphs of a d-class association scheme. Then, all $\mathbb{R}$-linear combinations of $A_0,\ A_1,\ \dots,\ A_d$ form a Bose-Mesner algebra. If all primitive idempotents of this algebra have the same rank, we call the scheme *pseudocyclic*.

Next, we will define amorphic association schemes. Given a d-class association scheme, we can take unions of classes to form larger edge sets of graphs (we call this process *fusion*). Note that the fusion of a scheme may not be a scheme again. If every fusion of an association scheme gives rise to a new association scheme, the original association scheme is called *amorphic*.

It is clear that each nontrivial relation of an amorphic association scheme must be strongly regular. In [33], A. V. Ivanov conjectured that the converse is also true, that is: if each nontrivial relation in an association scheme is strongly regular, then the association scheme must be amorphic. This conjecture turned out to be false, even though it is true for the case $d = 3$. The first counterexample was given by Van Dam in the case where the association scheme is imprimitive. (See [18].) Later on, Van Dam [19] also gave a counterexample in the case where the association scheme is primitive. More counterexamples were given by Ikuta and Munemasa [32] in the primitive case.

It should be noted that only a few known counterexamples to Ivanov's conjecture in the primitive case had been known until [26] was published, and no infinite family of counterexample was found. Thus, our second main research topic is to construct more counterexamples to A. V. Ivanov's conjecture on amorphic association schemes. Our results in [26] actually gave 15 infinite families of pseudocyclic and non-amorphic association schemes.

Our constructions come from cyclotomic association schemes. Let $\mathbb{F}_q$ be the finite field of order q. Let N be a positive integer that divides $q - 1$ such that $1 < N < q - 1$. Let $C_0, C_1, \ldots, C_{N-1}$ be cyclotomic classes of order N of $\mathbb{F}_q$, defined as above. Then, $(\mathbb{F}_q, \{\{0\}, C_0, \ldots, C_{N-1}\})$ is an *N-class association scheme*. We call this scheme *cyclotomic*. We prove that the unions of cyclotomic classes decribed in Chapter 4 give rise to new association schemes and the fusion schemes are pseudocyclic (Defined in Chapter 2). The Bannai-Muzychuk criterion plays an important role in the proofs. The statements and proofs of this fact constitute the main content of Chapter 4. By the results in [25], there are 15 of the above fusion schemes in which each relation is a strongly regular graph but the schemes are not amorphic. The counterexamples will be given immediately after finishing the preparations of Section 4.1 and 4.2.

Here, we need to make three remarks. First, what we obtain from this method are infinite families of association schemes. Second, the fusion schemes are obviously not cyclotomic association schemes again. Third, two of the counterexamples are generalizations of those given by Ikuta and Munemasa in [32].

Chapter 2

PRELIMINARIES

The main purpose of this chapter is to define basic terminology and introduce some important properties and results in combinatorics, algebra and number theory. They serve as ingredients in the proofs of our results in Chapter 3 and 4. We assume the reader has basic knowledge in algebra and algebraic number theory. We refer the reader who is not familiar with them to [37] and [34].

We first summarize the contents of this chapter. Most of the proofs of this chapter can be found in the references. Some important proofs will be given for the convenience of the reader. This chapter contains 5 sections. In Section 2.1, we shall introduce characters, Fourier analysis on finite Abelian groups and Gauss sums. Section 2.2 will be devoted to introducing designs, differences sets, strongly regular graphs and Cayley graphs. In Section 2.3, we shall introduce necessary results from algebra and number theory, especially Stickelberger's theorem. In Section 2.4, we shall give a brief introduction to some known results in the construction of strongly regular graphs using a union of cyclotomic classes. The last section is a brief introduction to symmetric association schemes.

In order to avoid redundancy, the concepts that were formally introduced in the last chapter will not be repeated. Moreover, we list some conventions of the dissertation as follows. Let p be a prime and q be a power of p. Let $\mathbb{F}_p$ be the finite field of order p and $\mathbb{F}_q$ be the finite field of order q. The nonzero elements of $\mathbb{F}_q$ form a multiplicative cyclic group of order $q-1$, which is denoted as $\mathbb{F}_q^*$.

We begin by an introduction of algebraic tools including characters and Fourier analysis on Abelian groups. Our main goal of Section 2.1 is to introduce Gauss sums over finite fields.

2.1 Algebraic Tools

Let $\mathbb{C}$ be the field of complex numbers and $\mathbb{C}^*$ be the set of all nonzero elements of $\mathbb{C}$. Let $(G,\ +)$ be a finite (additive) abelian group of order n with identity element 0.

Definition 2.1.1. *A* **character** χ *of the group G is a group homomorphism from G to $\mathbb{C}^*$, i.e. $\chi(x_1+x_2)=\chi(x_1)\chi(x_2)$ for all $x_1,\ x_2 \in G$.*

The *principal character* χ_0 is defined by $\chi_0(x)=1$, for all $a \in G$. Let χ be a nonprincipal character of G. Then, $\chi(0)=1$. It immediately follows that $\chi(x)^n=1$ for any element x of G. This implies that $\chi(x)$ is an n^{th} root of unity. Hence, χ in fact maps G to U, the group of all n^{th} complex roots of unity.

Let χ and ψ be two characters of G. The *multiplication* of χ and ψ is defined by $\chi\cdot\psi(x)=\chi(x)\psi(x)$. Clearly, the map $\overline{\chi}$ defined by $\overline{\chi}(x)=\overline{\chi(x)}$ is also a character of G. By

$$\chi\cdot\overline{\chi}(x)=\chi(x)\overline{\chi(x)}=|\chi(x)|^2=1,$$

the inverse of χ is given by $\overline{\chi}$. Then, we have the following theorem:

Theorem 2.1.2. *The set of all characters defined on the finite abelian group G (additively written) is a multiplicative abelian group. We denote this group as $\widehat{G}$. The identity element of $\widehat{G}$ is χ_0. The inverse of the element χ is given by $\overline{\chi}$.*

The group $\widehat{G}$ is called the *dual* group of G. The following proposition plays a fundamental role in the theory of characters.

Proposition 2.1.3. ([39], Theorem 5.4) *If χ is a nonprincipal character of the finite abelian group G, then*

$$\sum_{x\in G}\chi(x)=0. \tag{2.1}$$

If $x \in G$ and $x \neq 0$, then

$$\sum_{\chi\in\widehat{G}}\chi(x)=0. \tag{2.2}$$

Proof: Since χ is not trivial, there exists an element $y \in G$ such that $\chi(y) \neq 1$. Note that $y + G = G$. From

$$\chi(y) \sum_{x \in G} \chi(x) = \sum_{x \in G} \chi(y + x) = \sum_{x \in G} \chi(x),$$

we have

$$(\chi(y) - 1) \sum_{x \in G} \chi(x) = 0.$$

The equality (2.1) follows because $\chi(y) \neq 1$. The equality (2.2) follows from similar arguments as above. □

The groups G and $\widehat{G}$ have the following relationship:

Theorem 2.1.4. ([2], Corollary 1.5) $G \cong \widehat{G}$.

We remark that there is no straightforward isomorphism between G and $\widehat{G}$. The following two *orthogonal relations* are very useful to our proofs.

Theorem 2.1.5. *Let χ and ψ be two characters of G, then*

$$\frac{1}{|G|} \sum_{x \in G} \chi(x)\overline{\psi(x)} = \begin{cases} 0, & \text{if } \chi \neq \psi \\ 1, & \text{if } \chi = \psi \end{cases}. \tag{2.3}$$

On the other hand, if x and y are two elements of G, then

$$\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(x)\overline{\chi(y)} = \begin{cases} 0, & \text{if } x \neq y \\ 1, & \text{if } x = y \end{cases}. \tag{2.4}$$

Proof: From Proposition 2.1, we have

$$\sum_{x \in G} (\chi \cdot \overline{\psi})(x) = 0,$$

when $\chi \cdot \overline{\psi} \neq \chi_0$. When $\chi \cdot \overline{\psi} = \chi_0$, we have

$$\sum_{x \in G} 1 = |G|.$$

Thus, (2.3) holds. Since

$$\sum_{\chi \in \widehat{G}} \chi(x)\overline{\chi(y)} = \sum_{\chi \in \widehat{G}} \chi(x-y), \tag{2.5}$$

the second sum in (2.5) is equal to 0 by Theorem 2.1. When $x = y$, by Theorem 2.1.4, the second sum in (2.5) is equal to

$$\sum_{\chi \in \widehat{G}} \chi(x-y) = \sum_{\chi \in \widehat{G}} \chi(0) = \sum_{\chi \in \widehat{G}} 1 = |\widehat{G}| = |G|.$$

Thus, (2.4) holds. □

Let $\mathbb{C}^G$ be the space of functions f from G to $\mathbb{C}$. Elements of $\mathbb{C}^G$ can be identified with vectors in the vector space $\mathbb{C}^n$ by

$$f \mapsto (f(g_1),\ \dots,\ f(g_n)),\ f \in \mathbb{C}^G.$$

It is easy to see that $\mathbb{C}^G$ is an n-dimensional vector space over $\mathbb{C}$. We define the *inner product* of two elements f and x of $\mathbb{C}^G$ by

$$(f,\ h) = \frac{1}{|G|} \sum_{x \in G} \overline{f(x)} h(x). \tag{2.6}$$

It is straightforward to prove the following proposition.

Proposition 2.1.6. ([2], Theorem 1.7) *$\widehat{G}$ forms an orthonormal basis in $\mathbb{C}^G$.*

Proof: By Theorem 2.1.5, any two distinct elements of $\widehat{G}$ are orthogonal. Also, by Theorem 2.1.4, we have $|\widehat{G}| = n = \dim \mathbb{C}^G$ and the theorem follows immediately. □

By Proposition 2.1.6, any f in $\mathbb{C}^G$ can be written as

$$f = \sum_{\chi \in \widehat{G}} c_\chi \chi,$$

where $c_\chi = (\chi,\ f)$. The coefficients c_χ are called the *Fourier coefficients* of the function f. The *Fourier transform* of the function f is defined by

$$\widehat{f}(\chi) = \sqrt{|G|} \cdot c_{\overline{\chi}} = \frac{1}{\sqrt{|G|}} \sum_{x \in G} f(x)\chi(x). \tag{2.7}$$

We state and prove the following two lemmas.

Lemma 2.1.7. (Fourier inversion formula) *Let G be a finite abelian group and f be a function from G to $\mathbb{C}$. Then, we have*

$$f(x) = \frac{1}{\sqrt{|G|}} \sum_{\chi \in \widehat{G}} \widehat{f}(\chi)\overline{\chi(x)}, \text{ for all } x \in G$$

Proof: The conclusion of the lemma immediately follows by Theorem 2.1.5. □

Define

$$|\widehat{f}(\chi)| = ((\overline{\chi},\ f) \cdot \overline{(\overline{\chi},\ f)})^{\frac{1}{2}}. \tag{2.8}$$

The last lemma we need is called *Parseval's identity.*

Lemma 2.1.8. (Parseval's identity) *Let G be an abelian group, and let f be a function from G to $\mathbb{C}$. Then, we have*

$$\sum_{a \in G} |f(x)|^2 = \sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2.$$

Proof: By (2.8), we have

$$\begin{aligned}
\sum_{\chi \in \widehat{G}} |\widehat{f}(\chi)|^2 &= \sum_{\chi \in \widehat{G}^*} \left[\left(\frac{1}{\sqrt{|G|}} \sum_{x \in G} f(x)\chi(x) \right) \left(\frac{1}{\sqrt{|G|}} \sum_{x \in G} \overline{f(x)\chi(x)} \right) \right] \\
&= \sum_{x \in G} \sum_{y \in G} f(x)\overline{f(y)} \left(\frac{1}{|G|} \sum_{\chi \in \widehat{G}} \chi(x)\overline{\chi(y)} \right) \\
&= \sum_{x \in G} |f(x)|^2.
\end{aligned}$$

□

Now, we introduce characters of finite fields. Let $\mathbb{F}_{q^m}$ be the finite field of order q^m. The *trace function* from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ is defined as follows.

Definition 2.1.9. *The* **trace** *is a function from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ defined by*

$$\begin{aligned}
\mathrm{Tr}_{q^m/q} : \quad \mathbb{F}_{q^m} &\to \mathbb{F}_q, \\
x &\mapsto x + x^q + \cdots + x^{q^{m-1}}.
\end{aligned} \tag{2.9}$$

If $\mathbb{F}_q$ is the prime field $\mathbb{F}_p$, the trace $\mathrm{Tr}_{q^m/p}$ from $\mathbb{F}_{q^m}$ to $\mathbb{F}_p$ is called the **absolute trace***.*

Trace functions have the following properties.

Proposition 2.1.10. ([39], Theorem 2.23) *The trace function* $\mathrm{Tr}_{q^m/q}$ *defined in (2.9) satisfies the following properties:*

(1) $\mathrm{Tr}_{q^m/q}(\alpha+\beta) = \mathrm{Tr}_{q^m/q}(\alpha) + \mathrm{Tr}_{q^m/q}(\beta)$ *for all* $\alpha,\ \beta \in \mathbb{F}_{q^m}$*.*

(2) $\mathrm{Tr}_{q^m/q}(c\cdot\alpha) = c\cdot\mathrm{Tr}_{q^m/q}(\alpha)$ *for all* $\alpha \in \mathbb{F}_{q^m}$ *and* $c \in \mathbb{F}_q$*.*

(3) $\mathrm{Tr}_{q^m/q}$ *is a linear functional from* $\mathbb{F}_{q^m}$ *to* $\mathbb{F}_q$*, where* $\mathbb{F}_{q^m}$ *is viewed as a vector space over* $\mathbb{F}_q$*.*

(4) $\mathrm{Tr}_{q^m/q}(\alpha) = m\cdot\alpha$ *for all* $\alpha \in \mathbb{F}_q$*.*

(5) $\mathrm{Tr}_{q^m/q}(\alpha^q) = \mathrm{Tr}_{q^m/q}(\alpha)$ *for all* $\alpha \in \mathbb{F}_{q^m}$*.*

Additive characters are defined over $\mathbb{F}_q$, where $(\mathbb{F}_q,\ +)$ is a finite additive Abelian group. Let ξ_p be a fixed complex primitive p^{th} root of unity, and $\mathrm{Tr}_{q/p}$ be the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$. The *additive character* ψ_a of $\mathbb{F}_q$ is given by

$$\psi_a(x) = \xi_p^{\mathrm{Tr}_{q/p}(ax)},\ \text{ where } a \in \mathbb{F}_q.$$

We usually write ψ_1 simply as ψ, which is called the *canonical* additive character of $\mathbb{F}_q$. It is easy to see that every additive character of $\mathbb{F}_q$ can be expressed in this way, i.e.,

$$\{\psi_a \mid a \in \mathbb{F}_q\} = \widehat{(\mathbb{F}_q,\ +)}. \tag{2.10}$$

Note that $(\mathbb{F}_q^*,\ \cdot)$ is a finite multiplicative Abelian group. The *multiplicative characters* of $\mathbb{F}_q$ are the characters of $\mathbb{F}_q^*$.

The following proposition follows from Proposition 2.1.3.

Proposition 2.1.11. *Let* ψ_a *be an additive character of* $\mathbb{F}_q$ *and* χ *be a nontrivial multiplicative character of* $\mathbb{F}_q$*. Then, we have*

$$\sum_{x\in\mathbb{F}_q} \psi_a(x) = \begin{cases} 0, & a \neq 0 \\ q, & a = 0, \end{cases}$$

and

$$\sum_{x\in\mathbb{F}_q^*} \chi(x) = 0.$$

Let N be a positive integer with $N \mid (q-1)$, and let χ be a multiplicative character of $\mathbb{F}_q$ of order N, i.e., N is the least positive integer such that $\chi^N = \chi_0$. The *Gauss sum* $g(\chi)$ of order N is defined by

$$g(\chi) = \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x). \tag{2.11}$$

We should remark that the Gauss sum $g(\chi)$ is just the Fourier coefficient $c_{\overline{\chi}}$ in the expansion of ψ with respect to the multiplicative characters, that is,

$$\psi(x) = \frac{1}{\sqrt{|\mathbb{F}_q^*|}} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \widehat{\psi}(\chi)\overline{\chi}(x) = \frac{1}{|\mathbb{F}_q^*|} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} g(\chi)\overline{\chi}(x) \tag{2.12}$$

In fact, by Lemma 2.1.7, we have

$$\begin{aligned} \frac{1}{|\mathbb{F}_q^*|} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} g(\chi)\overline{\chi}(x) &= \frac{1}{|\mathbb{F}_q^*|} \sum_{\chi \in \widehat{\mathbb{F}_q^*}} \left(\sum_{y \in \mathbb{F}_q^*} \chi(y)\psi(y) \right) \overline{\chi}(x) \\ &= \frac{1}{|\mathbb{F}_q^*|} \sum_{y \in \mathbb{F}_q^*} \psi(y) \left(\sum_{\chi \in \widehat{\mathbb{F}_q^*}} \chi(y-x) \right) \\ &= \frac{1}{|\mathbb{F}_q^*|} \cdot \psi(x) \left(\sum_{\chi \in \widehat{\mathbb{F}_q^*}} \chi(0) \right) = \psi(x). \end{aligned}$$

In the following, we shall concern ourselves with character sums. Let D be a subset of an Abelian group G. Then, *character sums* $\chi(D)$ are defined by

$$\chi(D) = \sum_{x \in D} \chi(x) \tag{2.13}$$

for χ in $\widehat{G}$. We shall show that character sums are closely related to eigenvalues of Cayley graphs and Gauss sums.

2.2 Combinatorial Structures

In this section, we start to introduce the basic definitions and properties of objects of study from combinatorics. Association schemes will be introduced in a separate section of this chapter. We begin by the definition of designs.

A 2-$(v,\ k,\ \lambda)$ *design* (*balanced incomplete block design*, BIBD) is a pair $S = (\mathcal{P},\ \mathcal{B})$ such that

(1) The set $\mathcal{P}$ is called *point set*. The elements of $\mathcal{P}$ are called *points*. Write $v = |\mathcal{P}|$.
(2) The set $\mathcal{B}$ is a collection of subsets of $\mathcal{P}$, each of size k. The set $\mathcal{B}$ is called the *block set*. Denote $b = |\mathcal{B}|$.
(3) For each point $P \in \mathcal{P}$ and $B \in \mathcal{B}$, we say P is incident with B, if $P \in B$.
(4) For every 2 points of $\mathcal{P}$, there are exactly λ blocks of $\mathcal{B}$ incident with both of them.

In the following, we assume that $v > k$. The Fisher inequality gives a necessary condition for the existence of a BIBD.

Theorem 2.2.1. ([52], Theorem 19.6) *For a* 2-$(v,\ k,\ \lambda)$ *design with* $v > k$*, we have* $b \geq v$*.*

We list some basic properties of a BIBD in the following proposition. The proof can be found in [52] (pp. 219).

Proposition 2.2.2. *Let* $S = (\mathcal{P}, \mathcal{B})$ *be a BIBD with* v *points and* b *blocks. Let* P *be a point. We use* r_P *denote the number of blocks incident with* P*. Then, we have*
(1) r_P *is a constant, i.e.* r_P *is unrelated to the choice of* P*.*
(2) $bk = vr$*.*
(3) $\lambda(v - 1) = r(k - 1)$*.*

In the dissertation, we mainly concern ourselves with so-called symmetric designs. A BIBD with $b = v$ is called a *symmetric design* or *square design*. Equivalently, a BIBD in which any two distinct blocks intersect at exactly λ points is a symmetric design. Particularly, a (v, k, λ)-symmetric design with $\lambda = 1$ is called a *projective plane*. We call $n = k - 1$ the *order* of the plane. By Proposition 2.2.2, we have $v = n^2 + n + 1$. Thus, parameters of a projective plane must have the form $(n^2+n+1, n+1, 1)$. We usually call blocks of a projective plane *lines*. The Fano plane (see below) is the (unique) projective plane of order 2. ([52], Example 19.6)

An example of projective planes is usually constructed as follows. Let $\mathbb{F}_q^3$ be the 3-dimensional vector space over $\mathbb{F}_q$. Let $\mathcal{P}$ be the collection of all 1-dimensional

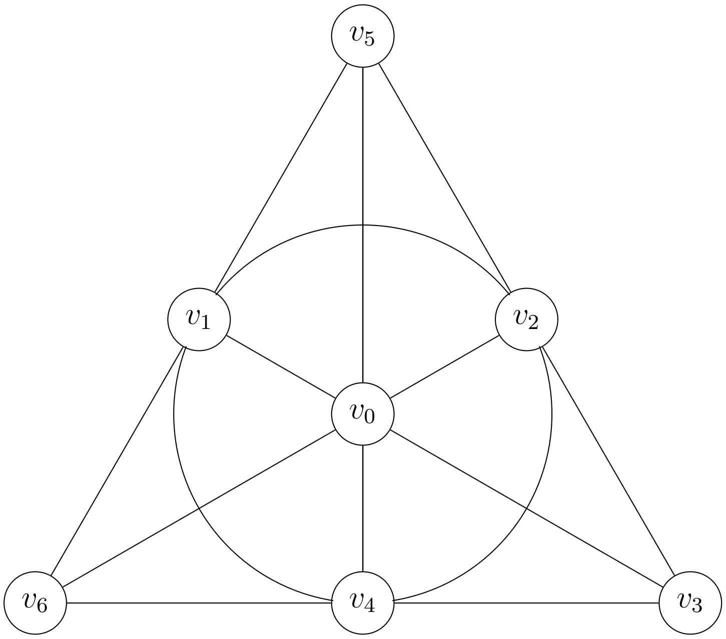

Figure 2.1: Fano plane

subspaces of $\mathbb{F}_q^3$ and $\mathcal{B}$ be the collection of all 2-dimensional subspaces of $\mathbb{F}_q^3$. If a 1-dimensional subspace is contained in a 2-dimensional subspace, we say that they are incident. It is easy to see that such structure is a BIBD with $\lambda = 1$. This vector space contains

$$\frac{q^3 - 1}{q - 1} = q^2 + q + 1$$

1-dimensional subspaces and the same number of 2-dimensional subspaces. Thus, the BIBD we constructed is symmetric. This is exactly a projective plane of order q. Usually, the design is denoted by $\mathrm{PG}(2, q)$. By the language of geometry, $\mathrm{PG}(2, q)$ stands for a projective geometry of dimension 2 over $\mathbb{F}_q$.

Now, we describe a more general case as follows. Let V be the d-dimensional vector space $\mathbb{F}_q^d$ for $d \geq 3$. We call the structure formed by the subspaces of V of dimension $k = 1, 2, \ldots, d-1$ the $(d-1)$-*projective geometry* $\mathrm{PG}(d-1, q)$. Furthermore, we call

$$\text{1-dimensional subspaces of } V \textit{points} \text{ of } \mathrm{PG}(d-1,\ q),$$

$$\text{2-dimensional subspaces of } V \textit{lines} \text{ of } \mathrm{PG}(d-1,\ q),$$

$$\vdots$$

$$(d-1)\text{-dimensional subspaces of } V \textit{hyperplanes} \text{ of } \mathrm{PG}(d-1,\ q).$$

The numbers of points and hyperplanes of $\mathrm{PG}(d-1,\ q)$ are both equal to $\frac{q^d-1}{q-1}$. It is easy to see that when $d=3$, $\mathrm{PG}(d-1,q)$ is just a projective plane of order q.

In the following, we shall focus on a special type of 2-$(v,\ k,\ \lambda)$ symmetric designs when $\lambda > 1$.

First, we define automorphism groups of a symmetric design. Two designs are *isomorphic* if there exists a bijection between the point sets which sends blocks to blocks and preserves incidence. This bijection is called an *isomorphism* of designs. An *automorphism* of a symmetric design is an isomorphism with itself. All automorphisms of a design form a group, where the operation of the group is functional composition. We call this group the *automorphism group* of the design. Of course, the automorphism group acts on both the point set and the block set of the symmetric design as a permutation group in the natural way.

A 2-$(v,\ k,\ \lambda)$ symmetric design is called *regular*, if there is an automorphism group G (written additively) of the design which acts on its point set regularly, and consequently acts on the block set regularly. (This bijection is usually called an *isomorphism* of a design.) For such a regular design, we identify the point set with the group G and a block B with a subset D of G. By the regularity of the action of G on the block set, the block set of the design will be given by $\{D+d \mid d \in G\}$, the set of *translations* of D. It immediately follows that $|(D+d)\cap D| = \lambda$ for any nonzero a of G. Thus, any nonzero element x of G has exact λ different representations as $x = d_1 - d_2$, $d_1, d_2 \in D$ and $d_1 \neq d_2$. In such a case, we call D (or any translate of D) a *difference set* of G. The following is the formal definition of difference sets as follows.

Definition 2.2.3. *Let G be an additively written group of size v and D be a subset of G of size k. Define the list of differences of D by $\Delta D = (d_1 - d_2 \ : \ d_1,\ d_2 \in D$ and $d_1 \neq d_2)$. We say that D is a $(v,\ k\ \lambda)$-difference set, if $\Delta D = \lambda(G \setminus \{0\})$.*

The following proposition is straightforward.

Proposition 2.2.4. *A regular 2-$(v,\ k,\ \lambda)$ symmetric design is nothing but a $(v,\ k,\ \lambda)$-difference set.*

In the study of differences sets, group rings and characters play fundamental roles. For a group G (written multiplicatively), the *group ring* $\mathbb{Z}[G]$ is the ring consisting of all elements of the form $\sum_{x\in G} a_x x$, where $a_x \in \mathbb{Z}$. The *addition* of two elements of $\mathbb{Z}[G]$ is defined by

$$\sum_{x\in G} a_x x + \sum_{x\in G} b_x x = \sum_{x\in G} (a_x + b_x) g.$$

The *scalar multiplication* of an integer a and an element $\sum_{g\in G} a_g g$ is defined by

$$a \cdot \left(\sum_{x\in G} a_x x \right) = \sum_{x\in G} (a a_x) x.$$

The *multiplication* of two elements of $\mathbb{Z}[G]$ is defined by

$$\left(\sum_{x\in G} a_x x \right) \cdot \left(\sum_{y\in G} b_y y \right) = \sum_{x\in G} \sum_{y\in G} a_x b_y x y.$$

Let $A = \sum_{g\in G} a_x x$ be an element of $\mathbb{Z}[G]$. We define $A^{(-1)} = \sum_{x\in G} a_x x^{-1}$.

It is convenient to determine a subset D of G (written multiplicatively with identity element 1) to be a difference set by using group ring notation. We identify a subset D of G with the element $\sum_{x\in D} x$ in $\mathbb{Z}[G]$, which will also be denoted by D. Then, the following lemma is straightforward but important.

Lemma 2.2.5. *A k-subset D of a group G (not necessarily Abelian) of order v is a $(v,\ k,\ \lambda)$-difference set in G if and only if the following identity holds:*

$$DD^{(-1)} = (k - \lambda) \cdot 1 + \lambda G. \tag{2.14}$$

Let χ be a character from an Abelian group G to $\mathbb{C}^*$. Denote $\sum_{x\in D}\chi(x)$ by $\chi(D)$. It is easy to see that $\chi(D^{(-1)}) = \overline{\chi(D)}$. Then, for Abelian groups, we have the following important lemma.

Lemma 2.2.6. *A k-subset D of an Abelian group G of order v is a $(v,\ k,\ \lambda)$-difference set in G if and only if*

$$|\chi(D)|^2 = \begin{cases} k-\lambda, & \text{for } \chi \neq \chi_0 \\ k^2, & \text{for } \chi = \chi_0 \end{cases} \tag{2.15}$$

Proof: Apply a character χ to both sides of (2.14), then (2.15) follows immediately from Proposition 2.1.3. For the converse direction, we will need the Fourier inversion formula. □

The following two examples are basic but important examples of difference sets.

Example: (Singer difference sets) Let $\mathrm{PG}(d-1, q)$ be the $(d-1)$-dimensional projective geometry over $\mathbb{F}_q$, where $d \geq 3$. Define an incidence structure $\mathcal{H} = (\mathcal{P},\ \mathcal{B})$ whose point set is the set of all points of $\mathrm{PG}(d-1,\ q)$ and block set $\mathcal{B}$ is the set of all hyperplanes of $\mathrm{PG}(d-1,\ q)$. A point P is said to be incident with a block B of $\mathcal{H}$, if P is contained in B. It is easy to see that $\mathcal{H}$ is a $(\frac{q^d-1}{q-1},\ \frac{q^{d-1}-1}{q-1},\ \frac{q^{d-2}-1}{q-1})$ symmetric design. Singer's theorem ([11], Theorem 6.2) says that $\mathcal{H}$ can be constructed from a difference set, which is called the Singer difference set. We should remark that when $d = 3$, the above construction leads to the classical projective plane of order q.

We construct Singer difference sets algebraically. Consider the quotient group $\mathbb{F}_{q^m}^*/\mathbb{F}_q^*$. Take a system L of coset representatives of $\mathbb{F}_q^*$ in $\mathbb{F}_{q^m}^*$ such that $\mathrm{Tr}_{q^m/q}$ maps L to $\{0,\ 1\}$. Define

$$L_0 = \{x \in L \mid \mathrm{Tr}_{q^m/q}(x) = 0\} \text{ and } L_1 = \{x \in L \mid \mathrm{Tr}_{q^m/q}(x) = 1\}.$$

Thus, $L = L_0 \cup L_1$. Then, L_0 is a $(\frac{q^m-1}{q-1},\ \frac{q^{m-1}-1}{q-1},\ \frac{q^{m-2}-1}{q-1})$-difference set, which is a Singer difference set. Yamamoto proved that $q\chi(L_0) = g(\chi)$ and $q\chi(L_1) = -g(\chi)$ for every nontrivial character $\chi \in \widehat{\mathbb{F}_{q^m}^*/\mathbb{F}_q^*}$. The proof can be found in [23]. We should remark that the significance of Yamamoto's result lies in revealing the connections between Singer difference sets (defined above) and Gauss sums.

Example: (Paley difference sets) For any finite field $\mathbb{F}_q$ where $q \equiv 3 (\text{mod } 4)$. The set S of all nonzero squares of $\mathbb{F}_q$. Then, S is a $(q,\ \frac{q-1}{2},\ \frac{q-3}{4})$-difference set. Such a difference set is called a *Paley difference set.*

Next, we shall develop the basic theory of strongly regular graphs. Let Γ be an srg$(v,\ k,\ \lambda,\ \mu)$ and A be the adjacency matrix of Γ. We say that a graph Γ^c is the *complement graph* of Γ, if they have the same vertex set and any two vertices of Γ^c are adjacent if and only if they are nonadjacent in Γ. A straightforward result is that Γ^c is srg$(v,\ v-k-1,\ v-2k+\mu-2,\ v-2k+\lambda)$.

Besides the examples listed in the first chapter, Paley graphs provide a family of interesting srgs. Let $q \equiv 1 (\text{mod } 4)$. The *Paley graph* Paley(q) is the graph with the finite field $\mathbb{F}_q$ as vertex set, where two vertices are adjacent when they differ by a (nonzero) square. It is strongly regular with parameters $(4t+1,\ 2t,\ t-1,\ t)$, where $q = 4t+1$. We should remark that the Paley graph Paley(q) is isomorphic to its complement.

The following theorem is a basic one in the theory of strongly regular graphs.

Theorem 2.2.7. ([14], Theorem 9.1.2) *For a regular graph Γ of order v and valency k, not complete nor edgeless, with adjacency matrix A, the following are equivalent:*
(1) Γ is an srg (v, k, λ, μ) for certain nonnegative integers λ, μ.
(2) $A^2 = (\lambda-\mu)A + (k-\mu)I + \mu J$ for certain real numbers λ and μ, where I, J are the identity matrix and the all-ones matrix, respectively.
(3) A has precisely two distinct restricted eigenvalues.

The proof of the above theorem is straightforward but it plays a fundamental role in the theory of strongly regular graphs. In fact, we shall show our theorem (Theorem 3.0.10) by using the equivalence between (1) and (3). For restricted eigenvalues of srgs, some basic properties are given in the following theorem.

Theorem 2.2.8. ([14], Theorem 9.1.3) *Let Γ be an srg (v, k, λ, μ). Set r and s to be restricted eigenvalues and f, g be their respective multiplicities. Then*

(1)

$$f,\ g = \frac{1}{2}\left\{v - 1 \pm \frac{(v-1)(\mu-\lambda)-2k}{\sqrt{(\mu-\lambda)^2+4(k-\mu)}}\right\}.$$

(2) $rs = \mu - k$ *and* $r + s = \lambda - \mu$.

(3) If r *and* s *are not integers, then* $f = g$ *and* $(v, k, \lambda, \mu) = (4t+1,\ 2t,\ t-1,\ t)$ *for some positive integer* t.

When $f \neq g$, r and s are both integers. The case of an srg with $f = g$ is called the *half case*. Such graphs are also called *conference graphs*. For conference graphs, their parameters must be the form $(4t+1,\ 2t,\ t-1,\ t)$. It is easy to see that Paley graphs are examples of the half-case, but there are many more examples. In Section 2.4, we shall see pseudocyclic association schemes are generalizations of the half-case srgs.

Finally, we discuss eigenvalues of Cayley graphs. From the following well-known theorem, we can see that eigenvalues of an Abelian Cayley graph are nothing but character sums. For the sake of convenience, we give a proof to this proposition here.

Proposition 2.2.9. *(See [14]) Let* G *be an Abelian group of order* n *and* $\Gamma = \mathrm{Cay}(G,\ D)$ *be a Cayley graph with the connection set* D. *Then, we have*

(1) The graph Γ *is regular.*

(2) The eigenvalues of Γ *are given by* $\chi(D) = \sum_{d\in D}\chi(d)$, *where* χ *ranges through all characters of* G.

Proof: Let x be a vertex of Γ. The number of edges incident with x is equal to $|\{x + a \mid a \in D\}| =: d_x$. Since $d_x = |D|$, Γ is a regular graph of valency $|D|$. This proves (1).

For (2), denote $V(\Gamma) = \{g_1,\ \ldots,\ g_n\}$ and $\widehat{G} = \{1 = \chi_0,\ \chi_1,\ \ldots,\ \chi_{n-1}\}$. It suffices to prove that

$$\begin{pmatrix}\chi_0(g_1)\\ \vdots \\ \chi_0(g_n)\end{pmatrix},\ \ldots,\ \begin{pmatrix}\chi_{n-1}(g_1)\\ \vdots \\ \chi_{n-1}(g_n)\end{pmatrix} \tag{2.16}$$

are linearly independent eigenvectors of the adjacency matrix A of Γ. Since

$$A\begin{pmatrix}\chi_i(g_1)\\ \vdots\\ \chi_i(g_n)\end{pmatrix}=\begin{pmatrix}\sum_{g_j\sim g_1}\chi_i(g_j)\\ \vdots\\ \sum_{g_j\sim g_n}\chi_i(g_j)\end{pmatrix}=\begin{pmatrix}\sum_{d\in D}\chi_i(g_1+d)\\ \vdots\\ \sum_{d\in D}\chi_i(g_n+d)\end{pmatrix}$$

$$=\begin{pmatrix}\chi_i(g_1)\chi_i(D)\\ \vdots\\ \chi_i(g_n)\chi_i(D)\end{pmatrix}=\chi_i(D)\begin{pmatrix}\chi_i(g_1)\\ \vdots\\ \chi_i(g_n)\end{pmatrix},$$

we have $(\chi_i(g_1),\ \ldots,\ \chi_i(g_n))^T$ is an eigenvector of the adjacency matrix A with respect to an eigenvalue $\chi_i(D)$. Moreover, by Corollary 2.1.5, the vectors in (2.16) are linearly independent. Thus, all the eigenvalues of Γ are given by $\chi(D)=\sum_{d\in D}\chi(d)$, where $\chi\in\widehat{G}$. □

By Theorem 2.1.5, we have $\sum_{i=1}^{n}\chi_j(g_i)\chi_0(g_i)=0$, when $j\neq 0$. It follows that the eigenvector associated to $\chi(D)$ is othorgonal to $\mathbf{1}$, when $\chi\neq\chi_0$. It follows that the eigenvectors associated to the eigenvalue $\chi(D)$ cannot be a multiple of $\mathbf{1}$. Thus, $\chi(D)$, $\chi\neq\chi_0$, are restricted eigenvalues of $\mathrm{Cay}(G,D)$. Furthermore, by the above proposition, the restricted eigenvalues of a Cayley graph $\mathrm{Cay}(G,D)$ are given by $\chi(D)$, where $\chi\neq\chi_0$.

We remark that eigenvalues of a Cayley graph over $(\mathbb{F}_q,+)$ are given by $\psi_a(D)$ for $a\in\mathbb{F}_q$ by (2.10).

As an example, we compute the spectrum of the following Cayley graph. The (undirected) pentagon is the Cayley graph $\mathrm{Cay}(\mathbb{Z}_5,\{\pm1\})$. The spectrum of the pentagon is

$$\{\xi+\xi^{-1}\mid\xi^5=1\}=\{2,\ \frac{-1+\sqrt{5}}{2}(\text{ multiplicity }2),\ \frac{-1-\sqrt{5}}{2}(\text{multiplicity }2)\}.$$

We now introduce cyclotomy of finite fields. Let γ be a primitive element of $\mathbb{F}_q$. Let $C_0,\ C_1,\ \ldots,\ C_{N-1}$ be the cyclotomic classes of order N. Let $\psi(x)$ be the canonical additive character of $\mathbb{F}_q$. Define N^{th} *cyclotomic periods* (or *Gauss periods*) by

$$\tau_a=\sum_{x\in C_a}\psi(x),\ 0\leq a\leq N-1.$$

Next, some basic properties of cyclotomic periods are presented in the following proposition. The second item of the theorem below reveals the connection between eigenvalues of the Cayley graphs with connection set C_a, $0 \le a \le N-1$, and Gauss sums. It plays an important role in our first research project.

Proposition 2.2.10. *Let γ be a primitive element of $\mathbb{F}_q$ and τ_a be N^{th} cyclotomic periods defined as above, $0 \le a \le N-1$. Write $C_0^{\perp} = \{\chi \in \widehat{\mathbb{F}_q^*} \mid \chi(x) = 1, \forall x \in C_0\}$. Then, we have*

(1) $\tau_a = \psi_{\gamma^a}(C_0)$

(2) $\tau_a = (1/N)\sum_{\chi \in C_0^{\perp}} g(\overline{\chi})\chi(\gamma^a)$.

Proof: (1) we have

$$\psi_{\gamma^a}(C_0) \;=\; \sum_{x\in C_0}\psi_{\gamma^a}(x) = \sum_{x\in C_0}\psi(\gamma^a x) = \sum_{x\in C_a}\psi(x) = \tau_a.$$

(2) we have

$$\begin{aligned}
\tau_a &= \sum_{x\in C_a}\psi(x)\\
&= \sum_{x\in C_a}\frac{1}{q-1}\sum_{\chi\in\widehat{\mathbb{F}_q^*}} g(\overline{\chi})\chi(x) \text{ by (2.12)}\\
&= \frac{1}{q-1}\sum_{\chi\in\widehat{\mathbb{F}_q^*}} g(\overline{\chi})\sum_{x\in C_a}\chi(x)\\
&= \frac{1}{q-1}\sum_{\chi\in\widehat{\mathbb{F}_q^*}} g(\overline{\chi})\sum_{x\in C_0}\chi(\gamma^a x)\\
&= \frac{1}{q-1}\sum_{\chi\in\widehat{\mathbb{F}_q^*}} g(\overline{\chi})\chi(\gamma^a)\sum_{x\in C_0}\chi(x)\\
&= \frac{1}{q-1}\sum_{\chi\in\widehat{\mathbb{F}_q^*}} g(\overline{\chi})\chi(\gamma^a)\sum_{x\in C_0^{\perp}}\chi(x)\\
&= \frac{|C_0|}{q-1}\sum_{\chi\in C_0^{\perp}} g(\overline{\chi}) = \frac{1}{N}\sum_{\chi\in C_0^{\perp}} g(\overline{\chi})\chi(\gamma^a)
\end{aligned}$$

□

Cyclotomic periods are closely related to eigenvalues of $\mathrm{Cay}(\mathbb{F}_q, D)$, where D is one single class or a union of cyclotomic classes.

If the connection set D is a single class, i.e., $D = C_0$, the restricted eigenvalues of the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ are exactly $\tau_0, \ \ldots, \ \tau_{N-1}$. This can be seen as follows. By Proposition 2.2.9, the restricted eigenvalues of $\mathrm{Cay}(\mathbb{F}_q, D)$ are given by $\psi(D)$ for nontrivial additive characters ψ of $\mathbb{F}_q$. Notice that $\widehat{(\mathbb{F}_q, +)} = \{\psi_a \mid a \in \mathbb{F}_q\}$. It suffices to prove that if a_1 and a_2 are two nonzero elements of $\mathbb{F}_q$ such that a_1/a_2 is a power of γ^N, then $\psi_{a_1}(D) = \psi_{a_2}(D)$. Write $a_1 = \gamma^{i_1 N+j}$ and $a_1 = \gamma^{i_2 N+j}$. Then, the above equality can be viewed by

$$\psi_{a_1}(D) = \sum_{x \in C_0} \psi(\gamma^{i_1 N+j} x) = \sum_{x \in C_0} \psi(\gamma^{i_2 N+j} x) = \psi_{a_2}(D).$$

Thus, the restricted eigenvalues of $\mathrm{Cay}(\mathbb{F}_q, D)$ are given by $\psi_{\gamma^a}(D)$, i.e., τ_a for $0 \le a \le N-1$.

If the connection set D is a union of cyclotomic classes of order N, say $D = \cup_{i \in I} C_i$, the restricted eigenvalues of $\mathrm{Cay}(\mathbb{F}_q, \ D)$ will be given by sums of cyclotomic periods, i.e., $\psi_{\gamma^a}(D) = \psi(\gamma^a D) = \sum_{i \in I} \tau_{i+a}$, $0 \le a \le N-1$.

By Proposition 2.2.10, $\psi_{\gamma^a}(D)$, $0 \le a \le N-1$, are determined by evaluating certain Gauss sums. The determination of Gauss sums is difficult in general. Explicit evaluations of Gauss sums are known only in a few cases. Using Stickelberger's theorem and other number theoretic tools introduced in the next section, we shall compute Gauss sums in certain cases.

2.3 Number Theoretic Tools

The main purpose of this section is to introduce some important properties of Gauss sums. We introduce basic terminology and properties of cyclotomic fields, we shall describe how to compute character sums through the evaluation of certain Gauss sums. Our treatment will be concise, developing only those aspects that will be needed in Chapter 3 and 4. The reader who is interested in a more systematic treatment of cyclotomic fields should consult one of the references, [34], [38] and [54].

Let $N > 1$ be a positive integer and $\xi_N = e^{2\pi i/N}$, a complex primitive N^{th} root of unity. Let $\mathbb{Z}/N\mathbb{Z}$ be the congruence classes modulo N and $(\mathbb{Z}/N\mathbb{Z})^*$ be the set of units of $\mathbb{Z}/N\mathbb{Z}$. Let ϕ be the Euler totient function. Thus, we have $|(\mathbb{Z}/N\mathbb{Z})^*| = \phi(N)$.

The field $\mathbb{Q}(\xi_N)$ is the splitting field of the polynomial $x^N - 1$ over $\mathbb{Q}$. This implies that $\mathbb{Q}(\xi_N)/\mathbb{Q}$ is a Galois extension. Let $G = \mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q})$. A well-known result is that the Galois group G is isomorphic to $(\mathbb{Z}/N\mathbb{Z})^*$. (See [34], Section 13.2.) Moreover, it is well known that $\mathbb{Z}[\xi_N]$ is the ring of integers of $\mathbb{Q}(\xi_N)$. $\mathbb{Z}[\xi_N]$ is a Dedekind domain, which means every nonzero proper ideal factors into a product of prime ideals. Every prime ideal of $\mathbb{Z}[\xi_N]$ is maximal. ([34], Corollary 2.) Therefore, if P is a prime ideal of $\mathbb{Z}[\xi_N]$ containing p, $\mathbb{Z}[\xi_N]/P$ is a finite field of characteristic p.

Let s and t be relatively prime integers. We use $\mathrm{ord}_s(t)$ to denote the multiplicative order of t modulo s. Write $(p) = p\mathbb{Z}[\xi_N]$. The following theorem completely determine the factorization of a prime p in $\mathbb{Z}[\xi_N]$.

Theorem 2.3.1. ([41], Theorem 8.8) *Let m be a positive integer and let p be a prime. Write $N = N'p^a$, where $\gcd(N',\ p) = 1$ and $a \geq 0$. Then, p factors in $\mathbb{Z}[\xi_N]$ as*

$$(p) = (P_1 \dots P_t)^{\phi(p^a)},$$

where $P_1,\ \dots,\ P_t$ are all prime ideals in $\mathbb{Z}[\xi_N]$ containing p and $t = \phi(N')/\mathrm{ord}_{N'}(p)$.

Let σ_p be the automorphism of $\mathbb{Q}[\xi_N]$ sending ξ_N to ξ_N^p. Then, we have

Proposition 2.3.2. ([34] pp. 197, Corollary) *Let p be a prime such that $p \nmid N$. If P is a prime ideal lying over on the prime p, then the group $G(P) = \{\sigma \in G \mid \sigma(P) = P\}$ is the cyclic group generated by σ_p.*

We call $G(P)$ the *decomposition group* of P. Let K be the *decomposition field* of p in $\mathbb{Q}(\xi_N)$, that is, $K = \{x \in \mathbb{Q}(\xi_N) \mid \sigma(x) = x,\ \text{for all } \sigma \in G(P)\}$. The Galois group of the extension of $K/\mathbb{Q}$ is as follows.

Proposition 2.3.3. *Let K be defined as above. Then, we have* $\mathrm{Gal}(K/\mathbb{Q}) = (\mathbb{Z}/N\mathbb{Z})^*/\langle p\rangle$.

Proof: Notice that K is the fixed field of the group $\langle \sigma_p \rangle$. Then, by Theorem 1.10 in Lang's book ([36], p. 265), $\langle p \rangle \cong H$, the Galois group of the extension $\mathbb{Q}(\xi_N)/\mathbb{K}$. It immediately follows that $\text{Gal}(\mathbb{K}/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*/\langle p \rangle$. □

Let ξ_p be a primitive p^{th} root of unity. Then, Gauss sums of order N defined in (2.11) belong to $\mathbb{Z}[\xi_N, \xi_p]$, the integer ring of $\mathbb{Q}(\xi_N, \xi_p)$. Define $\sigma_{a,b}$ to be the Galois automorphism of $\mathbb{Q}(\xi_N, \xi_p)$ by

$$\sigma_{a,b}(\xi_N) = \xi_N^a,\ \ \sigma_{a,b}(\xi_p) = \xi_p^b$$

The following lemma gives some useful properties of Gauss sums. For a proof of the lemma, we refer the reader to [9, p. 10] and [34, p. 208].

Lemma 2.3.4. *Let χ be a multiplicative character of $\mathbb{F}_q$ of order N. Then*
(1) $g(\chi) = -1$, if $\chi = \chi_0$, and $|g(\chi)|^2 = q$, if $\chi \neq \chi_0$.
(2) $\sigma_{a,b}(g(\chi)) = \overline{\chi}^a(b) g(\chi^a)$, where $\overline{\chi} = \chi^{-1}$.
(3) $\overline{g(\chi)} = \chi(-1) g(\overline{\chi})$, and $\sigma_{p,1}(g(\chi)) = g(\chi^p) = g(\chi)$.
(4) For a character of χ of order N, $g(\chi)^N \in \mathbb{Z}[\xi_N]$.

The first item of the above lemma gives the modulus of Gauss sums, but we need to evaluate Gauss sums in many cases. Using the following Stickelberger's theorem, certain types of Gauss sums can be determined explicitly.

Theorem 2.3.5. (Stickelberger's Theorem, see [9], Theorem 11.2.2) *Let G be the Galois group of $\mathbb{Q}(\xi_N)/\mathbb{Q}$ and $\mathbb{Z}[G]$ be the group ring. For a Gauss sum $g(\chi)$ of order N over $\mathbb{F}_q$, there exist a prime ideal P of $\mathbb{Z}[\xi_N]$ containing p and an element $\alpha = \sum_{a=1,\ \gcd(a,\ m)=1}^{N-1} a\sigma_a^{-1}$ in $\mathbb{Z}[G]$ such that*

$$(g(\chi)^N)\mathbb{Z}[\xi_N] = P^{\alpha} \tag{2.17}$$

For the proof of Stickelberger's theorem, we refer the monographs [9] or [34]. By Theorem 2.2.10, the evaluation of Gauss sums in some cases provides a feasible approach to determine cyclotomic periods, which are closely related to eigenvalues of a Cayley graph. In the next section, we shall determine some types of Gauss sums by using this theorem.

2.4 Some Known Constructions Of Strongly Regular Graphs

Let $N > 1$ be a proper divisor of $q-1$. Let γ be a primitive element of $\mathbb{F}_q$ and $C_0, \ldots, C_{N-1}$ be the cyclotomic classes of order N. Let ψ be the canonical additive character of $\mathbb{F}_q$. We construct Cayley graphs $\mathrm{Cay}(\mathbb{F}_q, D)$ with the connection set D being one single class or a union of some classes.

Based on the remarks at the end of Section 2.3, the eigenvalues of a Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ are given by $\psi_{\gamma^a}(D)$, $0 \le a \le N-1$. Thus, a Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ is an srg if and only if $|\{\psi_{\gamma^a}(D) \mid 0 \le a \le N-1\}| = 2$.

When the connection set D is a single class, i.e., $D = C_0$, the eigenvalues of the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D)$ are given by τ_a, $0 \le a \le N-1$. Thus, the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, C_0)$ is an srg if and only if $|\{\tau_a \mid 0 \le a \le N-1\}| = 2$. The simplest case is when D is the multiplicative group of a subfield $\mathbb{F}_{p^{f'}}$ of $\mathbb{F}_{p^f}$. Set $k = |C_0|$. In this case, $\psi(C_0)$, $\psi \in \widehat{(\mathbb{F}_q, +)}$ and $\psi \neq \psi_0$, take only two values as follows:

$$\psi(C_0) = \begin{cases} -1, & \text{if } \psi|_{\mathbb{F}_{p^{f'}}} \neq 1, \\ k, & \text{if } \psi|_{\mathbb{F}_{p^{f'}}} = 1. \end{cases}$$

This implies that $\mathrm{Cay}(\mathbb{F}_q, C_0)$ is an srg.

The next interesting case is when $-1 \in \langle p \rangle$, the cyclic subgroup generated by p in $\mathbb{Z}/N\mathbb{Z}$, or equivalently, there exists a positive integer t such that $-1 \equiv p^t \pmod{N}$. We call this case *semi-primitive*. In the semi-primitive case, τ_a, $0 \le a \le N-1$, take only two values, that is, we actually obtain an srg. To describe this procedure, we first cite the following theorem.

Theorem 2.4.1. ([9], Theorem 11.6.3) *Let $N > 2$ be an integer. If there exists a positive integer t such that $-1 \equiv p^t \pmod{N}$, with t chosen minimal. Let χ be a (multiplicative) character of order N of $\mathbb{F}_{p^f}$. (This implies that $N \mid p^f - 1$.) Then, $f = 2ts$ for some positive integer s. Let $g(\chi)$ be the Gauss sum on $\mathbb{F}_{p^f}$. Then, we have*

$$g(\chi) = \begin{cases} (-1)^{s-1} p^{ts}, & p = 2 \\ (-1)^{s-1+\frac{(p^t+1)s}{N}} p^{ts}, & p > 2. \end{cases}$$

By the above theorem, Gauss sums are completely determined in the semi-primitive case. The proof of this theorem was given in [9]. In fact, we are more interested in the number of eigenvalues of a Cayley graph in the semi-primitive case. It is easy to see that $\tau_a \in \mathbb{Q}(\xi_p)$, $0 \le a \le N-1$. The cyclotomic periods of order N are called *uniform*, if there exists a constant τ and a positive integer c such that $\tau_i = \tau$ all but $i = c$. By Theorem 2.4.1, we have the following corollary, which actually completely determines the values of eigenvalues of a Cayley graph in the semi-primitive case.

Corollary 2.4.2. *Let p be a prime, $N \ge 2$, $q = p^{2ts}$, where $s \ge 1$ and $-1 \equiv p^t (\text{mod } N)$ with t chosen minimal. Then, we have*

$$\begin{cases} \tau_{N/2} = \sqrt{q} - \dfrac{\sqrt{q}+1}{N};\ \tau_i = -\dfrac{\sqrt{q}+1}{N}, i \neq N/2 & \textit{where } s,\ p,\ \frac{\sqrt{q}+1}{N} \textit{ are all odd} \\ \tau_0 = (-1)^{s-1}\sqrt{q} + \dfrac{(-1)^s\sqrt{q}-1}{N};\ \tau_i = \dfrac{(-1)^s\sqrt{q}-1}{N}, i \neq 0 & \textit{otherwise.} \end{cases}$$

By the above theorem, we actually show that the Gauss periods are uniform in the semi-primitive case. We remark that the converse is also true, which was proved in [8].

The following corollary is straightforward by Corollary 2.4.2.

Corollary 2.4.3. *Let $N > 1$ be a proper divisor of $q-1$, and γ be a primitive element of $\mathbb{F}_q$. Let $C_0, \ldots, C_{N-1}$ be the cyclotomic classes of order N. If there exists a positive integer t such that $-1 \equiv p^t (\text{mod } N)$, then the union of any t classes $D = C_{i_1} \cup \cdots \cup C_{i_t}$, where $i_1 < \cdots < i_t$, generates a strongly regular Cayley graph.*

Schmidt and White proposed a conjecture that a cyclotomic srg must be one of 11 sporadic examples in Table I, besides the subfield examples and the semi-primitive examples. Until now, no further exceptional example has been found. (See [49].) In order to construct more srgs by using cyclotomic classes of finite fields, we use a union of cyclotomic classes as the connection set of a Cayley graph instead of one single class.

Let D be a union of cyclotomic classes $D = \cup_{i \in I} C_i$ for a subset I of $\{0, \ldots, N-1\}$. It is easy to see that the eigenvalues of the Cayley graph $\text{Cay}(\mathbb{F}_q, D)$ are essentially determined by cyclotomic periods, i.e., τ_a, $0 \le a \le N-1$. By Theorem 2.2.10, we compute cyclotomic periods through the evaluation of certain Gauss sums.

The first interesting case is the index 2 case, that is, $-1 \notin \langle p \rangle$ and $\langle p \rangle$ has index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$. We summarize the known results in this case. Many authors including McEliece [43], Langevine [36], Mbodj [42], Meijer and Van der Vlugt[45] studied the index 2 case. Finally, the Gauss sums of order N in the index 2 case are completed determined in [56]. Based on their results, we have the following constructions.

First, in the index 2 case, it can be shown that N has at most two odd prime divisors. Assuming that N is odd, we have the following three possibilities in the index 2 case (see [56]), where both p_1 and p_2 are primes.

(1) $N = p_1^m$, $p_1 \equiv 3 \pmod 4$;

(2) $N = p_1^m p_2^n$, $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$;

(3) $N = p_1^m p_2^n$, $p_1 \equiv 1, 3 \pmod 4$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$ and $p_2 \equiv 3 \pmod 4$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)/2$.

In the first case, we cite the following result about the evaluation of Gauss sums of order N, where $N = p_1^m$, $m \ge 1$.

Theorem 2.4.4. (Langevin, [36]) *Let $N = p_1^m$, where m is a positive integer, p_1 is a prime such that $p_1 > 3$ and $p_1 \equiv 3 \pmod 4$. Let p be a prime such that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = 2$ (that is, $f =: \mathrm{ord}_N(p) = \phi(N)/2$) and let $q = p^f$. Let χ be a multiplicative character of order N of $\mathbb{F}_q$, and h be the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then the Gauss sum $g(\chi)$ over $\mathbb{F}_q$ is determined up to complex conjugation by*

$$g(\chi) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0},$$

where

(1) $h_0 = \frac{f-h}{2}$,

(2) $b, c \not\equiv 0 \pmod p$,

(3) $b^2 + p_1 c^2 = 4p^h$,

(4) $bp^{h_0} \equiv -2 \pmod{p_1}$.

With the above theorem, Feng and Xiang obtained the following result in [25].

Theorem 2.4.5. (Feng and Xiang, [25]) *Let $p_1 \equiv 3 (\text{mod } 4)$ be a prime, $p_1 \neq 3$, $N = p_1^m$, and let p be a prime such that $f := \text{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and*

$$D = \cup_{i=0}^{p_1^{m-1}-1} C_i \subset \mathbb{F}_q^*.$$

Moreover, assume that $1 + p_1 = 4p^h$, where h is the class number of $\mathbb{Q}(\sqrt{-p_1})$. Then, $Cay(\mathbb{F}_q, D)$ is an srg.

We remark that it is a good question to generalize the above theorem to the case when $p_1 = 3$.

The second case was completely determined by Feng, Momihara and Xiang in [25, 27]. First, we cite the following theorem.

Theorem 2.4.6. (Mbodj, [42]) *Let $N = p_1^m p_2^n$, where m, n are positive integers, p_1 and p_2 are prime such that $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, $\text{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\text{ord}_{p_2^n}(p) = \phi(p_2^n)$. Let p be a prime such that $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle] = 2$ (that is, $f := \text{ord}_N(p) = \phi(N)/2$) and let $q = p^f$. Let χ be a multiplicative character of order N of $\mathbb{F}_q$, and h be the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$. Then the Gauss sum $g(\chi)$ over $\mathbb{F}_q$ is determined up to complex conjugation by*

$$g(\chi) = \frac{b + c\sqrt{-p_1p_2}}{2} p^{h_0},$$

where

(1) $h_0 = \frac{f-h}{2}$,

(2) $b, c \not\equiv 0 \pmod p$,

(3) $b^2 + p_1p_2c^2 = 4p^h$,

(4) $b \equiv 2p^{h/2} \pmod \ell$, here $\ell \in \{p_1, p_2\}$ is the prime congruent to 3 modulo 4.

With the above theorem, Feng and Xiang proved the following theorem.

Theorem 2.4.7. (Feng and Xiang, [25]) *Let $\{p_1 (\text{mod } 4), p_3 (\text{mod } 4)\} = \{1, 3\}$ be two primes and $N = p_1^m p_2$. Let p be a prime such that $\text{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\text{ord}_{p_2}(p) = \phi(p_2)$ and $f := \text{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and*

$$D = \cup_{i=0}^{p_1^{m-1}-1} C_{ip_2} \subset \mathbb{F}_q^*.$$

Moreover, assume that

$$\begin{aligned} p_1 &= 2p^{h/2} + (-1)^{(p_1-1)/2} b \\ p_2 &= 2p^{h/2} - (-1)^{(p_1-1)/2} b \\ p_1 p_2 &= 4p^h - 1 \end{aligned}$$

where h is the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$, h is even and $b \in \{1, -1\}$. Then, $Cay(\mathbb{F}_q, D)$ is an srg.

More recently, Feng, Momihara and Xiang in [27] generalized the above theorem based on the following theorem.

Theorem 2.4.8. ([56], Case B1; Theorem 4.10) *Let $N = p_1^m p_2^n$, where m and n are positive integers, p_1 and p_2 are primes such that $p_1 \equiv 1 (\text{mod } 4)$ and $p_2 \equiv 3 (\text{mod } 4)$. Let p be a prime such that $\text{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\text{ord}_{p_2^n}(p) = \phi(p_2^n)$ and $f := \text{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and χ be a character of order N of $\mathbb{F}_q$. Then, for $0 \le s \le m-1$ and $0 \le t \le n-1$, we have*

$$\begin{aligned} g(\chi^{p_1^s p_2^t}) &= p^{\frac{f - h p_1^s p_2^t}{2}} \left(\frac{b + c\sqrt{-p_1p_2}}{2} \right), \\ g(\chi^{p_1^m p_2^t}) &= -p^{\frac{f}{2}}, \\ g(\chi^{p_1^s p_2^n}) &= p^{\frac{f}{2}}, \end{aligned}$$

where h us the class number of $\mathbb{Q}(\sqrt{-p_1p_2})$, and b and c are integers determined by $b, c \not\equiv 0 (\text{mod } p)$, $4p^h = b^2 + p_1p_2c^2$, and $bp^{\frac{f-h}{2}} \equiv 2 (\text{mod } p_1p_2)$.

In [27], Feng, Momihara and Xiang proved the following theorem:

Theorem 2.4.9. (Feng, Momihara and Xiang, [27]) *Let $N = p_1^m p_2^n$, where m and n are positive integers, p_1 and p_2 are primes such that $p_1 \equiv 1 (\text{mod } 4)$ and $p_2 \equiv 3 (\text{mod } 4)$. Let p be a prime such that $\text{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\text{ord}_{p_2^n}(p) = \phi(p_2^n)$ and $f := \text{ord}_N(p) = \phi(N)/2$. Let $q = p^f$ and*

$$D = \cup_{i=0}^{p_1^{m-1}-1} \cup_{j=0}^{p_2^{n-1}-1} C_{ip_2^n + jp_1^m} \subset \mathbb{F}_q^*.$$

Moreover, assume that

$$\begin{aligned} p_1 &= 2p^{h/2} + b \\ p_2 &= 2p^{h/2} - b \\ p_1 p_2 &= 4p^h - 1 \end{aligned}$$

where h is the class number of $\mathbb{Q}(\sqrt{-p_1 p_2})$, h is even and $b \in \{1, -1\}$. Then, Cay$(\mathbb{F}_q, D)$ is an srg.

The next case we are interested is the index 4 case. Based on the results in [24], Ge, Xiang and Yuan in [28] constructed strongly regular Cayley graphs by using unions of cyclotomic classes as connection sets. In [28], they found two infinite families of srgs.

For the index 6 case, the main obstacle is that the evaluation of Gauss sums is not done. (This is an open problem.) After we closely studied the proofs in [28], it is realized that the explicit determination is not necessary. We shall give the statement of the theorem and its proof in Chapter 3.

2.5 Symmetric Association Schemes

This section contains a short account of the basic theory of association schemes. For the reader who is interested in association schemes, we recommend the references [5, 15, 29]. We shall present the Bannai-Muzychuk theorem, which is important to our proofs in Chapter 4.

Definition 2.5.1. *Let X be a finite set of size v. A* **symmetric association scheme** *with d classes is X together with $d+1$ distinct subsets R_i, $i = 0, \ldots, d$, of $X \times X$ such that*

(1) The sets $R_0, \ldots, R_d$ form a partition of $X \times X$ with $R_0 = \{(x, x) \mid x \in X\}$.

(2) If $x, y \in X$, if $(x, y) \in R_i$, then $(y, x) \in R_i$.

(3) For any $(x, y) \in R_k$ the number p_{ij}^k of $z \in X$ with $(x, z) \in R_i$ and $(z, y) \in R_j$ depends only on i, j and k. The numbers p_{ij}^k are called the **intersection numbers** *of the association scheme.*

In the following, we give some straightforward examples of association schemes. We leave to the reader to verify them with the above definition.

(1) A strongly regular graph and its complement form a symmetric 2-class association scheme. Let X be a set of size v. Denote Γ as a strongly regular graph srg$(v,\ k,\ \lambda,\ \mu)$. Then, the complement graph of Γ is a srg$(v,\ v-k-1,\ v-2k+\mu-2,\ v-2k+\lambda)$. Set

$$\begin{aligned} R_0 &= \{(x,\ x) \mid x \in X\}, \\ R_1 &= \{(x,\ y) \mid xy \text{ is an edge of the graph } \Gamma\}, \\ R_2 &= \{(x,\ y) \mid xy \text{ is not an edge of the graph } \Gamma\}. \end{aligned}$$

Thus, we can prove that $(X,\ \{R_0,\ R_1,\ R_2\})$ is a 2-class association scheme.

(2) Let X be a set of size of v and Ω be the collection of all 2-subset of X. Then, $|\Omega| = v(v-1)/2$. Define $R_0,\ R_1,\ R_2$ as follows:

$$\begin{aligned} R_0 &= \{(\alpha,\ \alpha) \mid \alpha \in \Omega\}, \\ R_1 &= \{(\alpha,\ \beta) \mid \alpha,\ \beta \in \Omega, \ \text{ and } |\alpha \cap \beta| = 1\}, \\ R_2 &= \{(\alpha,\ \beta) \mid \alpha,\ \beta \in \Omega, \ \text{ and } |\alpha \cap \beta| = 0\}, \end{aligned}$$

Then, one can show that $(\Omega,\ \{R_0,\ R_1,\ R_2\})$ is an association scheme. We call this scheme as a *triangular* association schemes, denoted as $T(v)$.

(3) Triangular association schemes can be generalized as follows. Let X be a set of size of v and Ω be the collection of all d-subsets of X. Then, $|\Omega| = \binom{v}{d}$. Define $R_0,\ R_1,\ \ldots,\ R_d$ as follows:

$$\begin{aligned} R_0 &= \{(\alpha,\ \alpha) \mid \alpha \in \Omega\}, \\ R_1 &= \{(\alpha,\ \beta) \mid \alpha,\ \beta \in \Omega, \ \text{ and } |\alpha \cap \beta| = d-1\}, \\ &\ \ \vdots \\ R_d &= \{(\alpha,\ \beta) \mid \alpha,\ \beta \in \Omega, \ \text{ and } |\alpha \cap \beta| = 0\}, \end{aligned}$$

Then, one can show that $(\Omega,\ \{R_0,\ R_1,\ \ldots,\ R_d\})$ is an association scheme. We call this scheme a *Johnson* association scheme, denoted as $J(v,\ d)$.

(4) Let X be an alphabet of size of q. Denote $\Omega = X^v$, the set of all v-tuples with entries in X. Consider the Hamming distance $\text{dist}(\alpha,\ \beta)$ of any two vectors of X^v, and define $R_0,\ R_1,\ \ldots,\ R_v$ as follows:

$$\begin{aligned}
R_0 &= \{(\alpha,\ \alpha) \mid \alpha \in \Omega\},\\
R_1 &= \{(\alpha,\ \beta) \mid \alpha,\ \beta \in \Omega, \ \text{ and } \text{dist}(\alpha,\ \beta) = 0\},\\
&\vdots\\
R_v &= \{(\alpha,\ \beta) \mid \alpha,\ \beta \in \Omega, \ \text{ and } \text{dist}(\alpha,\ \beta) = v\},
\end{aligned}$$

Then, one can show that $(\Omega,\ \{R_0,\ R_1,\ \ldots,\ R_v\})$ is an association scheme. We call this scheme a *Hamming* association scheme, denoted as $H(q,\ v)$.

Association schemes are generalizations of strongly regular graphs. Let $(X, \{R_i\}_{0\leq i\leq d})$ be an association scheme with d classes and $|X| = v$. Define the neighborhood of the point α in the graph $\Gamma_i = (X, R_i)$ by $R_i(\alpha) = \{\beta \in X \mid (\alpha,\ \beta) \in R_i\}$, $0 \leq i \leq d$. By Definition 2.5.1, $|R_i(\alpha)|$ is exactly p^0_{ii}, which is independent with the choice of α, $1 \leq i \leq d$. We use n_i to denote p^0_{ii}. It follows that Γ_i are regular graphs of valency n_i, $0 \leq i \leq d$. Notice that $R_0,\ \ldots,\ R_d$ are partition of $X \times X$. By Definition 2.5.1, we also have $n_0 + n_1 + \cdots + n_d = v$ with $n_0 = 1$.

From the above arguments, we actually show $p^k_{ij} = |R_i(\alpha) \cap R_j(\beta)|$, if $(\alpha, \beta) \in R_k$. Intersection numbers play an fundamental role in the theory of association schemes. We contain some of their basic properties in the following propsition.

Proposition 2.5.2. ([15]) *Let $(X, \{R_i\}_{0\leq i\leq d})$ be a d-class association scheme. We have*

(1) $p^k_{0j} = \delta_{jk}$ and $p^k_{i0} = \delta_{ik}$.

(2) $p^0_{ij} = n_i\delta_{ij}$.

(3) $\sum_{i=0}^{d} p^k_{ij} = n_j$.

(4) $n_k p^k_{ij} = n_i p^i_{kj}$.

Proof: We prove the items from (1) to (4) as follows:

(1) For $(\alpha, \beta) \in R_k$, $0 \leq k \leq d$, we have $R_0(\alpha) = \{\alpha\}$ and $R_j(\beta) = \{\gamma \mid (\beta, \gamma) \in R_j\}$.

Thus, $p_{0j}^k = |R_0(\alpha) \cap R_j(\beta)| = |\{\alpha\} \cap \{\gamma \mid (\beta, \gamma) \in R_j\}|$. It follows that $p_{0j}^k = 1$ when $j = k$; and equals to 0, otherwise. The second identity follows by similar arguments.

(2) Notice that $R_0(\alpha),\ \ldots,\ R_d(\alpha)$ partition X. This implies that $p_{ij}^0 = |R_i(\alpha) \cap R_j(\alpha)| = n_i$ if $i = j$; equals to 0, otherwise. This concludes the identity of the second item.

(3) Since $R_0(\alpha),\ \ldots,\ R_d(\alpha)$ are partition of X, we have, for $(\alpha, \beta) \in R_k$,

$$\sum_{i=0}^{d} p_{ij}^k = \sum_{i=0}^{d} |R_i(\alpha) \cap R_j(\beta)| = |\left(\cup_{i=0}^{d} R_i(\alpha)\right) \cap R_j(\beta)| = |X \cap R_j(\beta)| = |R_j(\beta)| = n_j.$$

(4) Take an element α of X. Then, for any $(\alpha, \beta) \in R_k$, there are exactly p_{ij}^k elements γ of X such that $(\alpha, \gamma) \in R_i$ and $(\beta,\ \gamma) \in R_j$. Through this way, we can obtain $n_k p_{ij}^k$ triangles. On the other hand, for any $(\alpha, \gamma) \in R_i$, there are exactly p_{kj}^i elements β of X such that $(\alpha, \beta) \in R_k$ and $(\beta,\ \gamma) \in R_j$. Through this way, we can obtain $n_i p_{kj}^i$ triangles.

It is easy to see that any triangules obtained by the first way can also be obtained by the second way. Then, we have $n_k p_{ij}^k \leq n_i p_{kj}^i$. For the similar reason, we have $n_i p_{kj}^i \leq n_k p_{ij}^k$, which actually implies that $n_k p_{ij}^k = n_i p_{kj}^i$. □

Moreover, if all Γ_i are connected, $(X, \{R_i\}_{0 \leq i \leq d})$ is called *primitive*. Otherwise, it is called *imprimitive*. We define *adjacency matrices* A_i, $0 \leq i \leq d$, of an association scheme $(X, \{R_i\}_{0 \leq i \leq d})$ by the adjacency matrix of Γ_i. In terms of adjacency matrices, the axioms of Definition 2.5.1 can be written as

(1) $\sum_{i=0}^{d} A_i = J$, where J is the all-one matrix of size $v \times v$.

(2) $A_0 = I$.

(3) $A_i A_j = A_j A_i$.

(4) $A_i A_j = \sum_k p_{ij}^k A_k$, for all i, j and $k \in \{0,\ \ldots,\ d\}$.

Thus, the vector space $B = \langle A_0,\ A_1,\ \ldots,\ A_d \rangle$ forms an algebra, which is called the *Bose-Mesner algebra* of an association scheme $(X, \{R_i\}_{0 \leq i \leq d})$. Notice that $A_0,\ \ldots,\ A_d$ are pairwise commutative, thus, they can be diagonalized simultaneously. More precisely, the n-dimensional real linear space $\mathbb{R}^v$ can be decomposed as

$$\mathbb{R}^v = V_0 \oplus V_1 \oplus \cdots \oplus V_d,$$

where V_i is the common eigenspace of $A_0,\ \ldots,\ A_d$ for $0 \leq i \leq d$. Let $E_0 = \frac{1}{|X|}J,\ E_1,\ \ldots,\ E_d$ be the projections of $\mathbb{R}^v$ to $V_0,\ V_1,\ \ldots,\ V_d$, respectively. The matrices $E_0,\ E_1,\ \ldots,\ E_d$ form a basis of B. This can be seen from the facts $E_0,\ E_1,\ \ldots,\ E_d$ are linearly independent and the dimension of B is not larger than $d+1$.

The basis transition matrix from $\{A_0,\ A_1,\ \ldots,\ A_d\}$ to $\{E_0,\ E_1,\ \ldots,\ E_d\}$ is denoted by $P = (p_{ij})_{0 \leq i,j \leq d}$, and is usually called the *first eigenmatrix* (or *character table*) of the scheme. Explicitly, P is the $(d+1) \times (d+1)$ matrix with rows and columns indexed by $0,\ 1,\ \ldots,\ d$ such that

$$(A_0,\ A_1,\ \ldots,\ A_d) = (E_0,\ E_1,\ \ldots,\ E_d)P.$$

The basis transition matrix from $\{E_0,\ E_1,\ \ldots,\ E_d\}$ to $\{A_0,\ A_1,\ \ldots,\ A_d\}$ is denoted by $Q = (q_{ij})_{0 \leq i,j \leq d}$, and is usually called the *second eigenmatrix* of the scheme. Explicitly, Q is the $(d+1) \times (d+1)$ matrix with rows and columns indexed by $0,\ 1,\ \ldots,\ d$ such that

$$(A_0,\ A_1,\ \ldots,\ A_d)Q = (E_0,\ E_1,\ \ldots,\ E_d).$$

It is easy to see that $PQ = QP = vI$.

Let $m_i = \text{rank}(E_i) = \text{Tr}(E_i)$. The m_i's are called the *multiplicities* of the scheme. We call the scheme $(X, \{R_i\}_{0 \leq i \leq d})$ *pseudocyclic*, if there exists an integer t such that $m_i = t$ for $1 \leq i \leq d$. The following theorem gives combinatorial characterizations of pseudocyclic association schemes.

Theorem 2.5.3. *Let $(X, \{R_i\}_{0 \leq i \leq d})$ be an association scheme. Then the following are equivalent.*

(1) $(X, \{R_i\}_{0 \leq i \leq d})$ is pseudocyclic.

(2) For some constant n, we have $n_i = n$ and $\sum_{i=1}^{d} p_{ii}^{j} = n-1$, for $1 \leq i \leq d$.

(3) $(X, \mathcal{B})$ is a $2-(v, n, n-1)$ design, where $\mathcal{B} = \{R_i(x) \mid x \in X, 1 \leq i \leq d\}$.

The proof of this theorem can be found in [15, p. 48] or [31, p. 84]. Part (2) of the above theorem will be useful in Section 4.

A classical example of pseudocyclic association schemes is the cyclotomic association scheme over a finite field. Let $q = p^f$, where p is a prime and f a positive integer. Let γ be a fixed primitive element of $\mathbb{F}_q$ and $N|q-1$ with $N > 1$. Let $C_0 = \langle \gamma^N \rangle$, and $C_i = \gamma^i C_0$ for $1 \leq i \leq N-1$. Assume that $-1 \in C_0$. Define $R_0 = \{(x,x) \mid x \in \mathbb{F}_q\}$, and for $i \in \{1, 2, \dots, N\}$, define $R_i = \{(x,y) \mid x, y \in \mathbb{F}_q, x - y \in C_{i-1}\}$. Then $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$ is *the cyclotomic association scheme of class N over $\mathbb{F}_q$*. The first eigenmatrix P of the cyclotomic scheme of class N is the following $(N+1)$ by $(N+1)$ matrix (with the rows of P arranged in a certain way)

$$P = \begin{pmatrix} 1 & \frac{N-1}{q} & \frac{N-1}{q} & \frac{N-1}{q} & \cdots & \frac{N-1}{q} \\ 1 & \tau_{N-1} & \tau_0 & \tau_1 & \cdots & \tau_{N-2} \\ 1 & \tau_{N-2} & \tau_{N-1} & \tau_0 & \cdots & \tau_{N-3} \\ \vdots & & & & & \\ 1 & \tau_0 & \tau_1 & \tau_2 & \cdots & \tau_{N-1} \end{pmatrix} \tag{2.18}$$

where the τ_i's are the cyclotomic periods (or Gauss periods) of order N defined by

$$\tau_i = \sum_{x \in C_i} \psi(x).$$

In the above defintion, ψ is the canonical additive character of $\mathbb{F}_q$.

Let $(X, \{R_0, R_1, \dots, R_d\})$ a d-class association scheme. For a partition $\Lambda_0 := \{0\}, \Lambda_1, \dots, \Lambda_{d'}$ of $\{0, 1, \dots, d\}$, let $R_{\Lambda_i} = \cup_{k \in \Lambda_i} R_k$, for $0 \leq i \leq d'$. If $(X, \{R_{\Lambda_i}\}_{0 \leq i \leq d'})$ forms an association scheme, then we say that $(X, \{R_{\Lambda_i}\}_{0 \leq i \leq d'})$ is a *fusion scheme* of the original scheme. Given a partition $\{\Lambda_i\}_{0 \leq i \leq d'}$ of $\{0, 1, 2, \dots, d\}$ with $\Lambda_0 = \{0\}$, there is a simple criterion in terms of the first eigenmatrix P of $(X, \{R_i\}_{0 \leq i \leq d})$ for deciding whether $(X, \{R_{\Lambda_i}\}_{0 \leq i \leq d'})$ forms an association scheme or not. For readers who are interested in this topic, we refer them to the references [14] and [15].

We state this criterion below

Theorem 2.5.4. (The Bannai-Muzychuk Criterion, see [4]) *Let P be the first eigenmatrix of an association scheme $(X, \{R_i\}_{0 \leq i \leq d})$. Let $\Lambda_0 := \{0\}, \Lambda_1, \dots, \Lambda_{d'}$ be a partition of $\{0, 1, \dots, d\}$. Then $(X, \{R_{\Lambda_i}\}_{0 \leq i \leq d'})$ forms a fusion association scheme if and only* *if there exists a partition $\{\Delta_i\}_{0\leq i\leq d'}$ of $\{0,1,2,\ldots,d\}$ with $\Delta_0=\{0\}$ such that each (Δ_i,Λ_j)-block of P has a constant row sum. Moreover, the constant row sum of the (Δ_i,Λ_j)-block is the (i,j) entry of the first eigenmatrix of the fusion scheme.*

Given a d-class association scheme $(X,\{R_0,R_1,\ldots,R_d\})$, if $(X,\{R_{\Lambda_i}\}_{0\leq i\leq d'})$ forms a fusion association scheme, for every partition $\{\Lambda_i\}_{0\leq i\leq d'}$ of $\{0,1,2,\ldots,d\}$ with $\Lambda_0=\{0\}$, then we call the original scheme $(X,\{R_i\}_{0\leq i\leq d})$ *amorphic*. Amorphic association schemes have intrinsic links with srgs. An srg$(v,\ k,\ \lambda,\ \mu)$ is said to be of *Latin square type* (respectively, *negative Latin square type*), if $(v,\ k,\ \lambda,\ \mu)=(m^2,\ t(m-\epsilon),\ \epsilon m+t^2-3\epsilon t,\ t(t-\epsilon))$ for some integer m, t and $\epsilon=1$ (respectively, $\epsilon=-1$). The following theorem (see [20]) is useful for our second research project.

Theorem 2.5.5. *All graphs in an amorphic association scheme with at least three classes are strongly regular of Latin square type, or they are all of negative Latin square type.*

We shall use this theorem to show that the examples in Chapter 4 are not amorphic, which give counterexamples to A. V. Ivanov's conjecture.

We remark that the above theorem may not hold when the association scheme has only two classes. Let $(X,\{R_0,R_1,R_2\})$ be a 2-class association scheme, where (X,R_1) is an srg which is neither Latin square type nor negative Latin square type. This scheme is clearly amorphic, but it does not satisfy the conclusions of Theorem 2.5.5.

For more information on amorphic association schemes, we refer the reader to [20].

Chapter 3

THE CONSTRUCTIONS OF STRONGLY REGULAR GRAPHS USING GAUSS SUMS OF EVEN INDEX

In this chapter, we construct strongly regular Cayley graphs in the index 6 case. As the discussion of Section 2.4, the main obstacle in the construct is the evaluation of Gauss sums of higher index (greater or equal than 6). But, in Theorem 3.0.9, we develop an approach to bypass this obstacle. Based on this conclusion, we shall give sufficient and necessary conditions in Theorem 3.0.10 that determine candidate Cayley graphs to be strongly regular.

Let $\mathbb{F}_q$ be the finite field of order q and γ be a primitive element of $\mathbb{F}_q$. Let $N > 1$ be a proper positive divisor of $q-1$. Let C_0, $C_1 = \gamma C_0$, $\ldots$, $C_{N-1} = \gamma^{N-1} C_0$ be the cyclotomic classes of order N of $\mathbb{F}_q$, where $C_0 = \langle \gamma^N \rangle \leq \mathbb{F}_q^*$.

In this chapter, we assume that (i) $\gcd(p(p-1), N) = 1$, where $N | (q-1)$, and $q = p^f$, f is the order of p modulo N, (ii) $-1 \notin \langle p \rangle$, the cyclic subgroup of $(\mathbb{Z}/N\mathbb{Z})^*$ generated by p. These assumptions have the following consequences.

First, the index $[(\mathbb{Z}/N\mathbb{Z})^* : \langle p \rangle]$, denoted by w, must be even. This can be seen as follows. From $\gcd(p(p-1), N) = 1$, we see that N is odd. Thus $\phi(N)$ is even, where ϕ is the Euler totient function. If w is odd, then $f = \phi(N)/w$ is even. It follows that $p^{f/2} \equiv -1 \pmod{N}$, contradicting the assumption that $-1 \notin \langle p \rangle$.

Secondly, let χ be a multiplicative character of $\mathbb{F}_q$ of order N. We claim that $g(\chi) \in \mathbb{Z}[\xi_N]$. We prove this claim as follows. For any $b \in \mathbb{F}_p^*$, since $\gcd(N, p-1) = 1$, we have $\chi(b) = 1$. Hence by Part (2) of Lemma 2.3.4, $\sigma_{1,b}(g(\chi)) = \bar{\chi}(b) g(\chi) = g(\chi)$. It follows that $g(\chi) \in \mathbb{Z}[\xi_N]$. We can actually go a little further. Let K be the decomposition field of the prime p in $\mathbb{Q}(\xi_N)$. Then it is well known [34, p. 197] that

$\mathrm{Gal}(\mathbb{Q}(\xi_N)/K) = \langle \sigma_{p,1} \rangle$. By Part (3) of Lemma 2.3.4, we have $g(\chi) \in K$. In fact, we have $g(\chi) \in O_K$, the integer ring of K.

Gauss sums $g(\chi)$ with χ being a multiplicative character of order N of $\mathbb{F}_q$ (and $-1 \notin \langle p \rangle$) are called *Gauss sums of index w*.

For our first research project, we assume $N = p_1^m$, where p_1 is an odd prime, $m \geq 1$ is an integer, and $w|(p_1 - 1)$. In this case, $\mathrm{Gal}(\mathbb{Q}(\xi_N)/\mathbb{Q}) \cong (\mathbb{Z}/N\mathbb{Z})^*$ is cyclic, and K is the unique imaginary subfield of $\mathbb{Q}(\xi_N)$ with $[K : \mathbb{Q}] = w$. Since $w|(p_1 - 1)$, we see that K is in fact a subfield of $\mathbb{Q}(\xi_{p_1})$. Therefore if χ is a multiplicative character of $\mathbb{F}_q$ of order N, we in fact have $g(\chi) \in \mathbb{Z}[\xi_{p_1}]$.

Let g be a primitive root modulo p_1. Define $\widetilde{U_j} = g^j \langle p \rangle \subseteq (\mathbb{Z}/p_1\mathbb{Z})^*$, for all $0 \leq j \leq w - 1$. Then $(\mathbb{Z}/p_1\mathbb{Z})^* = \cup_{j=0}^{w-1} \widetilde{U_j}$. For $0 \leq j \leq w - 1$, we define η_j by

$$\eta_j = \sum_{a \in \tilde{U}_j} \xi_{p_1}^a, \tag{3.1}$$

where ξ_{p_1} is a complex primitive p_1-th root of unity. The following lemma is well known (see [51]).

Lemma 3.0.6. *With the above assumptions, $\{\eta_j \mid 0 \leq j \leq w - 1\}$ is an integral basis of K.*

Proof: Note that $[K : \mathbb{Q}] = w$. Then, by Proposition 1 in [51], we know that $\eta_0, \ldots, \eta_{w-1}$ form a integral basis of K. □

Let χ be a multiplicative character of $\mathbb{F}_q$ of order N. Let r be the largest nonnegative integer such that $p^r | g(\chi)$. That is, $p^{-r} g(\chi) \in O_K$, but $p^{-(r+1)} g(\chi) \notin O_K$. Note that if χ' is another multiplicative character of $\mathbb{F}_q$ of order N, then there exists a $d \in (\mathbb{Z}/N\mathbb{Z})^*$ such that $\chi' = \chi^d$; it follows that $g(\chi') = g(\chi^d) = \sigma_{d,1}(g(\chi))$. This shows that the integer r does not depend on the choice of the multiplicative character of order N. The explicit computation of r can be done by using Stickelberger's theorem on the prime ideal factorization of Gauss sums as the following lemma.

Lemma 3.0.7. *Let χ be a multiplicative character of $\mathbb{F}_q$ of order N. With the above assumptions and notation, we have*

$$r = \frac{f - \tilde{f}}{2} + b,$$

where $\tilde{f} = \frac{p_1-1}{w}$, $b = \min\{b_0, b_1, \ldots, b_{w-1}\}$ and $b_j = \frac{1}{p_1}\sum_{z\in([1,p_1-1]\cap\tilde{U}_j)} z$ for all $0 \le j \le w-1$, here $[1, p_1-1]$ denotes the set of integers x, $1 \le x \le p_1 - 1$.

We proceed with our proof as follows. Let $G = \mathrm{Gal}(K/\mathbb{Q})$. By Lemma 2.3.3, we have $G \cong (\mathbb{Z}/N\mathbb{Z})^*/\langle p\rangle$, and thence have $\mathrm{Gal}(K/\mathbb{Q})$ is cyclic. Let g be a generator of $(\mathbb{Z}/N\mathbb{Z})^*/\langle p\rangle$ and set $U_i = g^i\langle p\rangle$, $0 \le i \le w-1$. Then, $\cup_{i=0}^{w-1} U_i = (\mathbb{Z}/N\mathbb{Z})^*$. The above congruence can be written as

$$G \cong \{U_i \mid 0 \le i \le w-1\}.$$

Set $\sigma = \sigma_g$ to be the generator of G. Let P be a prime ideal of O_K containing p. We have $P = O_K \cap P'$ for some P' of $\mathbb{Z}[\xi_N]$ containin p. By Stickelberger's theorem, we have

$$g(\chi)O_K = P^{\sum_{i=0}^{w-1} a_i\sigma^i}, \tag{3.2}$$

where

$$a_i = \frac{1}{N}\sum_{z\in[1,N-1]\cap U_i} z, \quad \text{for } 0 \le i \le w-1.$$

We remark that a_i, $0 \le i \le w-1$, are integers. Notice that $\sigma_{-1} = \sigma^{w/2}$. Therefore, we have

$$\overline{g(\chi)}O_K = \sigma^{w/2}(g(\chi)O_K) = P^{\sum_{i=0}^{w-1} a_i\sigma^{i+w/2} \pmod{w}} = P^{\sum_{i=-w/2}^{w/2-1} a_i\sigma^{i+w/2}}. \tag{3.3}$$

Moreover, since K is the decomposition field of p in $\mathbb{Q}[\xi_N]$, we have

$$pO_K = P^{\sum_{i=0}^{w-1}\sigma^i}.$$

Thus, by (3.2) and (3.3), we have

$$a_i + a_{i+w/2} = f = \frac{\phi(N)}{w}, \quad \text{for } 0 \le i \le w/2.$$

Notice that $[(\mathbb{Z}/p_1\mathbb{Z})^* : \langle p\rangle] = [(\mathbb{Z}/N\mathbb{Z})^* : \langle p\rangle] = w$. Thus, we say $(\mathbb{Z}/p_1\mathbb{Z})^*/\langle p\rangle$ is still generated by g. We shall finish our proof after proving the following lemma:

Lemma 3.0.8. *Under the above notations, we have*

$$a_i = \frac{f-\tilde{f}}{2} + b_i, \quad \textit{for } 0 \le i \le w-1.$$

Proof: Each z in $(\mathbb{Z}/N\mathbb{Z})^*$ can be expressed uniquely as $z = p_1 y + x$, where $0 \le y \le p_1^{m-1} - 1$ and $0 \le x \le p_1 - 1$. Hence, we have

$$\begin{aligned}
a_i &= \frac{1}{N} \sum_{z \in [1,N-1] \cap U_i} z \\
&= \frac{1}{N} \sum_{x \in [1,p_1-1] \cap \tilde{U_i}} \sum_{y=0}^{p_1^{m-1}-1} (p_1 y + x) \\
&= \frac{p_1}{N} \left(\sum_{x \in [1,p_1-1] \cap \tilde{U_i}} \sum_{y=0}^{p_1^{m-1}-1} y \right) + \frac{1}{N} \left(\sum_{x \in [1,p_1-1] \cap \tilde{U_i}} \sum_{y=0}^{p_1^{m-1}-1} x \right) \\
&= \frac{\phi(p_1)}{w} \frac{p_1^{m-1} - 1}{2} + b_i = \frac{f-\tilde{f}}{2} + b_i.
\end{aligned}$$

Now, we return to the proof of Lemma 3.0.7. Based on above arguments and Lemma 3.0.8, we have

$$g(\chi) O_K = p^{\frac{f-\tilde{f}}{2}} P^{\sum_{i=0}^{w-1} b_i, \sigma^i}$$

and

$$\overline{g(\chi)} O_K = p^{\frac{f-\tilde{f}}{2}} P^{\sum_{i=-w/2}^{w/2-1} b_i \sigma^{i+w/2}}.$$

Moreover, $b_i + b_{i+w/2} = \tilde{f}$, $0 \le i \le w-1$. By Lemma 2.3.4, without loss of generality, we assume b_0 is the smallest nonnegative integer of $\{b_0, \ \dots, \ b_{w-1}\}$. It immediately follows that $\frac{f-\tilde{f}}{2} + b_0$ is the maximal power of p in $g(\chi)$. □

The proof of Lemma 3.0.7 is a generalization of the proof in [24]. (See [24], pp. 1430). We should remark that Lemma 3.0.7 is still valid when N is any odd number.

Now, we are ready to prove our first theorem. Define

$$D := \bigcup_{i=0}^{p_1^{m-1}-1} C_i. \tag{3.4}$$

Then, the number of eigenvalues of the Cayley graphs whose connection sets are defined by (3.4) has the following property.

Theorem 3.0.9. *The Cayley graph Cay($\mathbb{F}_q$, D) is an undirected regular graph of valency $|D|$. It has at most $w+1$ distinct restricted eigenvalues.*

The proof is parallel to that of Theorem 3.1 in [28]. Since we will use some parts of the proof later on, we will give the complete proof here.

Proof: Since $N = p_1^m$ is odd, we have $2N|(q-1)$ or q is even; consequently $-C_0 = C_0$. Hence $-D = D$. It follows that Cay($\mathbb{F}_q$, D) is undirected. As $0 \notin D$, we see that Cay($\mathbb{F}_q$, D) has no loops. From definition, we deduce that Cay($\mathbb{F}_q$, D) is a regular graph of valency $|D|$.

The restricted eigenvalues of Cay($\mathbb{F}_q$, D), as explained in [14, p. 136], are given by

$$\psi(\gamma^a D) = \sum_{x \in D} \psi(\gamma^a x),$$

where $0 \le a \le N-1$. By (3.4) and Lemma 2.2.10, we have

$$\begin{aligned}\psi(\gamma^a D) &= \sum_{i=0}^{p_1^{m-1}-1} \psi(\gamma^a C_i) = \sum_{i=0}^{p_1^{m-1}-1} \tau_{i+a} \\ &= \frac{1}{N} \sum_{\chi \in C_0^{\perp}} g(\overline{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}). \end{aligned} \tag{3.5}$$

If $\chi \in C_0^{\perp}$ and $\chi = \chi_0$ (the trivial character), then $g(\overline{\chi}) = -1$ and $\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}) = p_1^{m-1}$. If $\chi \in C_0^{\perp}$ and $\mathrm{ord}(\chi) \neq 1$, then $\mathrm{ord}(\chi) = p_1^{\ell}$, $1 \le \ell \le m$ since $\mathrm{ord}(\chi)||C_0^{\perp}|$. For those characters χ with $1 \neq \mathrm{ord}(\chi) < p_1^m$, we have

$$\sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i}) = \chi(\gamma^a) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma)^i = \chi(\gamma^a) \frac{\chi(\gamma)^{p_1^{m-1}} - 1}{\chi(\gamma) - 1} = 0.$$

Thus, in (3.5), the terms corresponding to characters of order p_1^{ℓ}, $1 \le \ell \le m-1$, vanish. Hence (3.5) can be simplified to

$$\psi(\gamma^a D) = \frac{1}{N}[-p_1^{m-1} + \sum_{\chi \in C_0^{\perp}, \mathrm{ord}(\chi) = p_1^m} g(\overline{\chi}) \sum_{i=0}^{p_1^{m-1}-1} \chi(\gamma^{a+i})]. \tag{3.6}$$

Define a multiplicative character θ of $\mathbb{F}_q$ by setting $\theta(\gamma) = \xi_N$. Then $\langle\theta\rangle = C_0^\perp$ since $C_0^\perp$ is the unique subgroup of $\widehat{\mathbb{F}_q^*}$ of order N. Thus any multiplicative character χ of order p_1^m can be expressed as θ^d for some d in $(\mathbb{Z}/N\mathbb{Z})^*$. We have

$$\psi(\gamma^a D) = \frac{1}{N}[-p_1^{m-1} + \sum_{d\in(\mathbb{Z}/N\mathbb{Z})^*} g(\overline{\theta}^d) \sum_{i=0}^{p_1^{m-1}-1} \theta^d(\gamma^{a+i})] \tag{3.7}$$

For convenience, we set

$$S_a := \sum_{d\in(\mathbb{Z}/N\mathbb{Z})^*} g(\overline{\theta}^d) \sum_{i=0}^{p_1^{m-1}-1} \theta^d(\gamma^{a+i}). \tag{3.8}$$

Let r be the positive integer given in Lemma 3.0.7 such that $p^{-r}g(\overline{\theta}) \in O_K$. By Lemma 3.0.6, we have

$$g(\overline{\theta}) = p^r(N_0\eta_0 + \cdots + N_{w-1}\eta_{w-1}), \tag{3.9}$$

where $N_0, \ldots, N_{w-1}$ are integers and $\eta_0, \ldots, \eta_{w-1}$ are defined in (3.1). From Lemma 2.3.4, we have $g(\overline{\theta}^d) = \sigma_{d,\,1}(g(\overline{\theta}))$. To simplify notation, we simply write σ_d for $\sigma_{d,1}$. It follows that

$$\begin{aligned} g(\overline{\theta}^d) &= \sigma_d(g(\overline{\theta})) = \sigma_d(p^r(N_0\eta_0 + \cdots + N_{w-1}\eta_{w-1})) \\ &= p^r(N_0\eta_0^{\sigma_d} + \cdots + N_{w-1}\eta_{w-1}^{\sigma_d}). \end{aligned}$$

Now writing $d \in (\mathbb{Z}/N\mathbb{Z})^*$ as $d = d_1 + p_1 d_2$, where $d_1 \in (\mathbb{Z}/p_1\mathbb{Z})^*$ and $d_2 \in \mathbb{Z}/p_1^{m-1}\mathbb{Z}$, we have $\eta_j^{\sigma_d} = \sigma_d(\sum_{c\in\tilde{C}_j} \xi_{p_1}^c) = \sum_{c\in\tilde{C}_j} \sigma_{d_1+p_1^{m-1}d_2}(\xi_{p_1}^c) = \eta_j^{\sigma_{d_1}}$. We have

$$\begin{aligned} g(\overline{\theta}^d) &= p^r(N_0\eta_0^{\sigma_d} + \cdots + N_w\eta_w^{\sigma_d}) \\ &= p^r(N_0\eta_0^{\sigma_{d_1}} + \cdots + N_w\eta_w^{\sigma_{d_1}}) \\ &= \sigma_{d_1}(p^r(N_0\eta_0 + \cdots + N_w\eta_w)) \\ &= \sigma_{d_1}(g(\overline{\theta})) = g(\overline{\theta}^{d_1}). \end{aligned} \tag{3.10}$$

Hence (3.8) can be written as

$$\begin{aligned}
S_a &= \sum_{d\in(\mathbb{Z}/N\mathbb{Z})^*} g(\overline{\theta}^d)\sum_{i=0}^{p_1^{m-1}-1}\theta^d(\gamma^{a+i})\\
&= \sum_{d_1\in(\mathbb{Z}/p_1\mathbb{Z})^*}\ \sum_{d_1\in\mathbb{Z}/p_1^{m-1}\mathbb{Z}} g(\overline{\theta}^{d_1+p_1d_2})\sum_{i=0}^{p_1^{m-1}-1}\theta^{d_1+p_1d_2}(\gamma^{a+i})\\
&= \sum_{d_1\in(\mathbb{Z}/p_1\mathbb{Z})^*}\ \sum_{i=0}^{p_1^{m-1}-1} g(\overline{\theta}^{d_1})\theta^{d_1}(\gamma^{a+i})\sum_{d_2\in\mathbb{Z}/p_1^{m-1}\mathbb{Z}}\theta^{p_1d_2}(\gamma^{a+i}).
\end{aligned}$$

Note that $\sum_{d_2\in\mathbb{Z}/p_1^{m-1}\mathbb{Z}}\theta^{d_2p_1(a+i)}(\gamma)=0$ if and only if $p_1^{m-1}\nmid(a+i)$. We only need to consider the terms for which $p_1^{m-1}\mid(a+i)$. For each $0\le a\le N-1$, there exists a unique $i_a\in\{0,1,\ldots,p_1^{m-1}-1\}$ such that $p_1^{m-1}\mid(a+i_a)$; writing $a+i_a=p_1^{m-1}j_a$, $j_a\in\mathbb{Z}/p_1\mathbb{Z}$, we have

$$S_a=p_1^{m-1}\sum_{d_1\in(\mathbb{Z}/p_1\mathbb{Z})^*}g(\overline{\theta}^{d_1})\theta^{d_1}(\gamma^{p_1^{m-1}j_a})=p_1^{m-1}\sum_{d_1\in(\mathbb{Z}/p_1\mathbb{Z})^*}g(\overline{\theta}^{d_1})\xi_{p_1}^{j_ad_1}. \tag{3.11}$$

For each $j\in\mathbb{Z}/p_1\mathbb{Z}$, define an additive character ψ_j on $\mathbb{Z}/p_1\mathbb{Z}$ such that $\psi_j(d_1)=\xi_{p_1}^{jd_1}$. We have

$$\begin{aligned}
S_a &= p_1^{m-1}\sum_{d_1\in(\mathbb{Z}/p_1\mathbb{Z})^*}g(\overline{\theta}^{d_1})\psi_{j_a}(d_1)\\
&= p_1^{m-1}p^r\sum_{i=0}^{w-1}\sum_{d_1\in\widetilde{C_i}}(N_0\eta_0^{\sigma_{d_1}}+\cdots+N_{w-1}\eta_{w-1}^{\sigma_{d_1}})\psi_{j_a}(d_1)\\
&= p_1^{m-1}p^r[(N_0\eta_0+N_1\eta_1+\cdots+N_{w-1}\eta_{w-1})\sum_{d_1\in\widetilde{C_0}}\psi_{j_a}(d_1)\\
&\quad+(N_0\eta_1+N_1\eta_2+\cdots+N_w\eta_0)\sum_{d_1\in\widetilde{C_1}}\psi_{j_a}(d_1)\\
&\quad\cdots\\
&\quad+(N_0\eta_{w-1}+N_1\eta_0+\cdots+N_{w-1}\eta_{w-2})\sum_{d_1\in\widetilde{C_{w-1}}}\psi_{j_a}(d_1)].
\end{aligned}\tag{3.12}$$

Let $M_0=N_0+N_1+\cdots+N_{w-1}$. Note that $\sum_{i=0}^{w-1}\eta_i=-1$. We continue the computations of S_a by considering two cases.

Case 1. $j_a = 0$. In this case, $\psi_{j_a}(d_1) = 1$ for all $d_1 \in \mathbb{Z}/p_1\mathbb{Z}$. It follows that $\sum_{d_1 \in \widetilde{C_z}} \psi_{j_a}(d_1) = (p_1 - 1)/w$, $0 \leq z \leq w-1$. Thus we have

$$S_a = \frac{p_1 - 1}{w} p_1^{m-1} p^r (N_0 \sum_{i=0}^{w-1} \eta_i + N_1 \sum_{i=0}^{w-1} \eta_i + \cdots + N_{w-1} \sum_{i=0}^{w-1} \eta_i) = \frac{1-p_1}{w} p_1^{m-1} p^r M_0$$

Case 2. $j_a \neq 0$. In this case, j_a must belong to a unique coset of $\langle p \rangle$ in $(\mathbb{Z}/p_1\mathbb{Z})^*$, say $j_a \in g^t \langle p \rangle$, where $0 \leq t \leq w-1$. In this case, for any $0 \leq z \leq w-1$, we have

$$\sum_{d_1 \in \widetilde{C_z}} \psi_{j_a}(d_1) = \eta_{z+t},$$

where the subscript $z+t$ of η_{z+t} is read modulo w. In the following, the subscripts of η_i and K_j should also be read modulo w.

Define

$$\begin{aligned} &K_0 = \eta_0^2 + \cdots + \eta_{w-1}^2, \\ &K_1 = \eta_0\eta_1 + \cdots + \eta_{w-1}\eta_0, \\ &\cdots \\ &K_{w-1} = \eta_0\eta_{w-1} + \cdots + \eta_{w-1}\eta_{w-2}. \end{aligned}$$

Then

$$\begin{aligned} S_a &= p_1^{m-1}p^r[(N_0\eta_0 + N_1\eta_1 + \cdots + N_{w-1}\eta_{w-1})\eta_t \\ &\quad +(N_0\eta_1 + N_1\eta_2 + \cdots + N_{w-1}\eta_0)\eta_{1+t} \\ &\quad \cdots \\ &\quad +(N_0\eta_{w-1} + N_1\eta_0 + \cdots + N_{w-1}\eta_{w-2})\eta_{w-1+t}] \\ &= p_1^{m-1}p^r[N_0(\eta_0\eta_t + \eta_1\eta_{1+t} + \cdots + \eta_{w-1}\eta_{w-1+t}) \\ &\quad +N_1(\eta_0\eta_{w-1+t} + \eta_1\eta_t + \cdots + \eta_{w-1}\eta_{w-2+t}) \\ &\quad \cdots \\ &\quad +N_{w-1}(\eta_0\eta_{1+t} + \eta_1\eta_{2+t} + \cdots + \eta_{w-1}\eta_t)] \\ &= p_1^{m-1}p^r(N_0K_t + N_1K_{t+1} + \cdots + N_{w-1}K_{t+w-1}) \qquad (3.13) \end{aligned}$$

As above , we have shown that w is even and f is odd. The Gauss periods η_j satisfy the following relations (see [51]):

$$K_{w/2} = (1 + (w-1)p_1)/w, \ K_j = (1-p_1)/w, \text{ if } j \neq w/2.$$

Clearly, there exists a unique element in the set $\{t+i \mid 0 \le i \le w-1\}$ that is congruent to $w/2$ modulo w, say $t + h(a) \equiv w/2 \pmod{w}$. We have

$$\begin{aligned} S_a &= p_1^{m-1}p^r[\frac{1-p_1}{w}(M_0 - N_{h(a)}) + \frac{1+(w-1)p_1}{w}N_{h(a)}] \\ &= p_1^{m-1}p^r(\frac{1-p_1}{w}M_0 + p_1 N_{h(a)}). \end{aligned} \tag{3.14}$$

Therefore in this case, we have

$$S_a \in \{p_1^{m-1}p^r(\frac{1-p_1}{w}M_0 + p_1N_i) \mid 0 \le i \le w-1\}.$$

Summing up, let

$$\begin{aligned} E &= \left\{\frac{1}{p_1}(-1 + \frac{1-p_1}{w}p^rM_0)\right\} \\ &\quad \cup \left\{\frac{1}{p_1}(-1 + \frac{1-p_1}{w}p^rM_0) + p^rN_i \mid 0 \le i \le w-1\right\}. \end{aligned} \tag{3.15}$$

We have shown that the restricted eigenvalues of Cay$(\mathbb{F}_q, D)$ belong to E. Since $|E| \le w+1$, we see that Cay$(\mathbb{F}_q, D)$ has at most $w+1$ distinct restricted eignevalues. The proof of the theorem is now complete. □

Next we give necessary and sufficient conditions for Cay$(\mathbb{F}_q, D)$ to be an srg. The proof uses discrete Fourier transforms, which were first employed in the proof of Theorem 3.1 in [50].

Theorem 3.0.10. *Let p_1 be a prime, $m \ge 1$, $N = p_1^m$. Let $p \neq p_1$ be a prime, $f =$ ord$_N(p)$, $w = \phi(N)/f$, and $q = p^f$. Assume that $-1 \notin \langle p \rangle$, $\gcd(p(p-1), N) = 1$ and $w|(p_1 - 1)$. Let r be given in Lemma 3.0.7 and D be defined as in (3.4). Then Cay($\mathbb{F}_q$, D) is a strongly regular graph if and only if there exists an integer ℓ, $1 \le \ell \le w-1$, such that*

$$\frac{p^r(1-p_1)\ell}{w} \equiv \epsilon \pmod{p_1} \tag{3.16}$$

and

$$p^s = \frac{\ell}{w}\left(p_1 - \frac{(p_1-1)\ell}{w}\right), \tag{3.17}$$

where $s = f - 2r$ and $\epsilon = \pm 1$.

Proof: Suppose that $\mathrm{Cay}(\mathbb{F}_q,\, D)$ is a strongly regular graph. Then by Theorem 2.2.7, $\mathrm{Cay}(\mathbb{F}_q,\, D)$ has exactly two distinct restricted eigenvalues. By our computations of the restricted eigenvalues of $\mathrm{Cay}(\mathbb{F}_q,\, D)$ in the proof of Theorem 3.0.9, we must have $N_i \in \{0, \epsilon\}$ for all $0 \le i \le w-1$, where $\epsilon \neq 0$ is an integer. Thus (3.9) becomes

$$g(\overline{\theta}) = \epsilon p^r \sum_{i\in I} \eta_i,$$

where $I = \{i \mid N_i = \epsilon, 0 \le i \le w-1\}$. From $|g(\overline{\theta})|^2 = p^f$, we obtain that

$$|\sum_{i\in I} \eta_i|^2 = p^{f-2r}/\epsilon^2. \tag{3.18}$$

It follows that ϵ must be a power of p. Since r is the largest power of p dividing the Gauss sum $g(\overline{\theta})$ (see Lemma 3.0.7), we have $\epsilon = \pm 1$.

Let $s = f - 2r$ and $D' = \cup_{i\in I}\widetilde{C_i} \subset (\mathbb{Z}/p_1\mathbb{Z})^*$. From (3.18), we see that D' is a difference set in $(\mathbb{Z}/p_1\mathbb{Z}, +)$ with parameters $(p_1, \frac{p_1-1}{w}\ell, \frac{p_1-1}{w}\ell - p^s)$, where $\ell = |I|$. From the basic parameter relation for difference sets, we obtain that

$$p^s = (\ell/w)(p_1 - (p_1-1)\ell/w).$$

Next we claim that $\frac{p^r(1-p_1)\ell}{w} \equiv \epsilon \pmod{p_1}$. This can be seen as follows.

$$\begin{aligned} \psi(\gamma^a D) &= \frac{1}{p_1^m}(-p_1^{m-1} + S_a) \\ &= \frac{1}{p_1}(-1 + \epsilon p^r(1-p_1)\ell/w) + p^r N_{h(a)}. \end{aligned}$$

Since $\psi(\gamma^a D)$ are integers for all $0 \le a \le N-1$, we see that $(1-p_1)\ell p^r/w \equiv \epsilon \pmod{p_1}$.

Conversely, let

$$x = \frac{1}{p_1}\left(-1 + \frac{1-p_1}{w}p^r\ell\epsilon\right),$$

with $\epsilon = \pm 1$. By (3.16), we have $x \in \mathbb{Z}$. Define a function φ on $(\mathbb{Z}/N\mathbb{Z}, +)$ by

$$\varphi(a) := \frac{\psi(\gamma^a D) - x}{p^r}, \ \forall a \in \mathbb{Z}/N\mathbb{Z}. \tag{3.19}$$

We claim that the range of φ is a subset of $\mathbb{Z}$. First we note that $\psi(\gamma^a D)$ are algebraic integers. Secondly by the computations in the proof of Theorem 3.0.9, we have $\psi(\gamma^a D) = \frac{1}{p_1}(-1 + \frac{1-p_1}{w} p^r M_0)$ or $\frac{1}{p_1}(-1 + \frac{1-p_1}{w} p^r M_0) + p^r N_{h(a)}$, which are rationals. Thus we must have $\psi(\gamma^a D) \in \mathbb{Z}$. It follows that $\frac{1-p_1}{w} p^r M_0 \equiv 1 \pmod{p_1}$. On the other hand, by assumption, we have $\frac{(1-p_1)p^r \ell}{w} \equiv \epsilon \pmod{p_1}$. Combining these two congruences, we obtain

$$M_0 \equiv \epsilon \ell \pmod{p_1},$$

from which we see that $\varphi(a) \in \mathbb{Z}$ indeed.

To simplify notation, we use G to denote the cyclic group $(\mathbb{Z}/N\mathbb{Z}, +)$. Then $\widehat{G} = \{\nu^j \mid 0 \leq j \leq N-1\}$, where ν is the character of G sending 1 to ξ_N. The Fourier transform $\hat{\varphi}$ of φ is given by

$$\hat{\varphi}(\nu^j) = \frac{\sum_{a\in G} \varphi(a)\nu^j(a)}{\sqrt{N}},$$

for $0 \leq j \leq N-1$.

When $j = 0$, we have

$$\hat{\varphi}(\nu^0) = \frac{\sum_{a\in G}(\psi(\gamma^a D) - x)}{\sqrt{N}p^r} = \frac{\sqrt{N}(-1 - p_1 x)}{p_1 p^r} = \sqrt{N}\frac{\epsilon(p_1 - 1)\ell}{w p_1}. \tag{3.20}$$

For $1 \leq j \leq N-1$, we have

$$\begin{aligned} \hat{\varphi}(\nu^j) &= \frac{\sum_{a\in G}(\psi(\gamma^a D) - x)\nu^j(a)}{\sqrt{N}p^r} \\ &= \frac{\sum_{a\in G}\psi(\gamma^a D)\nu^j(a)}{\sqrt{N}p^r}. \end{aligned} \tag{3.21}$$

By (3.7), we have

$$\begin{aligned} \hat{\varphi}(\nu^j) &= \frac{1}{p^r\sqrt{N}} \sum_{a\in G} \frac{1}{N}\left(-p_1^{m-1} + S_a\right)\nu^j(a) \\ &= \frac{1}{p^r N\sqrt{N}} \sum_{a\in G} S_a \nu^j(a) \\ &= \frac{1}{p^r N\sqrt{N}} \sum_{d\in(\mathbb{Z}/N\mathbb{Z})^*} g(\overline{\theta}^d) \sum_{i=0}^{p_1^{m-1}-1} \theta(\gamma)^{di} \sum_{a\in G} \xi_N^{a(d+j)}. \end{aligned} \tag{3.22}$$

If $p_1|j$, then the (inner) sum $\sum_{a\in G}\xi_N^{a(d+j)} = 0$ since $d \in (\mathbb{Z}/N\mathbb{Z})^*$ (i.e., d is relatively prime to N); we thus have $\hat{\varphi}(\nu^j) = 0$.

If $\gcd(p_1, j) = 1$, then the (inner) sum $\sum_{a\in G}\xi_N^{a(d+j)}$ is nonzero (and equals N) if and only if $j \equiv -d \pmod{N}$; in this case, we have

$$\hat{\varphi}(\nu^j) = \frac{1}{p^r\sqrt{N}} g(\theta^j)(\sum_{i=0}^{p_1^{m-1}-1} \xi_N^{-ji}).$$

Note that the above formula also holds true for those j such that $1 \le j \le N-1$ and $p_1|j$ since $\sum_{i=0}^{p_1^{m-1}-1}\xi_N^{-ji} = 0$ if $p_1|j$. Therefore for all $1 \le j \le N-1$, we have

$$\hat{\varphi}(\nu^j) = \frac{1}{p^r\sqrt{N}} g(\theta^j)(\sum_{i=0}^{p_1^{m-1}-1} \xi_N^{-ji}). \tag{3.23}$$

Using the definition of φ, we have

$$\sum_{a\in G}\varphi(a) = \sum_{a\in G}\frac{\psi(\gamma^a D) - x}{p^r} = N\frac{-1 - xp_1}{p^r p_1} = \frac{N}{p_1}\cdot\frac{\epsilon(p_1-1)\ell}{w}. \tag{3.24}$$

From (3.20), (3.23) and Parseval's identity, we have

$$\begin{aligned}
\sum_{a\in G}\varphi(a)^2 &= \sum_{j=0}^{N-1}|\hat{\varphi}(\nu^j)|^2 = |\hat{\varphi}(\nu^0)|^2 + \sum_{j=1}^{N-1}|\hat{\varphi}(\nu^j)|^2 \\
&= \frac{N(p_1-1)^2\ell^2}{w^2p_1^2} + \frac{p^s}{N}\sum_{j=1}^{N-1}|\sum_{i=0}^{p_1^{m-1}-1}\xi_N^{-ji}|^2 \\
&= \frac{N(p_1-1)^2\ell^2}{w^2p_1^2} + \frac{p^s}{N}\sum_{i,k=0}^{p_1^{m-1}-1}\left(\sum_{j=0}^{N-1}\xi_N^{j(k-i)} - 1\right) \\
&= \frac{N}{p_1^2}\left(\frac{(p_1-1)^2\ell^2}{w^2} + p^s(p_1-1)\right) \\
&= \frac{N}{p_1}\cdot\frac{(p_1-1)\ell}{w},
\end{aligned} \tag{3.25}$$

where in the last step of the above computations we used the condition (3.17). Let $\kappa = \frac{N}{p_1}\cdot\frac{\ell(p_1-1)}{w}$ and $S = \{a \in \mathbb{Z}/N\mathbb{Z} \mid \varphi(a) \neq 0\}$ (that is, S is the support of φ). We have

$$0 \le \sum_{a\in S}(\varphi(a) - \epsilon)^2 = |S| - \kappa.$$

On the other hand, from $\sum_{a\in G}\varphi(a)^2=\kappa$ and $\varphi(a)\in\mathbb{Z}$, we have $\kappa\geq|S|$. Therefore we must have $|S|=\kappa$ and $\sum_{a\in S}(\varphi(a)-\epsilon)^2=0$. Hence $\varphi(a)\in\{0,\epsilon\}$ for all $a\in G$. It follows that the $\psi(\gamma^a D)$, $0\leq a\leq N-1$, take only two values. By Theorem 2.2.7, $\mathrm{Cay}(\mathbb{F}_q, D)$ is an srg. The proof is now complete. □

Remark 3.0.11. *Condition (3.16) is equivalent to*

$$\frac{p^b(1-p_1)\ell}{w}\equiv\pm1 \pmod{p_1} \tag{3.26}$$

This can be seen as follows. If we square both sides of (3.16), we obtain $\frac{p^{2b+f-\tilde{f}}(1-p_1)^2\ell^2}{w^2}\equiv 1 \pmod{p_1}$. *Noting that* $p^f\equiv1 \pmod{p_1}$ *and* $p^{\tilde{f}}\equiv 1 \pmod{p_1}$, *we have* $\frac{p^{2b}(1-p_1)^2\ell^2}{w^2}\equiv 1 \pmod{p_1}$. *Since* p_1 *is prime, we must have* $\frac{p^b(1-p_1)\ell}{w}\equiv\pm1 \pmod{p_1}$. *The converse can be proved similarly. We comment that (3.26) is much easier to use since it does not involve* m *any more.*

Corollary 3.0.12. *Let* p_1 *be a prime,* $m\geq 1$, $N=p_1^m$. *Let* $p\neq p_1$ *be a prime,* $f=\mathrm{ord}_N(p)$, $w=\phi(N)/f$, *and* $q=p^f$. *Assume that* $-1\not\in\langle p\rangle$, $\gcd(p(p-1),N)=1$ *and* $w|(p_1-1)$. *Let* $\tilde{f}=\mathrm{ord}_{p_1}(p)$, D *be defined as in (3.4), and* $\tilde{D}$ *the subgroup of* $\mathbb{F}_{p^{\tilde{f}}}^*$ *of index* p_1. *Then Cay(*$\mathbb{F}_q$, D*) is an srg if and only if Cay(*$\mathbb{F}_{p^{\tilde{f}}}$, $\tilde{D}$*) is an srg.*

The proof is clear by Theorem 3.0.10 and the above remark. We omit the details.

After finishing this project, we became aware of the very interesting paper [44] by Momihara. In [44], the author gave a recursive construction of strongly regular Cayley graphs, generalizing all but the first example in the statement of the Schmidt-White conjecture into infinite families. In particular, the two index 6 examples are generalized into infinite families while we could only generalize one of the index 6 examples in this dissertation. However, the approach taken here is different from that of [44] since ours is a direct construction. Also we obtained two conditions (3.16) and (3.17) which are necessary and sufficient for our construction to give rise to an srg. These conditions reveal an interesting connection between strongly regular Cayley graphs and cyclic difference sets in $(\mathbb{Z}/p_1\mathbb{Z}, +)$, which will be useful in future investigation of strongly regular Cayley graphs and cyclic difference sets.

With the definition of D in (3.4) and Theorem 3.0.10, we have the following three infinite families of srgs. Our first example is nothing but a generalization of an example in Table I.

Example 3.0.13. Let $p = 11$, $p_1 = 43$ and $N = p_1^m$ for $m \geq 1$. It is easy to use induction to prove that $\mathrm{ord}_{43^m}(11) = \phi(43^m)/6$ for all $m \geq 1$. Let $\mathbb{F}_q$ be the finite field of order $q = 11^f$, where $f = \phi(43^m)/w$, $w = 6$. We claim that $\mathrm{Cay}(\mathbb{F}_q, D)$, with $D = \cup_{i=0}^{p_1^{m-1}-1} C_i$, is an srg. We could use Corollary 3.0.12 together with the result in Table I to prove this claim. But we prefer to do it without relying on the result in Table I.

In this example, we have $\tilde{f} = 7$ and $b = 3$ (here b is obtained by computing $\min\{b_0, b_1, \ldots, b_5\}$ and $b_j = \frac{1}{p_1}\sum_{z \in ([1,p_1-1] \cap \tilde{C}_j)} z$, $0 \leq j \leq 5$). It follows that $s = 1$. Since $\frac{3}{6}(43 - (43-1) \times \frac{3}{6}) = 11$, (3.17) is satisfied with $\ell = 3$. Next $\frac{3 \times (1-43) \times 11^3}{6} \equiv -1 \pmod{43}$, we see that (3.26) is satisfied. It follows by Theorem 3.0.10 and Remark 3.0.11 that $\mathrm{Cay}(\mathbb{F}_q, D)$ is a strongly regular graph. This family of srg generalizes Example 5 in Table I.

Example 3.0.14. Let $p = 5$, $p_1 = 31$ and $N = p_1^m$ for $m \geq 1$. It is easy to use induction to prove that $\mathrm{ord}_{31^m}(5) = \phi(31^m)/10$. Let $\mathbb{F}_q$ be the finite field of order $q = 5^f$, where $f = \phi(31^m)/w$ with $w = 10$. Now $\tilde{f} = 3$. Let $\tilde{D}$ be the subgroup of $\mathbb{F}_{5^3}^*$ of index $p_1 = 31$. Then $\tilde{D}$ is nothing but $\mathbb{F}_5^*$, i.e. the multiplicative group of the prime subfield of $\mathbb{F}_{5^3}$. Trivially $\mathrm{Cay}(\mathbb{F}_{p^{\tilde{f}}}, \tilde{D})$ is an srg. By Corollary 3.0.12, $\mathrm{Cay}(\mathbb{F}_q, D)$ with $D = \cup_{i=0}^{p_1^{m-1}-1} C_i$ is an srg.

Example 3.0.15. Let $p = 2$, $p_1 = 127$ and $N = p_1^m$ for $m \geq 1$. Again it is easy to use induction to prove that $\mathrm{ord}_{127^m}(2) = \phi(127^m)/18$. Let $\mathbb{F}_q$ be the finite field of order $q = 2^f$, where $f = \phi(127^m)/w$ with $w = 18$. Now $\tilde{f} = 7$. Let $\tilde{D}$ be the subgroup of $\mathbb{F}_{2^7}^*$ of index $p_1 = 127$. Then $\tilde{D}$ is nothing but $\mathbb{F}_2^* = \{1\}$. Trivially $\mathrm{Cay}(\mathbb{F}_{p^{\tilde{f}}}, \tilde{D})$ is an srg.

By Corollary 3.0.12, $\mathrm{Cay}(\mathbb{F}_q,\ D)$ with $D = \cup_{i=0}^{p_1^{m-1}-1} C_i$ is an srg. It should be noted that as an srg, $\mathrm{Cay}(\mathbb{F}_q,\ D)$ is not trivial at all.

Chapter 4

PSEUDOCYCLIC AND NON-AMORPHIC FUSION SCHEMES

In this chapter, we construct counterexamples to A. I. Ivanov's conjecture. In fact, we are aiming for obtaining infinite families. Our examples are in the index 2 case. By the results in [25], every relation of the examples we obtain defines an srg, which is neither Latin square nor negative Latin square. Then, we obtain counterexamples to Ivanov's conjecture through this approach. Furthermore, by the Bannai-Muzychuk criterion, the counterexamples are pseudocyclic.

Let $\mathbb{F}_q$ be the finite field of order q and γ be a primitive element of $\mathbb{F}_q$. Let $N > 1$ be a proper positive divisor of $q-1$ and N is odd. Let C_0, $C_1 = \gamma C_0$, $\ldots$, $C_{N-1} = \gamma^{N-1}C_0$ be the cyclotomic classes of order N of $\mathbb{F}_q$, where $C_0 = \langle \gamma^N \rangle \leq \mathbb{F}_q^*$. Assume that $-1 \in C_0$. Define $R_0 = \{(x,x) \mid x \in \mathbb{F}_q\}$, and for $i \in \{1, 2, \ldots, N\}$, define $R_i = \{(x,y) \mid x, y \in \mathbb{F}_q, x - y \in C_{i-1}\}$. Then $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$ is the cyclotomic association scheme of class N over $\mathbb{F}_q$.

By the results in Baumert, Mill and Ward's paper, [8], we have:

Proposition 4.0.16. *The association scheme* $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$ *is amorphic if and only if* -1 *is congruent to a power of* p *modulo* N*.*

Proof: Bannai and Munemasa proved the Proposition in their paper [10]. □

Below we shall show that even in the case index 2, where -1 is not in the subgroup $\langle p \rangle$, the cyclic group generated by p and $\langle p \rangle$ has index 2 in $(\mathbb{Z}/N\mathbb{Z})^*$, the cyclotomic association scheme $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$ is not amorphic, we can still have interesting fusion schemes of $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$.

Based on Section 2.4, if N is odd, we have the following three possibilities in the index 2 case (see [56]), where both p_1 and p_2 are primes.

(1) $N = p_1^m$, $p_1 \equiv 3 \pmod 4$;

(2) $N = p_1^m p_2^n$, $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)$;

(3) $N = p_1^m p_2^n$, $p_1 \equiv 1, 3 \pmod 4$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$ and $p_2 \equiv 3 \pmod 4$, $\mathrm{ord}_{p_2^n}(p) = \phi(p_2^n)/2$.

We first deal with the second case when $n = 1$.

4.1 The Index 2 Case With $N = p_1^m p_2$

In this subsection, we assume that $N = p_1^m p_2$ ($m \geq 1$), p_1, p_2 are primes such that $\{p_1 \pmod 4, p_2 \pmod 4\} = \{1, 3\}$, p is a prime such that $\gcd(p, N) = 1$, $\mathrm{ord}_{p_1^m}(p) = \phi(p_1^m)$ and $\mathrm{ord}_{p_2}(p) = \phi(p_2)$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, and as before let $C_0, C_1, \ldots, C_{N-1}$ be the N-th cyclotomic classes of $\mathbb{F}_q$. Note that here we have $-C_i = C_i$ for all $0 \leq i \leq N-1$ since either $2N | (q-1)$ or q is even. For convenience, we define $d := p_1 p_2$. For $0 \leq k \leq d-1$, define

$$D_k = \bigcup_{i=0}^{p_1^{m-1}-1} C_{ip_2 + kp_1^{m-1}} \tag{4.1}$$

Note that $D_k = \gamma^{kp_1^{m-1}} D_0$ and $\{0\}, D_0, D_1, \ldots, D_{d-1}$ form a partition of $\mathbb{F}_q$. Now define $R'_0 = R_0$ and

$$R'_k = \{(x, y) \mid x, y \in \mathbb{F}_q, x - y \in D_{k-1}\}. \tag{4.2}$$

We will show that $(\mathbb{F}_q, \{R'_k\}_{0 \leq k \leq d})$ is a fusion scheme of $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$. Our proof depends on Theorem 2.4.6. (See [42])

Let χ_1 be the multiplicative character of order p_1^m of $\mathbb{F}_q$ defined by $\chi_1(\gamma) = \exp(\frac{2\pi i}{p_1^m})$, and let χ_2 be the multiplicative character of order p_2 of $\mathbb{F}_q$ defined by $\chi_2(\gamma) = \exp(\frac{2\pi i}{p_2})$. By Theorem 2.4.6, we have

$$g(\bar{\chi}_1 \bar{\chi}_2) = \frac{b + c\sqrt{-p_1 p_2}}{2} p^{h_0}, \tag{4.3}$$

where $h_0 = \frac{f-h}{2}$ (h is the class number of $\mathbb{Q}(\sqrt{-p_1 p_2})$), $b, c \not\equiv 0 \pmod p$, $b^2 + p_1 p_2 c^2 = 4p^h$, and $b \equiv 2p^{h/2} \pmod \ell$, here $\ell \in \{p_1, p_2\}$ is the prime congruent to 3 modulo 4.

Now, we are ready to prove the first case when $N = p_1^m p_2$.

Theorem 4.1.1. *With the definition of R'_k given in (4.2), $(\mathbb{F}_q, \{R'_k\}_{0\le k\le d})$ is a pseudocyclic association scheme.*

Proof: We will first prove that $(\mathbb{F}_q, \{R'_k\}_{0\le k\le d})$ is an association scheme by using the Bannai-Muzychuk criterion discussed in Section 1.

For each a, $0 \le a \le N-1$, there exists a unique $i_a \in \{0, 1, ..., p_1^{m-1}-1\}$ such that $p_1^{m-1} \mid (a + p_2 i_a)$. It follows that there is a unique j_a, $0 \le j_a \le p_1p_2 - 1$, such that $a \equiv -p_2 i_a + p_1^{m-1} j_a \pmod N$. It is now easy to check that $-ip_2 + jp_1^{m-1}$, $0 \le i \le p_1^{m-1}-1$ and $0 \le j \le p_1p_2 - 1$, form a complete set of residues modulo N.

The group of additive characters of $\mathbb{F}_q$ consists of ψ_0 and ψ_{γ^a}, $0 \le a \le q-2$, where ψ_0 is the trivial character and ψ_{γ^a} is defined by

$$\psi_{\gamma^a} : \mathbb{F}_q \to \mathbb{C}^*, \quad \psi_{\gamma^a}(x) = \xi_p^{\mathrm{Tr}(\gamma^a x)}. \tag{4.4}$$

We usually write ψ_1 simply as ψ. The character values of D_0 were computed in the proof of Theorem 5.1 [25]. Since D_k is a (multiplicative) translate of D_0, we know the character values of D_k as well. Explicitly, for each a, $0 \le a \le N-1$, write

$$a \equiv -p_2 i_a + p_1^{m-1} j_a \pmod N,$$

with $0 \le i_a \le p_1^{m-1} - 1$ and $0 \le j_a \le p_1p_2 - 1$. For convenience we introduce the Kronecker delta δ_{a,p_1}, which equals 1 if $p_1|a$, 0 otherwise. Also we define δ_{a,p_2} by setting it equal to 1 if $p_2|a$, 0 otherwise. By the results in [25], we have

$$\psi_{\gamma^a}(D_k) = \psi(\gamma^{a+p_1^{m-1}k} D_0) = \frac{1}{N} T_{a+p_1^{m-1}k},$$

where

$$\begin{aligned} T_{a+p_1^{m-1}k} = {} & -p_1^{m-1} - (-1)^{\frac{p_1-1}{2}} p_1^{m-1} p_2 \sqrt{q}\,\delta_{a+p_1^{m-1}k,p_2} - (-1)^{\frac{p_2-1}{2}} p_1^m \sqrt{q}\,\delta_{j_a+k,p_1} \\ & + \frac{b}{2} p^{h_0} p_1^{m-1} (p_1 \delta_{j_a+k,p_1} - 1)(p_2 \delta_{a+p_1^{m-1}k,p_2} - 1) \\ & - \left(\frac{a+p_1^{m-1}k}{p_2}\right)\left(\frac{j_a+k}{p_1}\right) \frac{c}{2} p^{h_0} p_1^m p_2 \end{aligned}$$

In the above formula, b, c are given by (4.3), and $(\frac{\cdot}{p_2})$, $(\frac{\cdot}{p_1})$ are Legendre symbols. Observe that $a + p_1^{m-1}k \equiv -p_2 i_a + p_1^{m-1}(j_a + k) \pmod N$. So $\delta_{a+p_1^{m-1}k,p_2} = \delta_{j_a+k,p_2}$, and $\left(\frac{a+p_1^{m-1}k}{p_2}\right) = \left(\frac{p_1}{p_2}\right)^{m-1}\left(\frac{j_a+k}{p_2}\right)$. Therefore, $\psi_{\gamma^a}(D_k)$ is independent of i_a.

In order to apply the Bannai-Muzychuk criterion, we define the following partition of $\{\psi_{\gamma^a} \mid a \in \mathbb{Z}/N\mathbb{Z}\}$. For each j, $0 \le j \le d-1$, define

$$\Delta_{j+1} = \{\psi_{\gamma^{-p_2 i + p_1^{m-1} j}} \mid 0 \le i \le p_1^{m-1} - 1\},$$

and $\Delta_0 = \{\psi_0\}$. Clearly $\Delta_0, \Delta_1, \ldots, \Delta_d$ form a partition of $\{\psi_{\gamma^a} \mid a \in \mathbb{Z}/N\mathbb{Z}\}$. For each $0 \le k \le d-1$, since $\psi_{\gamma^a}(D_k)$ is independent of i_a (here $a \equiv -p_2 i_a + p_1^{m-1} j_a \pmod N$), we see that $\psi_{\gamma^a}(D_k)$ is a constant for those a in the same subset of the above partition. By the Bannai-Muzychuk criterion (with $\Lambda_0 = \{0\}$, $\Lambda_{j+1} = \{1 + ip_2 + p_1^{m-1} j \mid 0 \le i \le p_1^{m-1} - 1\}$, $0 \le j \le d-1$), we see that $(\mathbb{F}_q, \{R_0', R_1', \ldots, R_d'\})$ is an association scheme.

Next we show that the association scheme $(\mathbb{F}_q, \{R_k'\}_{0 \le k \le d})$ is pseudocyclic. To this end, we show that the following group ring equation holds in $\mathbb{Z}[(\mathbb{F}_q, +)]$.

Claim: $\sum_{k=0}^{d-1} D_k^2 = (q-1)\cdot 0_{\mathbb{F}_q} + (\frac{q-1}{p_1 p_2} - 1)(\mathbb{F}_q - 0_{\mathbb{F}_q})$, where $0_{\mathbb{F}_q}$ is the zero element in $\mathbb{F}_q$.

For any a, $0 \le a \le N-1$, we write $a \equiv -i_a p_2 + j_a p_1^{m-1} \pmod N$ with $i_a \in \{0, 1, \ldots, p_1^{m-1} - 1\}$ and $j_a \in \{0, 1, 2, \ldots, d-1\}$. Since $\psi_{\gamma^a}(D_k)$ is independent of i_a, we may assume that $i_a = 0$. We now compute

$$\sum_{k=0}^{d-1} \psi_{\gamma^a}(D_k)^2 = \frac{1}{N^2} \sum_{k=0}^{d-1} T^2_{p_1^{m-1}(j_a+k)} = \frac{1}{N^2} \sum_{k=0}^{d-1} T^2_{kp_1^{m-1}}.$$

Since the last expression above is independent of a, we see that the $\sum_{k=0}^{d-1} \psi_{\gamma^a}(D_k)^2$ are equal to the same constant for all $0 \le a \le N-1$. Since each D_k is a union of some N-th cyclotomic classes, it follows that $\sum_{k=0}^{d-1} \psi_{\gamma^a}(D_k)^2$ are equal to the same constant for all $0 \le a \le q-2$. Therefore, by the inversion formula, we have

$$\sum_{k=0}^{d-1} D_k^2 = (n - \lambda) \cdot 0_{\mathbb{F}_q} + \lambda \mathbb{F}_q,$$

for some integers n, λ. Now applying the principal character to both sides, and computing the coefficients of $0_{\mathbb{F}_q}$ on both sides, we have

$$n = p_1p_2 \cdot \frac{q-1}{p_1p_2},$$
$$n + (q-1)\lambda = d \cdot \left(\frac{q-1}{p_1p_2}\right)^2.$$

It follows that $n = q-1$, and $\lambda = \frac{q-1}{p_1p_2} - 1$. The claim is now established. A direct consequence is that $\sum_{i=0}^{d-1} p_{i,i}^j = \frac{q-1}{N} - 1$, for all j, where $p_{i,i}^j$ are the intersection parameters given by $D_i^2 = \sum_{j=0}^{d-1} p_{i,i}^j D_j + p_{i,i}^0 \cdot 0_{\mathbb{F}_q}$. By Part (2) of Theorem 2.5.3, the association scheme $(\mathbb{F}_q, \{R'_k\}_{0\le k\le d})$ is pseudocyclic. The proof is complete. □

In order to obtain counterexamples to Ivanov's conjecture, we need each R'_k $(1 \le k \le d)$ in Theorem 4.1.1 to be strongly regular. Note that R'_k is just the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D_{k-1})$, and $\mathrm{Cay}(\mathbb{F}_q, D_{k-1}) \cong \mathrm{Cay}(\mathbb{F}_q, D_0)$ for all $1 \le k \le d$ since $D_{k-1} = \gamma^{(k-1)p_1^{m-1}} D_0$. It follows that if $\mathrm{Cay}(\mathbb{F}_q, D_0)$ is strongly regular, then all R'_k, $1 \le k \le d$, are strongly regular. In [25], we obtained necessary and sufficient conditions for $\mathrm{Cay}(\mathbb{F}_q, D_0)$ to be strongly regular. (Theorem 2.4.7)

Based on the results in [25], we used a computer to search for p, p_1, p_2 satisfying the conditions in Theorem 2.4.7. Feng, Wu and Xiang found six infinite families of strongly regular graphs in this way. By the discussion preceding Theorem 2.4.7, and since the parameters of each of the six examples of srg are neither Latin square type nor negative Latin square type, each of the six families of srg gives rise to an infinite class of counterexamples to Ivanov's conjecture by Theorem 2.5.5. In Chapter 5, we shall list the parameters of these examples. For the detailed reasons why we have strongly regular graphs, we refer the reader to [25].

Example 4.1.2. *Let $p = 2$, $q = 2^{4\cdot 3^{m-1}}$, $p_1 = 3$, $p_2 = 5$, $N = 3^m \cdot 5$, with $m \ge 1$. Then we have a 15-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\le k\le 15})$ in which each relation R'_k, $1 \le k \le 15$, is strongly regular.*

We remark that when $m = 2$, Example 4.1.2 is the same as Example 1 in [32].

Example 4.1.3. *Let $p = 2$, $q = 2^{4\cdot 5^{m-1}}$, $p_1 = 5$, $p_2 = 3$, $N = 5^m \cdot 3$, with $m \geq 1$. Then we have a 15-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 15})$ in which each relation R'_k, $1 \leq k \leq 15$, is strongly regular.*

We remark that when $m = 2$, Example 4.1.3 is the same as Example 2 in [32].

Example 4.1.4. *Let $p = 3$, $q = 3^{12\cdot 5^{m-1}}$, $p_1 = 5$, $p_2 = 7$, $N = 5^m \cdot 7$, with $m \geq 1$. Then we have a 35-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 35})$ in which each relation R'_k, $1 \leq k \leq 35$, is strongly regular.*

Example 4.1.5. *Let $p = 3$, $q = 3^{12\cdot 5^{m-1}}$, $p_1 = 7$, $p_2 = 5$, $N = 7^m \cdot 5$, with $m \geq 1$. Then we have a 35-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 35})$ in which each relation R'_k, $1 \leq k \leq 35$, is strongly regular.*

Example 4.1.6. *Let $p = 3$, $q = 3^{144\cdot 17^{m-1}}$, $p_1 = 17$, $p_2 = 19$, $N = 17^m \cdot 19$, with $m \geq 1$. Then we have a 323-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 323})$ in which each relation R'_k, $1 \leq k \leq 323$, is strongly regular.*

Example 4.1.7. *Let $p = 3$, $q = 3^{144\cdot 19^{m-1}}$, $p_1 = 19$, $p_2 = 17$, $N = 19^m \cdot 17$, with $m \geq 1$. Then we have a 323-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 323})$ in which each relation R'_k, $1 \leq k \leq 323$, is strongly regular.*

We remark that by using Corollary 3.2 in [32], one can further obtain 3-class fusion schemes of the above pseudocyclic association schemes, in which two relations are strongly regular graphs, while the third relation is not (see the character table of these 3-class fusion schemes in the statement of Corollary 3.2 of [32]).

4.2 The Index 2 Case With $N = p_1^m$

In this subsection, we assume that $N = p_1^m$ (here $m \geq 1$, $p_1 > 3$ is a prime such that $p_1 \equiv 3 \pmod 4$), p is a prime such that $\gcd(N, p) = 1$, and $f := \mathrm{ord}_N(p) = \phi(N)/2$. Let $q = p^f$, and as before let $C_0, C_1, \ldots, C_{N-1}$ be the N-th cyclotomic classes of $\mathbb{F}_q$.

Note that $-C_i = C_i$ for all $0 \leq i \leq N-1$ since either $2N|(q-1)$ or q is even. For $0 \leq k \leq p_1 - 1$, define

$$D_k = \bigcup_{i=0}^{p_1^{m-1}-1} C_{i+kp_1^{m-1}} \tag{4.5}$$

Note that $D_k = \gamma^{kp_1^{m-1}} D_0$ and $\{0\}, D_0, D_1, \ldots, D_{p_1-1}$ form a partition of $\mathbb{F}_q$. Now define $R'_0 = R_0$ and

$$R'_k = \{(x,y) \mid x, y \in \mathbb{F}_q, x - y \in D_{k-1}\}. \tag{4.6}$$

We will show that $(\mathbb{F}_q, \{R'_k\}_{0 \leq k \leq p_1})$ is a fusion scheme of $(\mathbb{F}_q, \{R_i\}_{0 \leq i \leq N})$.

Let χ be the multiplicative character of $\mathbb{F}_q$ defined by $\chi(\gamma) = \exp(\frac{2\pi i}{N})$. By Theorem 2.4.4, we have

$$g(\bar{\chi}) = \frac{b + c\sqrt{-p_1}}{2} p^{h_0}, \quad b, c \not\equiv 0 \pmod{p}, \tag{4.7}$$

where $h_0 = \frac{f-h}{2}$ and h is the class number of $\mathbb{Q}(\sqrt{-p_1})$, $b^2 + p_1 c^2 = 4p^h$, and $bp^{h_0} \equiv -2 \pmod{p_1}$.

Now, we are ready to prove the first case when $N = p_1^m$.

Theorem 4.2.1. *With the definition of R'_k given in (4.6), $(\mathbb{F}_q, \{R'_k\}_{0 \leq k \leq p_1})$ is a pseudocyclic association scheme.*

Proof: The proof is similar to that of Theorem 4.1.1. For each a, $0 \leq a \leq N-1$, there is a unique $i_a \in \{0, 1, \ldots, p_1^{m-1} - 1\}$, such that $p_1^{m-1}|(a + i_a)$. It follows that there is a unique $j_a, 0 \leq j_a \leq p_1 - 1$, such that $a \equiv -i_a + p_1^{m-1} j_a \pmod{N}$. It is now easy to check that $-i + jp_1^{m-1}$, $0 \leq i \leq p_1^{m-1} - 1$ and $0 \leq j \leq p_1 - 1$, form a complete set of residues modulo N.

The group of additive characters of $\mathbb{F}_q$ consists of ψ_0 and ψ_{γ^a}, $0 \leq a \leq q-2$. The character values of D_0 were computed in the proof of Theorem 4.1 [25]. Since D_k is a (multiplicative) translate of D_0, we know the character values of D_k as well. Explicitly, for each a, $0 \leq a \leq N-1$, write

$$a \equiv -i_a + p_1^{m-1} j_a \pmod{N},$$

with $0 \leq i_a \leq p_1^{m-1} - 1$ and $0 \leq j_a \leq p_1 - 1$. For convenience, we also introduce the Kronecker delta δ_{j_a}, which equals 1 if $p_1 | j_a$, and 0 otherwise. By the results in [25], we have

$$\psi_{\gamma^a}(D_k) = \psi(\gamma^{a+kp_1^{m-1}} D_0) = \frac{1}{N} T_{a+kp_1^{m-1}},$$

where

$$T_{a+kp_1^{m-1}} = -p_1^{m-1} + \frac{p^{h_0} p_1^{m-1} b}{2}(p_1 \delta_{j_a+k} - 1) - \frac{p^{h_0} p_1^m c}{2}\left(\frac{j_a + k}{p_1}\right).$$

In the above formula, b, c are given in (4.7), and $(\frac{\cdot}{p_1})$ is the Legendre symbol. It is important to note that $\psi_{\gamma^a}(D_k)$ is independent of i_a.

We define the following partition of $\{\psi_{\gamma^a} \mid a \in \mathbb{Z}/N\mathbb{Z}\}$. For each j, $0 \leq j \leq p_1 - 1$, we define

$$\Delta_{j+1} = \{\psi_{\gamma^{-i+p_1^{m-1}j}} \mid 0 \leq i \leq p_1^{m-1} - 1\},$$

and $\Delta_0 = \{\psi_0\}$. Then clearly $\Delta_0, \Delta_1, \ldots, \Delta_{p_1}$ form a partition of $\{\psi_{\gamma^a} \mid a \in \mathbb{Z}/N\mathbb{Z}\}$. For each $0 \leq k \leq p_1 - 1$, since $\psi_{\gamma^a}(D_k)$ is independent of i_a (here $a \equiv -i_a + p_1^{m-1} j_a \pmod{N}$), we see that $\psi_{\gamma^a}(D_k)$ is a constant for those a in the same subset of the above partition. By the Bannai-Muzychuk criterion (with $\Lambda_0 = \{0\}$, $\Lambda_{j+1} = \{1 + i + p_1^{m-1} j \mid 0 \leq i \leq p_1^{m-1} - 1\}$, $0 \leq j \leq p_1 - 1$), we see that $(\mathbb{F}_q, \{R'_0, R'_1 \ldots, R'_{p_1}\})$ is an association scheme.

Similarly we can show that the following group ring equation holds in $\mathbb{Z}[(\mathbb{F}_q, +)]$:

$$\sum_{k=0}^{p_1-1} D_k^2 = (q-1) \cdot 0_{\mathbb{F}_q} + (\frac{q-1}{p_1} - 1)(\mathbb{F}_q - 0_{\mathbb{F}_q}),$$

from which the pseudocyclicity of the scheme $(\mathbb{F}_q, \{R'_0, R'_1, \ldots, R'_{p_1}\})$ follows. We omit the details of the proof of the above group ring equation. The proof is now complete. □

In order to obtain counterexamples to Ivanov's conjecture, we need to have each R'_k $(1 \leq k \leq p_1)$ in Theorem 4.2.1 to be strongly regular. Note that R'_k is just the Cayley graph $\mathrm{Cay}(\mathbb{F}_q, D_{k-1})$, and $\mathrm{Cay}(\mathbb{F}_q, D_{k-1}) \cong \mathrm{Cay}(\mathbb{F}_q, D_0)$ for all $1 \leq k \leq p_1$ since $D_{k-1} = \gamma^{(k-1)p_1^{m-1}} D_0$. Again it follows that if $\mathrm{Cay}(\mathbb{F}_q, D_0)$ is strongly regular, then all

R'_k, $1 \le k \le p_1$, are strongly regular. In [25], we obtained necessary and sufficient conditions for $\mathrm{Cay}(\mathbb{F}_q, D_0)$ to be strongly regular. (Theorem 2.4.5)

Based on the results in [25], Feng, Wu and Xiang used a computer to search for p, p_1 satisfying the conditions in Theorem 2.4.5. We found six infinite families of strongly regular graphs in this way. By the discussion preceding Theorem 2.4.5, each of the six examples of srg gives rise to a class of infinitely many counterexamples to Ivanov's conjecture by Theorem 2.5.5. In Chapter 5, we shall list the parameters of these examples. For the detailed reasons why we have strongly regular graphs, we refere the reader to [25].

Example 4.2.2. *Let $p = 2$, $q = 2^{3\cdot 7^{m-1}}$, $p_1 = 7$, $N = p_1^m$, $m \ge 1$ is an integer. Then we have a 7-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\le k\le 7})$ in which each relation R'_k, $1 \le k \le 7$, is strongly regular.*

We remark that when $m = 2$, Example 4.2.2 is the same as Example 3 of [32].

Example 4.2.3. *Let $p = 3$, $q = 3^{53\cdot 107^{m-1}}$, $p_1 = 107$, $N = p_1^m$, $m \ge 1$ is an integer. Then we have a 107-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\le k\le 107})$ in which each relation R'_k, $1 \le k \le 107$, is strongly regular.*

Example 4.2.4. *Let $p = 5$, $q = 5^{9\cdot 19^{m-1}}$, $p_1 = 19$, $N = p_1^m$, $m \ge 1$ is an integer. Then we have a 19-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\le k\le 19})$ in which each relation R'_k, $1 \le k \le 19$, is strongly regular.*

Example 4.2.5. *Let $p = 5$, $q = 5^{249\cdot 499^{m-1}}$, $p_1 = 499$, $N = p_1^m$, $m \ge 1$ is an integer. Then we have a 499-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\le k\le 499})$ in which each relation R'_k, $1 \le k \le 499$, is strongly regular.*

Example 4.2.6. *Let $p = 17$, $q = 17^{33\cdot 67^{m-1}}$, $p_1 = 67$, $N = p_1^m$, $m \ge 1$ is an integer. Then we have a 67-class pseudocyclic fusion scheme $(\mathbb{F}_q, \{R'_k\}_{0\le k\le 67})$ in which each relation R'_k, $1 \le k \le 67$, is strongly regular.*

Example 4.2.7. *Let* $p = 41$, $q = 41^{81\cdot 163^{m-1}}$, $p_1 = 163$, $N = p_1^m$, $m \geq 1$ *is an integer. Then we have a* 163*-class pseudocyclic fusion scheme* $(\mathbb{F}_q, \{R'_k\}_{0\leq k\leq 163})$ *in which each relation* R'_k, $1 \leq k \leq 163$, *is strongly regular.*

Again we remark that by using Corollary 3.2 in [32], one can further obtain 3-class fusion schemes of the above pseudocyclic association schemes, in which two relations are strongly regular graphs, while the third relation is not.

Chapter 5

SOME OPEN PROBLEMS

In this chapter, we present some open problems that are related to the materials in the previous chapters.

Problem 1: Prove Conjecture 1.0.1.

Schmidt and White proposed the conjecture in [50] by using the language of irreducible cyclic codes. In fact, there is a one-to-one correspondence between cyclotomic srgs and two-weight irreducible cyclic codes. (See [14, 17, 40]) Hence, their conjecture gives a conjectural classification of all cyclotomic srgs as we mentioned in Chapter 1.

Table I lists all sporadic examples of cyclotomic srgs up to the number of vertices being 100,000.

Partial results on Conjecture 1.0.1 was given in [50]. Their proof was only about the index 2 case. Moreover, their proof is valid only when the generalized Riemann conjecture is true. After [50], there has been no essential progress on this problem.

Problem 2: Evaluate Gauss sums of the index 6 or higher explicitly.

Though we found a way to bypass this main obstacle in Chapter 3, it is still a good question to evaluate Gauss sums of index 6 or higher.

Problem 3: Generalize the last example in [21]. (Example (b) of [21])

This problem comes from De Lange's paper [21]. De Lange constructed four strongly regular Cayley graphs in this paper using unions of cyclotomic classes of finite fields. All but the last example have been generalized to be infinite families. Find a generalization of the last example.

REFERENCES

[1] Y. Aubry, P. Langevin, On the weight of binary irreducible cyclic codes, *Workshop on Coding and Cryptography WCC'05 (Springer)* **3969** *Norway* (2006), 46–54.

[2] L. Babai, *The Fourier transform and equations over finite Abelian groups*, available at: http://people.cs.uchicago.edu/∼laci/reu02/fourier.pdf.

[3] R. A. Bailey, *Association schemes, designed experiments, algebra and combinatorics*, Cambridge University Press, 2004.

[4] E. Bannai, Subschemes of some association schemes, *J. Algebra* **144** (1991), 167–188.

[5] E. Bannai, T. Ito, *Algebraic Combinatorics I: Association Schemes*, Benjamin/Cummings, Menlo Park, 1984.

[6] E. Bannai, A. Munemasa, Davenport-Hasse theorem and cyclotomic association schemes, *Proc. Algebraic Combinatorics*, Hirosaki University, 1990.

[7] L. D. Baumert, J. Mykkeltveit, Weight distributions of some irreducible cyclic codes, *DSN Progr. Rep.* **16** (1973), 128–131.

[8] L. D. Baumert, M. H. Mills, R. L. Ward, Uniform Cyclotomy, *J. Number Theory* **14** (1982), 67-82.

[9] B. C. Berndt, R. J. Evans, K. S. Williams, *Gauss and Jacobi Sums*, A Wiley-Interscience Publication, New York, 1998.

[10] R. C. Bose, D. M. Mesner, On linear associative algebras corresponding to association schemes of partially balanced designs, *Annals of Mathematical Statistics* **30** (1959), 21-38.

[11] T. Beth, D. Jungnickel, H. Lenz, *Design Theory*, second edition, Cambridge University Press, Cambridge, (1999).

[12] R. C. Bose, Strongly regular graphs, partial geometries, and partially balanced designs, *Pacific J. Math.* **13** (1963), 389-419.

[13] R. C. Bose, T. Shimamoto, Classification and analysis of partially balanced incomplete block designs with two associate classes, *Journal of the American Statistical Association*, **47** (1952), 151-184.

[14] A. E. Brouwer, W. H. Haemers, *Spectra of Graphs*, Universitext, Springer-Verlag, New York, 2012.

[15] A. E. Brouwer, A. M. Cohen, A. Neumaier, *Distance Regular Graphs, Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)], 18.* Springer-Verlag, Berlin, 1989.

[16] A. E. Brouwer, J. H. Van Lint, Strongly Regular Graphs and Partial Geometries, *Enumeration and Design - Proc. Silver Jubilee Conf. on Combinatorics, Waterloo* (1982), 85-122.

[17] R. Calderbank, W. M. Kantor, The geometry of two-weight codes, *Bull. Lond. Math. Soc.* **18**(2) (1986), 97-122.

[18] E. R. van Dam, A characterization of association schemes from affine spaces, *Des. Codes Cryptogr.* **21** (2000), 83–86.

[19] E. R. van Dam, Strongly regular decompositions of the complete graph, *J. Algebraic Combin.* **17** (2003), 181–201.

[20] E. R. van Dam, M. Muzychuk, Some implications on amorphic association schemes, *J. Combin. Theory* (A) **117** (2010), 111–127.

[21] C. L. M. De Lange, Some new cyclotomic strongly regular graphs, *J. Algebraic Combin.* **4** (1995), 329-330.

[22] Ph. Delsarte, *An algebraic approach to the association schemes of coding theory*, Philips Res. Rep. Suppl. **10**, N.V. Philips' Gloeilampenfabrieken, 1973.

[23] R. Evans, H. Holmann, C. Kratenthaler, Q. Xiang, Gauss sums, Jacobi sums and p-ranks of cyclic difference sets, *J. Combin. Theory Ser. A* **87** (1999), 74-119.

[24] K. Feng, J. Yang, S. Luo, Gauss sum of index 4: (1) Cyclic case, *Acta Math. Sin. (English Ser.)* **21-6** (2005), 1425-1434.

[25] T. Feng, Q. Xiang, Strongly regular graphs from unions of cyclotomic classes, *J. Combin. Theory (B)*, **102** (2012), 982-995.

[26] T. Feng, F. Wu, Q. Xiang, Pseudocyclic and non-amorphic fusion schemes of the cyclotomic association schemes , *Designs, Codes and Cryptography*, **65** (2012), 247-257.

[27] T. Feng, K. Momihara, Q. Xiang, Constructions of strongly regular Cayley graphs and skew Hadamard difference sets from cyclotomic classes, submitted. `arXiv:1201.0701`.

[28] G. Ge, Q. Xiang, T. Yuan, Constructions of strongly regular Cayley graphs using index 4 Gauss sums, *J. Algebraic Combin.* **37** (2013), 313–329

[29] C. Godsil, *Association schemes*, http://quoll.uwaterloo.ca/mine/Notes/assoc2.pdf .

[30] C. Godsil, G. Royle, *Algebraic Graph Theory*, Springer-Verlag, New York, 2001.

[31] H. D. L. *Hollmann, Association schemes*, Master Thesis, Eindhoven University of Technology, 1982.

[32] T. Ikuta, A. Munemasa, Pseudocyclic association schemes and strongly regular graphs, *European J. Combin.* **31** (2010), 1513-1519.

[33] A. A. Ivanov, C. E. Praeger, Problem session at ALCOM-91, *Europ. J. Combin.* **15** (1994), 105-112.

[34] K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Second Edition, Springer-Verlag, New York, 1990.

[35] P. Langevin, A new class of two-weight codes, *Finite Fields and Applications, Glasgow, 1995, in: London Math. Soc. Lecture Note Ser.* **233** (1996), 181-187.

[36] P. Langevin, Calculs de certaines sommes de Gauss, *J. Number Theory*, **63** (1997), 59-64.

[37] S. Lang, *Algebra*, Rev. Third Edition, Springer-Verlag, 2000.

[38] S. Lang, *Cyclotomic fields I and II*, Combined Revised Edition, Springer-Verlag, 1994.

[39] R. Lidl, H. Niederreiter, *Finite Fields*, Addison-Wesley, 1983.

[40] S. L. Ma, A survey of partial difference sets, *Des. Codes Cryptogr.* **4** (1994), 221-261.

[41] H. B. Mann, *Introduction to algebraic number theory*, Ohio State University Press, Columbus 1955.

[42] O. D. Mbodj, Quadratic Gauss sums, *Finite Fields and Appl.*, **4** (1998), 347–361.

[43] R. J. McEliece, Irreducible cyclic codes and Gauss sums. *Combinatorics (Proc. NATO Advanced Study Inst., Breukelen, 1974), Part 1: Theory of designs, finite geometry and coding theory*, 179-196.

[44] K. Momihara, Strongly regular Cayley graphs, skew Hadamard difference sets, and rationality of relative Gauss sums, accepted. `arXiv:1202.6414`.

[45] P. Meijer, M. van der Vlugt, The evaluation of Gauss sums for characters of 2-power order, *J. Number Theory*, **100** (2003), 381-395.

[46] M. E. Muzychuk, *V-rings of permutation groups with invariant metric*, Ph.D. thesis, Kiev State University, 1987.

[47] P. Ribenboim, *Algebraic Numbers*, New York: Wiley, 1972.

[48] J. Storer, *Cyclotomy and Difference Set*, Chicago: Markham, 1963.

[49] B. Schmidt, *Characters and cyclotomic fields in finite geometry*, LNM 1797, Springer, (2002).

[50] B. Schmidt, C. White, All two-weight irreducible cyclic codes?, *Finite Fields and Their Appl.* **8** (2002), 1-17.

[51] F. Thaine, Properties that characterize Gaussian periods and cyclotomic numbers, *Proc. AMS* **124** (1996), 35-45.

[52] J. H. Van Lint, R. Wilson, *A course in combinatorics*, second edition, Cambridge university press, 2001.

[53] F. Wu, Constructions of Strongly Regular Cayley Graphs using Even Index Gauss Sums, *J. Combinatorial Designs*, accepted.

[54] L. C. Washington, *Introduction to Cyclotomic fields*, Second Edition, Springer-Verlag, 1997.

[55] Qing, Xiang, Cyclotomy, Gauss sums, difference sets and strongly regular Cayley graphs, *Proceedings of Sequences and Their Applications - SETA 2012, 7th International Conference, Waterloo, ON, Canada, June 4-8*, (2012), 245–256.

[56] Y. Yang, L. Xia, Complete solving of explicit evaluation of Gauss sums in the index 2 case, *Sci. China Ser. A* **53**(9) (2010), 2525-2542.