Graphs of integral distance and their properties

by

Olivier Habineza

A thesis submitted in fulfilment of the requirements for the degree of PhD
in the
Department of Mathematics and Applied Mathematics,
University of the Western Cape

Supervisor: **Prof. Eric Mwambene**

September 2021

Declaration of Authorship

I declare that *Graph of integral distances and their properties* is my own work, that it has not been submitted for any degree or examination in any other university, and that all the sources I have used or quoted have been indicated and acknowledged by complete references.

Olivier Habineza September 2021

Signed:..

List of Symbols

Symbol	**Description**
$G, H, K, \cdots$	Groups
$\cong$	Isomorphism symbol
$\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \cdots$	Sets of numbers
$\mathbb{Z}_m$	Set of equivalence classes in $\mathbb{Z}$ modulo m
F	Field
F^*	$F \setminus \{0\}$
F^m	m-dimensional vector space over F
x	Scalar of F
$\mathbf{u}$	vector of F^m
$\mathbf{e}_i$ or $\mathbf{e}^{(i)}$	Vector with 1 at the i^{th} position and 0 elsewhere
A^T	Transpose of a matrix A
I_m	Identity $m \times m$ matrix
Γ	Graph
Γ^C	Complementary of a graph Γ
$\varnothing$	Empty set
$V(\Gamma)$	Vertex set of Γ
$E(\Gamma)$	Edge set of Γ
$\mathcal{P}_2(V)$	Set of subsets of V with exactly two elements
$\deg(x)$	Degree of the vertex x
$\mathbf{srg}(v, k, \lambda, \mu)$	Strongly regular graph with parameters v, k, λ, and μ
$\mathrm{Aut}\ \Gamma$	Automorphism group of Γ
$\mathrm{Cay}(G, S)$	Cayley graph with vertex set G and connecting set S
$\mathfrak{B}$	Boolean algebra or field of sets

$\mathbb{F}_q$	A finite field with q elements, $q = p^r$, p prime
$\mathbb{F}_q[x]$	Set of polynomials in x over $\mathbb{F}_q$
$(\mathbb{F}_q, 0)$ or $(0, \mathbb{F}_q)$	Set of elements of the form $(x, 0)$ or $(0, x)$, respectively, with $x \in \mathbb{F}_q$
$\mathbb{F}_q \cdot \mathbf{Q}$	Set of vectors of the form $x.\mathbf{Q}$ with $x \in \mathbb{F}_q$
$q \equiv 1 \pmod 4$	q congruent or equivalent to 1 modulo 4
$\square_q$	Set of all perfect squares in $\mathbb{F}_q$
$d^2(\mathbf{u}, \mathbf{v})$ or $N(\mathbf{u} - \mathbf{v})$	Squared distance between vectors $\mathbf{u}$ and $\mathbf{v}$ in $\mathbb{F}_q^m$
$N(\mathbf{x})$ of $d^2(\mathbf{0}, \mathbf{x})$	Norm of $\mathbf{x}$ in $\mathbb{F}_q^m$
$N^{\phi}(\mathbf{x})$	Norm of $\mathbf{x}$ in hyperbolic coordinates over $\mathbb{F}_q$ (ϕ is a switch to hyperbolic coordinates, see Chapter 3)
$\mathcal{C}_q$	Unit circle in $\mathbb{F}_q$
$\mathfrak{G}_{m,q}$	Graph of integral distances over $\mathbb{F}_q$ in m dimensions
$S^{(m)}$	Connecting set for the graph $\mathfrak{G}_{m,q}$, $m \geq 2$, as a Cayley graph
$\mathcal{Z}(m, q)$	Set of elements of $\mathbb{F}_q^m$ with zero norm
$\mathcal{S}(m, q)$	Set of elements of $\mathbb{F}_q^m$ whose norm is a non-zero perfect square
$\mathcal{N}(m, q)$	Set of elements of $\mathbb{F}_q^m$ whose norm is a non-square
$\mathcal{D}(m, q)$	Degree of the integral distance graph $\mathfrak{G}_{m,q}$
$\mathcal{A}(m, q)$ or $\mathcal{B}(m, q)$	Number of common neighbors of two adjacent vertices $\mathbf{0}$ and $\mathbf{v}$ with $\langle \mathbf{v}, \mathbf{v} \rangle \neq 0$ or $\langle \mathbf{v}, \mathbf{v} \rangle = 0$, respectively, $\mathbf{v} \in \mathbb{F}_q^m$
$P(q)$	Paley graph of order q, $q = p^r$, p prime, and $q \equiv 1 \pmod 4$
$\mathrm{Aut}(\mathbb{F}_q)$	Group of automorphisms of a field $\mathbb{F}_q$
$\mathrm{Aut}(G)$	Group of automorphisms of G
$\mathrm{Inn}(G)$	Group of inner automorphisms of G
$\mathrm{Out}(G)$	Group of outer automorphisms of G
$\mathrm{Aut}(\mathbb{F}_q^m)$	Automorphism group of the graph $\mathfrak{G}_{m,q}$
$\mathrm{AffAut}(\mathbb{F}_q^2)$	Affine automorphism group of the graph $\mathfrak{G}_{2,q}$
1_G	Identity element of G
$H \leqslant G$	H a subgroup of G
$H < G$	H a proper subgroup of G
$H \lhd G$	H a normal subgroup of G
G/H	Quotient group of G by H
$\langle H, K \rangle$	Group generated by two subgroups H and K
$\Delta \times \Gamma$	Cartesian product of Δ by Γ

Δ^r	Cartesian r^{th} power of Δ
$T_1 \times \cdots \times T_m$	Direct product of groups $T_1, \cdots, T_m$
T^m	Direct m^{th} power of the group T
$V_1 \oplus V_2$	Direct sum of two vector subspaces V_1 and V_2
$H \rtimes K$	Semi direct product of H by K
$C_G(H)$, $N_G(H)$	Centralizer, Normalizer of H in G
$Z(G)$	Center of G
$[m]$	The set $\{1, \cdots, m\}$ where m is any positive integer
S_Ω or $S_{[n]}$	Symmetric group over the set Ω or $[n]$, respectively
x^ϕ	Image of the point x by the homomorphism ϕ
α^x	Action of an element x of a group over a point α
α^G	Orbit of α for G
G_α	Stabilizer of α in G
G_Δ	Elementwise stabilizer of Δ in G
$G_{\alpha_1, \cdots, \alpha_k}$	Elementwise stabilizer of $\{\alpha_1, \cdots, \alpha_k\}$ in G
$H \wr_\Gamma K$	Wreath product of H by K with respect to the action of K on Γ
$\lambda_{\mathbf{u}}$	Translation by the vector $\mathbf{u}$ of $\mathbb{F}_q^m$
$\mathrm{Soc}(G)$	Socle of G
$G_{\{\Delta\}}$	Setwise stabilizer of Δ in G
$\mathrm{Graph}(\Delta)$	Orbital digraph
$\mathrm{AG}_m(F)$	Affine geometry of dimension m over F
$\mathrm{GL}_m(F)$	General linear group of dimension m over F
$\mathrm{AGL}_m(F)$	Affine linear group of dimension m over F
$\mathrm{A\Gamma L}_m(F)$	Affine semi-linear group of dimension m over F
$\Gamma\mathrm{L}_m(F)$	General semi-linear group of dimension m over F
$\mathrm{SL}_m(F)$	Special linear group of dimension m over F
$\mathrm{SU}_m(F)$	Special unitary group of dimension m over F
$\Omega_{\mathrm{m}}^{\epsilon}(\mathrm{F})$	Orthogonal group of dimension m over F; $\epsilon = +, -$
$\mathrm{B}_m(F)$, $\mathrm{D}_m(F)$	Chevalley groups
$\mathrm{Sz}(F)$	Suzuki group
$\mathrm{ASL}_m(F)$	Affine special linear group of dimension m over F
$\mathrm{PGL}_m(F)$	Projective linear group of dimension m over F
$\mathrm{PSL}_m(F)$ or $\mathrm{L}_m(F)$	Projective special linear group of dimension m over F
$\mathrm{PSU}_m(F)$	Projective special unitary group of dimension m over F

Abstract

Understanding the geometries of points in space has been attractive to mathematicians for ages. As a model, twelve years ago, Kurz and Meyer [32] considered point sets in the m-dimensional affine space $\mathbb{F}_q^m$ over a finite field $\mathbb{F}_q$ with $q = p^r$ elements, p prime, where each squared Euclidean distance of two points is a square in $\mathbb{F}_q$. The latter points are said to be at integral distance in $\mathbb{F}_q^m$, and the sets above are called integral point sets.

In exploring this phenomenon, graphs of integral distances have prominently featured. A graph of integral distances in $\mathbb{F}_q^m$ contains points in $\mathbb{F}_q^m$ as vertices, and $\{\mathbf{x}, \mathbf{y}\}$ is an edge if and only if $\mathbf{x}$ and $\mathbf{y}$ are at integral distance.

The thesis aims to explore some pertinent properties of integral distance graphs and their generalizations. In particular, they will be explored as Cayley graphs and strongly regular graphs. The thesis further explores some factorizations of the integral distance graph to determine the constituents having the same properties as the original graph. In particular, those constituent graphs will also be explored as Cayley and strongly regular graphs. In addition, it will further delve into the Boolean algebra of the Cayley sets of the constituent graphs of the integral distance graphs as well as their strong regularity.

Having looked at strong regularity of various small orders of integral distance graphs, Kurz and Meyer [32] conjectured that integral distance graphs are strongly regular exactly for $m \equiv 0 \pmod 2$. We will prove the conjecture.

Finally, the thesis will look at the automorphism groups of the constituent graphs of integral distance graphs in comparison with the automorphism groups of the original graphs. Since the m-dimensional case for symmetries with $m > 2$ was given in [32], our focus will restrict to the dimension $m = 2$. Basically, we deal with $q \equiv 1 \pmod 4$, where only the constituent graphs from the two base subsets of $\mathbb{F}_q^2$ (see Chapter 3) will be in consideration. In particular, we show that the automorphism group of one constituent is isomorphic to the direct product of the group of translations by the elements of $\mathbb{F}_q^2$ with the wreath product of the symmetric group $S_{[q-1]}$ by $S_{[2]}$, and that of the other constituent is isomorphic to the automorphism group of the original graph.

September 2021.

Dedication

I dedicate this study:

to our Almighty God, who gives me the strength and knowledge for my everyday life;

to my late father and mother who passed away in my early life;

to my brothers, sisters and other relatives for their moral and financial support;

and,

to all my friends around the world.

Acknowledgement

First of all, I would like to thank my supervisor Prof. Eric Mwambene for his support, motivation, and guidance. I am also grateful for his introduction of Graph Theory to me during my Honours' studies, which is a key to my work. In addition, I wish to thank Dr. Washeela Fish for her introduction of Coding Theory during my Honours' studies as a key of introducing me in to the world of Finite Fields, which is in turn another key of my research.

As my initial research was supposed to be for an MSc program, I wish to appreciate again my supervisor, together with Prof. Justin Munyakazi, Mrs. Nathalie Isaac, Mrs. Sedicka Kassiem from International Student Office, and the external examiners who had to read my work for its upgrade to a PhD degree. I would like to appreciate Dr. Mozart Umba Nsuami, Dr. Vodah Tope Sunday, together with my supervisor for their technical advice in using a LaTeX program for writing my thesis and supporting documents for upgrade of my Masters' degree to a PhD.

In terms of living costs, I wish to appreciate the University of the Western Cape to grant me different positions; namely, that of a Teaching Assistant and that of an Associate Lecturer in the Department of Mathematics and Applied Mathematics. Thanks to Prof. David Holgate, Mr. Allen Taylor, Mrs. Ntombizandile Lukas, Dr. Grant Muller, Dr. Cloud Makasu, and Dr. Mozart Umba Nsuami for their support. Also, I wish to thank the University and the National Research Fund (NRF) to grant me a bursary to cover all my fees in Masters' program until its upgrade to a PhD program.

My appreciation is also expressed greatly to my family members worldwide especially my in-law Dr. Guillaume Ndayambaje and his wife for their moral support as another key to complete my research. In addition, I wish to thank my sisters and relatives from European Union, USA, here in South Africa and elsewhere worldwide; namely, Mr. Vincent Gatwabuyenge, Mrs. Natacha Uwanyirigira, Mrs. Chantal Usanase, Mrs. Marie Noëlle Uwase, Mrs. Diana Uwinshuti and many more for their financial and moral support and their help to come here to South Africa. Also, my friends around the world are highly appreciated for their advices and help.

Finally, I wish to thank the Lord God in the name of Jesus Christ for His help, His guidance and being my guardian during all my studies.

Publications arising from this thesis

Habineza, O., Mwambene, E., On strong regularity of integral distance graphs. *Ready for submission.*

Habineza, O., Mwambene, E., Automorphism groups of the constituent graphs of integral distance graphs. *Ready for submission.*

List of Figures

List of Tables

Contents

Chapter 1

Introduction

1.1 Introduction and background

Two points in an Euclidean space are said to be at integral distance if their squared Euclidean distance is a perfect square. Integral point sets were defined in m-dimensional Euclidean spaces as sets of points with pairwise integral distances in Euclidean metric. (See [20, 21, 27, 29, 32]).

Characterisation of integral point sets in an Euclidean space has always been one of the mathematicians' enterprise since the time of Pythagoreans, who studied rectangles with integral side lengths and integral diagonals [21, 32]. Applications originate in Chemistry (molecules), Physics (Wavelengths), Robotics, Architecture; just to mention a few; see [19, 32].

There are a lot of unsolved problems concerning integral point sets that persist [7, Section 5.1] [32]. For example, it is not known whether a perfect cuboid, that is a box with integral edges, face diagonals and body diagonals exists [18, Problem D18] [21,23,32]. Another famous problem of integral point sets in an Euclidean space is that posted by P. Eldős, who asked for the existence of seven points in the plane, no three on a line, no four on a circle with pairwise integral distances [18, Problem D20] [22, 29]. Several conjectures and incorrect proof circulated that such a point set cannot exist, see [32]. Recently, the problem has been imported to understanding integral distances of inner product spaces [21].

A lot of work on integral point sets has been done in Euclidean spaces; see for instance [19, 24, 28, 30–32]. Some authors also consider other spaces. For instance, Banach spaces [15], integral point sets over rings [25], or integral point sets over finite fields [10, 21, 32] have been considered.

In this thesis, it is our focus to examine the properties of the inner product space $\mathbb{F}_q^m$ over a finite field $\mathbb{F}_q$ with $q = p^r$, p prime, and examine the graph of integral distances over the finite field $\mathbb{F}_q$.

For $m = 1$ or q even, all distances in affine spaces are integral and therefore offer nothing interesting. It is therefore self-evident that the focus has been on $m \geq 2$ and q odd. Hence we would like to examine if the properties of integral distances over a finite field $\mathbb{F}_q$ differ for dimensions $m = 2$ and $m > 2$. We are keenly interested in the properties of the squared distance between zero and a point for $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ in two dimensions. There, such a distance will be shown to be a reducible polynomial in the former case, and an irreducible polynomial in the latter case for q. We will also like to extend the results to dimensions greater than two and investigate if the squared distance between zero and a point is an irreducible polynomial for all cases of q.

An approach we will like to consider in this thesis is to construct graphs from the set of inner product spaces $\mathbb{F}_q^m$. This has been called the integral distance graph denoted by $\mathfrak{G}_{m,q}$. Our aim here is to examine if such a relational structure is a Cayley graph as well a strongly regular graph for some cases of m.

We will further consider the Boolean algebra of the Cayley sets of the constituents graphs of integral distance graphs, and investigate the properties of those constituent graphs which are Cayley for all $q = p^r$, p prime and $p > 2$.

Paley graphs denoted by $P(q)$, $q = p^r$, p prime, and $q \equiv 1 \pmod 4$, are defined as graphs with vertex set $\mathbb{F}_q$, a finite field with q elements, and whose vertices are connected by an edge if their difference is a perfect square in that field [12, 29]. Such graphs were shown in [12, Propositions 2.2.1-2.2.3 and Corollary 2.2.1] to be connected, symmetric, self-complementary, and strongly regular. In two dimensions and $q \equiv 3 \pmod 4$, the integral distance graph is isomorphic to a Paley graph of square order, see Theorem 5.3. In some sense, therefore these graphs generalize Paley graphs [32].

Finally, we will consider the action of automorphisms of integral distance graphs in relation to the automorphism group of the constituents.

In m dimensions with $m > 2$, it has been shown in [27, 32] that the automorphism group of the integral distance graph $\mathfrak{G}_{m,q}$ is contained in the affine semi-linear group $\mathrm{A\Gamma L}_m(\mathbb{F}_q)$. The former contains $\mathrm{Aut}(\mathbb{F}_q)$, consisting of Frobenius homomorphisms and the group of all translations. Hence the linear automorphisms of $\mathfrak{G}_{m,q}$ were shown to be only the elements $A \in \mathrm{GL}_m(\mathbb{F}_q)$ such that AA^T (with A^T the transpose of the matrix A) is a scalar matrix αI_m with $\alpha \in \mathbb{F}_q^*$ and I_m the $m \times m$ identity matrix, with further details. (See [32, Theorem 3.2]). Additionally in two dimensions, further details of automorphism of $\mathfrak{G}_{2,q}$ were given in [29] for $q \equiv 3 \pmod 4$, and in [26] for $q \equiv 1 \pmod 4$. Hence our point of interest for symmetries will only focus on the two-dimensional case for $q \equiv 1 \pmod 4$. Here, we shall only deal with automorphism groups of the constituent graphs of $\mathfrak{G}_{2,q}$.

In this thesis, we deal with finite structures only.

1.2 Overview of the thesis

The purpose of this thesis is to present what we consider as the building blocks of integral distance graphs and all its pertinent properties. We shall focus on integral distances over a finite field whose order is an odd prime power.

In Chapter 2, we begin by defining some basic concepts of graph theory, graph automorphisms and Cayley graphs. We shall look at the Boolean algebra of Cayley sets. We shall also consider integral distances and some of their properties. We shall present primitive groups and their characterizations.

In Chapter 3, we look at the integral distance graph $\mathfrak{G}_{m,q}$ and we show that it is a Cayley graph. First, we define the two base subsets of $\mathbb{F}_q^2$, $q \equiv 1 \pmod 4$; namely, S_1 and S_2. The former set consists of all non-zero vectors of $\mathbb{F}_q^2$ with a zero product of components, and the latter consist of vectors of $\mathbb{F}_q^2$ whose product of components is a non-zero perfect square. We will show that S_1 and S_2 are Cayley sets and see if they form the basis of a Boolean algebra of Cayley sets, so that the corresponding constituent graphs of $\mathfrak{G}_{2,q}$ to each element of the Boolean algebra is a Cayley graph. There, we will show that $\mathfrak{G}_{2,q}$ is a Cayley graph for every prime power q.

In Chapter 4, we show that all the constituent graphs of the integral distance graph $\mathfrak{G}_{2,q}$ mentioned above are strongly regular. We deduce that $\mathfrak{G}_{2,q}$, $q \equiv 1 \pmod 4$, is strongly regular, and then we determine if we have a Boolean algebra of Cayley sets for strong regularity of the corresponding Cayley graphs. In addition, we show the strong regularity of $\mathfrak{G}_{2,q}$ for $q \equiv 3 \pmod 4$. Finally, we prove the conjecture given in [32], showing that the integral distance graph $\mathfrak{G}_{m,q}$ with $m > 2$ is strongly regular exactly for $m \equiv 0 \pmod 2$.

In Chapter 5, since the m-dimensional case for $m > 2$ in terms of symmetries of $\mathfrak{G}_{m,q}$ has been studied in [27, 32], we will restrict to the case of $m = 2$. Basically, we shall look at the automorphism groups of constituent graphs $\Gamma_i = \mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2$, of the integral distance graph $\mathfrak{G}_{2,q}$ with some details of the automorphism groups of the latter graph for $q \equiv 1 \pmod 4$. In addition, we shall present some details of automorphism group of $\mathfrak{G}_{2,q}$ for $q \equiv 3 \pmod 4$ in comparison with the automorphism group of the Paley graph $P(q^2)$.

Chapter 6 provides a summary of the study and give an outlook for further studies.

Chapter 2

Preliminaries

In this chapter, we present the necessary preliminaries relating to graph theory, integral distances and primitive permutation groups. Naturally, we begin with a formal definition of a graph. Thereafter, we define various concepts that pertain to our study. We also present definitions and basic properties of integral distances in two dimensions and extend the exploration to $m > 2$. Finally, we present some definitions and results related to finite primitive permutation groups to be used in Chapter 5.

2.1 Graphs, Cayley graphs, automorphisms of a graph and Boolean algebra of sets

Definition 2.1 A graph is a pair of sets $\Gamma = (V, E)$ such that $E \subset \mathcal{P}_2(V)$, where $\mathcal{P}_2(V)$ is the set of all subsets of V with two elements. The elements of V are the *vertices* of the graph Γ and the elements of E are its edges.

Elsewhere, a graph $\Gamma = (V, E)$ is a set of V vertices together with a binary relation E, which is irreflexive and symmetric. There is a one-to-one correspondence between irreflexive and symmetric relation on a set V and $\mathcal{P}_2(V)$. We use these definitions interchangeably.

The vertex set of a graph Γ is denoted by $V(\Gamma)$ and its edge set by $E(\Gamma)$, whenever there is a possibility of ambiguity.

Let $\Gamma = (V, E)$ be a finite graph. The *complement* of Γ is a graph Γ^C with $V(\Gamma^C) =$

$V(\Gamma)$ and $E(\Gamma^C) = \mathcal{P}_2(V) \backslash E(\Gamma)$. That is, $\{x, y\} \in E(\Gamma^C)$ if and only if $\{x, y\} \notin E(\Gamma)$.

The *order* of a graph Γ is the number of its vertices and is denoted by $|\Gamma|$. If $|\Gamma|$ is finite, then it is said that the graph is *finite*; otherwise, the graph is *infinite*. If $|\Gamma| = 0$, then Γ is called the *empty graph*.

Two vertices x, y of Γ are *adjacent* or *neighbors* if $\{x, y\}$ is an edge in Γ. The set of all neighbors of x is denoted by $N(x)$. Similarly two edges $e = \{x, y\}$ and $e' = \{x', y'\}$ are *adjacent* or *incident* if they have a vertex in common; i.e., $\{x, y\} \cap \{x', y'\} \neq \varnothing$.

If in $\Gamma = (V, E)$, the symmetry of the binary relation is not insisted upon, then we speak of a *directed graph* or *digraph*. In this case, the adjacency is represented by the pairs of the form (u, v) joining u to v. Those pairs are called *arcs*. In the latter, the vertex u is called the *tail* and the vertex v is called the *head*.

The order of the set $N(x)$ is called the *degree* of x and is denoted by $\deg(x)$. It is said that a vertex is *isolated* if $\deg(x) = 0$. A graph Γ is called *k-regular* if all the vertices of Γ have degree k. If $|V(\Gamma)| = n$ and Γ is an $(n-1)$-regular graph, then Γ is called a *complete graph*. The complete graph on n vertices is denoted by K_n.

Theorem 2.1 [2,5] *Let $\Gamma = (V, E)$ be a graph. Then*

$$2|E(\Gamma)| = \sum_{x \in V(\Gamma)} \deg(x).$$

Theorem 2.1 is referred to as the *handshaking lemma*. As can be seen, it states that the sum of degrees of vertices of each graph is twice the number of edges. It is easy to see that, in a k-regular graph Γ, we have $2|E(\Gamma)| = k|V(\Gamma)|$. This means that k or $|V(\Gamma)|$ is even.

We now define various types of sequences of vertices that are used in exploring connectivity in graphs.

Definition 2.2 Let $\Gamma = (V, E)$ be a graph.

(a) A *walk* is a sequence of vertices $v_0, v_1, \cdots, v_k$ such that $\{v_i, v_{i+1}\}$ is an edge for every $i \in \{0, 1, \cdots, k-1\}$; and k is called the *length of the walk*.

(b) A *trail* is a walk in which every edge is distinct.

(c) A *path* is a trail in which every vertex in $\{v_0, v_1, \cdots, v_{k-1}\}$ is distinct.

(d) A *cycle* is a path in which $v_k = v_0$. An *n-cycle* is a cycle with n vertices.

Let $\Gamma = (V, E)$ be a graph. Define a relation $\sim$ on V by $x \sim y$ if and only if there exists a path from x to y. If $x \sim y$, then x and y are said to be *connected*. It is not hard to see that $\sim$ is an equivalence relation. Each equivalence class $[x]$ is called a *component* of the graph. If a graph has more than one component, then it is *disconnected*; otherwise, it is *connected*.

A class of graphs which is at the core of our thesis display a certain kind of symmetry. We now define it.

Definition 2.3 Let Γ be a k-regular graph with $|\Gamma| = n$. If there exists two non-negative integers λ, μ such that every two adjacent vertices have λ common neighbors, and every two non-adjacent vertices have μ common neighbors; then Γ is called a *strongly regular graph* with parameters (n, k, λ, μ). Γ is denoted by $\mathrm{srg}(n, k, \lambda, \mu)$.

Amongst others, the parameters of strongly regular graphs satisfy the following equality whose proof is in [2, Theorem 11.10.3].

Proposition 2.2 [2] *Let Γ be a $\mathrm{srg}(n, k, \lambda, \mu)$. Then*

$$\mu(n - k - 1) = k(k - \lambda - 1).$$

It is obvious to see that the complement of a strongly regular graph is strongly regular, and to figure out the relationship between their parameters. The latter relationship is given in the following result with a proof in [2, Theorem 11.10.4].

Theorem 2.3 [2, 4, 16] *The complement Γ^C of a strongly regular graph Γ with parameters (v, k, λ, μ) is strongly regular with parameters $(v', k', \lambda', \mu') = (v, v - k - 1, v - 2 - 2k + \mu, v - 2k + \lambda)$.*

Graph homomorphisms are maps between graphs that respect the essence of relational structures. We now present the concepts.

Definition 2.4 Let Γ and Λ be graphs. Let $\phi : V(\Gamma) \longrightarrow V(\Lambda)$ be a mapping.

(a) If $\{x, y\} \in E(\Gamma)$ implies $\{x^\phi, y^\phi\} \in E(\Lambda)$, then ϕ is called a *homomorphism*.

(b) If ϕ is a bijective homomorphism and ϕ^{-1} is an homomorphism, then ϕ is called an *isomorphism*. In this case, Γ and Λ are said to be isomorphic and denoted by $\Gamma \cong \Lambda$.

(c) A graph Γ is *self-complementary* if it is isomorphic to its complement.

(d) If ϕ is an isomorphism from a graph to itself, then ϕ is called an *automorphism*.

The automorphisms of a graph Γ form a group under composition. The automorphism group is denoted by Aut Γ.

As alluded to, in this thesis we shall consider the automorphism groups of graphs of integral distance. Since the automorphisms form a group, we consider the action of this group on the set of vertices or edges. For any vertex $x \in V$ and automorphism $\gamma \in$ Aut Γ, we define the action of γ on x as x^γ. Similarly, for an edge $\{x, y\} \in E$, we define the action of γ on $\{x, y\}$ as $(\{x, y\})^\gamma = \{x^\gamma, y^\gamma\}$. If for any two vertices $x, y \in V$ there exists an automorphism $\gamma \in$ Aut Γ such that $x^\gamma = y$, then the group Aut Γ is said to *act transitively* on V. Edge-transitivity is similarly defined. Formally, we have the following.

Definition 2.5 Let $\Gamma = (V, E)$ be a graph.

(a) If Aut Γ acts transitively on $V(\Gamma)$, then Γ is said to be *vertex-transitive*.

(b) If Aut Γ acts transitively on $E(\Gamma)$, then Γ is said to be *edge-transitive*.

(c) Let H be a subgroup of Aut Γ which acts transitively on $V(\Gamma)$. If H has the same order as $V(\Gamma)$, then H is said to act *regularly* on $V(\Gamma)$.

It is to be noted that, if a graph is vertex-transitive, then every vertex has the same degree. Further, every vertex is contained in the same amount of cycles of each size. For these reasons, vertex-transitivity is a measure of symmetry of graphs.

Graphs have been defined on various algebraic structures [36]. Most commonly, graphs have been defined on groups. In doing so, the vertices of the graph are naturally defined as the elements of the group. In order to define the irreflexive and symmetric relation, subsets of the group elements are chosen in a certain way, satisfying certain conditions. These subsets are known as *Cayley sets* and defined as follows.

Definition 2.6 Let G be a group and 1_G be the identity element of G. Let $S \subset G$. If $1_G \notin S$ and $s^{-1} \in S$ whenever $s \in S$, then S is called a *Cayley set* on G.

Now let G be a group and S a Cayley set on G. We define a relation $\mathcal{E}$ on G by $(x, y) \in \mathcal{E}$ if and only if $y = xs$ where $s \in S$. Since $1_G \notin S$, it is impossible that $x = xs$ for some $s \in S$. Thus $(x, x) \notin \mathcal{E}$, and so $\mathcal{E}$ is irreflexive. In addition, we have $ys^{-1} = x$ so that $(y, x) \in \mathcal{E}$ since $s^{-1} \in S$. Hence $\mathcal{E}$ is symmetric. Therefore this brings us to the following definition of a Cayley graph.

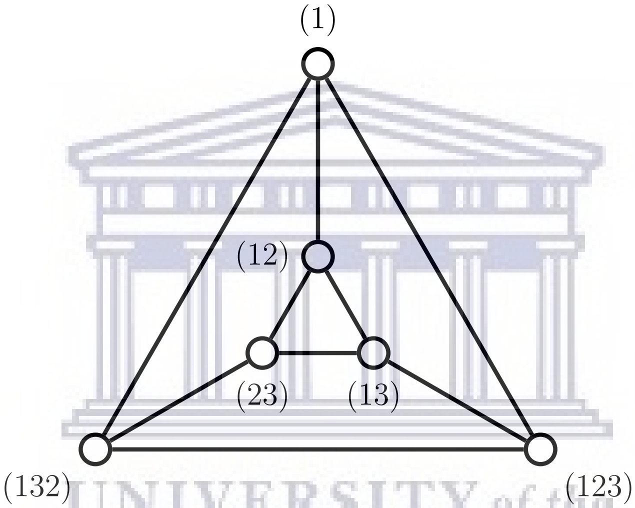
Definition 2.7 Let G be a group and S a Cayley set on G. By the *Cayley graph*

$\Gamma = \mathrm{Cay}(G, S)$, is meant the graph defined by

$$\begin{aligned} V(\Gamma) &:= G; \\ E(\Gamma) &:= \{\{x, xs\} : x \in G, s \in S\}. \end{aligned}$$

s^{-1} is understood as $-s$ in an additive group whenever it is applicable.

Example 1 Consider the symmetric group S_3. $U = \{(12), (123), (132)\}$ is clearly a Cayley set on S_3 since it is closed under inverses and does not contain the identity permutation. The Cayley graph $\mathrm{Cay}(S_3, U)$ is illustrated below.



It is easy to show that the edges correspond exactly to the set $E = \{\{x, xs\} : x \in S_3, s \in U\}$.

Example 2 Let $G = \mathbb{Z}_2^n$, n copies of $\mathbb{Z}_2$, and $S = \{\mathbf{e}_1, \mathbf{e}_2, \cdots, \mathbf{e}_n\}$, where $\mathbf{e}_i$ is the vector with 1 at the i^{th} position and zeros everywhere else. It is easy to see that S is a Cayley set in G. The graph $\mathrm{Cay}(G, S)$ is the classical hypercube.

Example 3 Let G be any group and $S = G \setminus \{1_G\}$. The complete graph K_n is the Cayley graph $\mathrm{Cay}(G, S)$.

It is a classical result that being a Cayley graph is preserved under complementation of sets. The latter is stated as follows.

Proposition 2.4 *Let G be a group and S a Cayley set. For the Cayley graph $\Gamma = \mathrm{Cay}(G, S)$, the complement Γ^C is Cayley.*

For the rest of this section, we present a theorem regarding vertex-transitivity of a Cayley graph, and a proposition regarding isomorphism of Cayley graphs. For completeness, we give proofs.

Theorem 2.5 [1, 16, 36] *Let G be a group and S a Cayley set of G. The Cayley graph $\Gamma = \mathrm{Cay}(G, S)$ is vertex-transitive.*

Proof. For a fixed $g \in G$, let $\lambda_g : V(\mathrm{Cay}(G, S)) \mapsto V(\mathrm{Cay}(G, S))$ be defined by

$$v \mapsto gv$$

for all $v \in V(\mathrm{Cay}(G, S))$. Clearly, λ_g permutes the elements of $V(\mathrm{Cay}(G, S))$. To show that $\lambda_g \in \mathrm{Aut}(\mathrm{Cay}(G, S))$, we must show that $\{v, u\} \in E(\mathrm{Cay}(G, S))$ if and only if $\{gv, gu\} \in E(\mathrm{Cay}(G, S))$.

Suppose that $\{v, u\} \in E(\mathrm{Cay}(G, S))$. Then we have that $v = us$ for some $s \in S$, or equivalently $u^{-1}v = s$. But $(gu)^{-1}gv = u^{-1}g^{-1}gv = u^{-1}v$. Therefore $\{v, u\} \in E(\mathrm{Cay}(G, S))$ if and only if $\{gv, gu\} \in E(\mathrm{Cay}(G, S))$, and λ_g is in $\mathrm{Aut}(\mathrm{Cay}(G, S))$.

Now given any vertices v, u in Cay(G, S), the mapping $\lambda_{v^{-1}u}$ maps v to u since $vv^{-1}u = u$. Thus any Cayley graph is vertex-transitive. □

Proposition 2.6 [16] *Let ϕ be an automorphism of the group G and let S be a Cayley set of G. Then* $\mathrm{Cay}(G, S) \cong \mathrm{Cay}(G, S^{\phi})$.

Proof. Given any two vertices $v, u \in V(\mathrm{Cay}(G, S))$, we have that v and u are adjacent if $u^{-1}v \in S$. Indeed,

$u^{-1}v \in S \Rightarrow (u^{-1}v)^{\phi} = (u^{-1})^{\phi}v^{\phi} = (u^{\phi})^{-1}v^{\phi} \in S^{\phi}$.

Thus v^{ϕ} and u^{ϕ} are adjacent if v and u are connected.

Conversely, assume that $v^{\phi}, u^{\phi} \in V(\mathrm{Cay}(G, S^{\phi})$ are adjacent for some $v, u \in V(\mathrm{Cay}(G, S))$. Then $(u^{\phi})^{-1}v^{\phi} \in S^{\phi}$. Indeed, $(u^{\phi})^{-1}v^{\phi} = (u^{-1}v)^{\phi} \in S^{\phi} \Rightarrow u^{-1}v \in S$ since ϕ is an automorphism of G. Thus v and u are adjacent if v^{ϕ} and u^{ϕ} are.

Therefore ϕ is an isomorphism from $\mathrm{Cay}(G, S)$ to $\mathrm{Cay}(G, S^{\phi})$. □

After we have defined all the pertinent concepts of graphs related to our work, we now turn to another object which shall be used in all the remaining chapters.

Definition 2.8 A *concrete Boolean algebra* or a *field of sets* is a collection $\mathfrak{B}$ of subsets of some set X which contains the empty set and is closed under the set theoretic operations of finite union, finite intersection, and taking complements. In other words,

(i) $A \in \mathfrak{B} \Rightarrow A^C \in \mathfrak{B}$ ($A^C = X \setminus A$);

(ii) $A, B \in \mathfrak{B} \Rightarrow A \cap B \in \mathfrak{B}$; and

(iii) $A, B \in \mathfrak{B} \Rightarrow A \cup B \in \mathfrak{B}$.

It follows easily that the concrete Boolean algebra is also closed under the operation of taking differences. The concrete Boolean algebra generated by a family $\mathcal{A}$ of subsets of X is defined as the smallest Boolean algebra $\mathfrak{B}$ of subsets of X containing $\mathcal{A}$.

Let G be a group, $X = G \setminus \{1_G\}$, and $\mathfrak{B} = \{S \subseteq X : S$ is a Cayley set$\}$. It has been shown in [36] that $\mathfrak{B}$ is a Boolean algebra in the following terms.

Theorem 2.7 [36] *Let G be any group and $X = G \setminus \{1_G\}$. Let S and S' be Cayley sets in G. Then the following are Cayley sets:*

(i) *$S \cap S'$;*

(ii) *$S \cup S'$; and,*

(iii) *$X \setminus S$.*

2.2 Basic definitions and properties of integral distances in $\mathbb{F}_q^2$

In this section, q will always be a power of a prime p. Unless otherwise noted, p will be assumed to be odd. $\mathbb{F}_q$ denotes the finite field of order q. The set of all perfect squares in $\mathbb{F}_q$ including the zero element will be denoted by $\square_q$. When we speak about points and lines in $\mathbb{F}_q^2$, we refer to the affine plane over $\mathbb{F}_q$. In the context of integral distance in $\mathbb{F}_q^2$, the metric used to define distance is the following.

Definition 2.9 The *norm* $N : \mathbb{F}_q^2 \longrightarrow \mathbb{F}_q$ of a point $\mathbf{x} = (x_1, x_2)$ is defined by $N(\mathbf{x}) = x_1^2 + x_2^2$. Two points $\mathbf{x}$ and $\mathbf{y}$ in $\mathbb{F}_q^2$ are said to be at *integral distance* if

$N(\mathbf{x}-\mathbf{y}) \in \square_q$. A point set $\mathcal{P}$ is called *integral* if all pairs of points are at integral distance. An integral point set $\mathcal{P}$ is called *maximal* if there is no integral point set in $\mathbb{F}_q^2$ containing $\mathcal{P}$ properly.

For two points $\mathbf{x}$ and $\mathbf{y}$, $N(\mathbf{x}-\mathbf{y})$ can be interpreted as the squared Euclidean distance between $\mathbf{x}$ and $\mathbf{y}$. If q is the power of even p, then, for the sake of completeness, we give our own proof that the matter is trivial when $q \equiv 0 \pmod 2$.

Theorem 2.8 [21] *Let $\mathbb{F}_{2^n}$ be a finite field. Then $\square_{2^n} = \mathbb{F}_{2^n}$.*

Proof. We have to show that every element of $\mathbb{F}_{2^n}$ is a square root of some element of $\mathbb{F}_{2^n}$.

We need to show that, given $x \in \mathbb{F}_{2^n}$, there exists $a \in \mathbb{F}_{2^n}$ such that $x = a^2$.

If $x = 0$ or $x = 1$, the case is trivial.

Let β be the multiplicative generator of $\mathbb{F}_{2^n}^*$.

If $x = \beta^i$, we have the following cases.

Case 1: i is even; i.e., $i = 2k$ with $k \in \mathbb{N}$.

Consider $a = \beta^k$. Then $a^2 = \beta^{2k} = x$.

Case 2: i is odd; i.e., $i = 2k+1$ with $k \in \mathbb{N}$.

We have $x = \beta^{2k+1}$. Multiplying both sides by β^{2^n-1}, we get

$$\begin{aligned} x\beta^{2^n-1} = \beta^{2k+1}\beta^{2^n-1} &\Rightarrow x = \beta^{2k+1+2^n-1}; \\ &\Leftrightarrow x = \beta^{2k+2^n}; \\ &\Leftrightarrow x = \beta^{2(k+2^{n-1})}. \end{aligned}$$

Consider $a = \beta^{k+2^{n-1}}$.

Then $a^2 = \beta^{2(k+2^{n-1})} = x$.

Therefore the result follows. □

The above case shows that, if q is even, then every point set $\mathcal{P} \subseteq \mathbb{F}_q^2$ is integral. Hence the only maximal integral point set is $\mathbb{F}_q^2$. For this reason, as alluded to, we only pay attention to the case when $q \equiv 1 \pmod 2$.

In counting arguments, we constantly use the number of elements which are perfect squares in $\mathbb{F}_q^*$ for which we present below.

Theorem 2.9 [21] *Let $\mathbb{F}_q$ be a finite field of order q with q odd. Then $|\Box_q| = \dfrac{q+1}{2}$.*

Proof. For $\Box_q^* = \Box_q \setminus \{0\}$, we first have to show that $\Box_q^*$ is a subgroup of $\mathbb{F}_q^*$, and that $\dfrac{|\mathbb{F}_q^*|}{|\Box_q^*|} = 2$.

Now $1 \in \Box_q^*$ since $1^2 = 1$.

Secondly, let $x, y \in \Box_q^*$; i.e., there exists $a, b \in \mathbb{F}_q^*$ such that $x = a^2$ and $y = b^2$.

Then $xy^{-1} = a^2(b^2)^{-1} = a^2(b^{-1})^2 = a \cdot a \cdot b^{-1} \cdot b^{-1} = ab^{-1} \cdot ab^{-1} = (ab^{-1})^2 \in \Box_q^*$.

Therefore $\Box_q^*$ is a subgroup of $\mathbb{F}_q^*$.

It is a classical result that the multiplicative group $\mathbb{F}_q^*$ is a cyclic group [33, Theorem 2.8]. Hence, by the Fundamental Theorem of Cyclic Groups, all its subgroups are cyclic.

Let a be a multiplicative generator of $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$.

Since $|\mathbb{F}_q^*| = q - 1$, it follows that $\mathbb{F}_q^* = \{1, a, a^2, \cdots, a^{q-2}\}$ because $a^{q-1} = 1$ (q odd).

Consequently, as $\Box_q^*$ is the set of all squared elements of $\mathbb{F}_q^*$, then a^2 is the generator of $\Box_q^*$; i.e., $\Box_q^* = \{1, a^2, a^4, \cdots\}$. By the Fundamental Theorem of Cyclic Groups, $\dfrac{|\mathbb{F}_q^*|}{|\Box_q^*|} = 2$.

Therefore

$$\begin{aligned}\Box_q^* = \Box_q \setminus \{0\} &\Rightarrow \Box_q = \Box_q^* \cup \{0\} \\ &\Rightarrow |\Box_q| = |\Box_q^* \cup \{0\}| = \frac{q-1}{2} + 1 = \frac{q+1}{2}.\end{aligned}$$

□

We now present sets of directions of lines in $\mathbb{F}_q^2$. This will help us understand maximal integral point sets in $\mathbb{F}_q^2$.

For a line $\mathbf{L} = \mathbf{P} + \mathbb{F}_q \cdot \mathbf{Q}$ with $\{\mathbf{P}, \mathbf{Q}\} \subseteq \mathbb{F}_q^2$, $\mathbf{Q} \neq (0,0)$, $\mathbf{D} = \mathbb{F}_q \cdot \mathbf{Q}$ is called the *direction* of $\mathbf{L}$. If $N(\mathbf{Q}) \in \Box_q$, then $\mathbf{D}$ is an *integral direction.* If $N(\mathbf{Q}) = 0$, then D is a *vanishing direction.* Notice that the set of integral directions is completely determined if two arbitrary points $\mathbf{x}$ and $\mathbf{y}$ in it are at integral distance.

For a point set $\mathcal{P} \subseteq \mathbb{F}_q^2$, a direction $\mathbf{D}$ is called a direction determined by $\mathcal{P}$ if $\mathbf{D} = \mathbb{F}_q \cdot (\mathbf{P} - \mathbf{Q})$ with $\{\mathbf{P}, \mathbf{Q}\} \subseteq \mathcal{P}$. For the sake of completeness, we give our own proof of the following statement in order to determine the slopes of such directions.

Lemma 2.10 [21] *The slopes of direction determined by $\mathcal{P} \subseteq \mathbb{F}_q^2$ are elements of $\mathbb{F}_q \cup \{\infty\}$.*

Proof. Consider the direction $\mathbf{D} = \mathbb{F}_q(x, y)$ with $x, y \in \mathbb{F}_q$. $\mathbf{D}$ has slope $\dfrac{y}{x} = yx^{-1} \in \mathbb{F}_q$ provided that $x \neq 0$. If $x = 0$, the direction $\mathbf{D}$ is of slope ∞.

Now we have a bijection between the slopes and $\mathbb{F}_q \cup \{\infty\}$. Consider the directions $\mathbf{D} = \mathbb{F}_q(x, y)$ and $\mathbf{D}' = \mathbb{F}_q(x', y')$. The slope of $\mathbb{F}_q(x, y)$ is the slope of $\mathbb{F}_q(1, yx^{-1})$, and the slope of $\mathbb{F}_q(x', y')$ is the slope of $\mathbb{F}_q(1, x'y'^{-1})$.

It is enough to consider the slope z of $\mathbf{D}$ and the slope z' of $\mathbf{D}'$. If $\mathbb{F}_q(1, z) \neq \mathbb{F}_q(1, z')$, then $z \neq z'$, and therefore there is a bijection between the slopes and $\mathbb{F}_q \cup \{\infty\}$. □

There is a critical difference between fields $\mathbb{F}_q$ with $q \equiv 1 \pmod 4$ to those with $q \equiv 3 \pmod 4$. The following important result is used to discuss the pertinent matter that ensues from this fact. For completeness, we give our own proof for it.

Theorem 2.11 [29,32] *For a finite field $\mathbb{F}_q$ with $q = p^r, p \neq 2$, $-1 \in \square_q$ if and only if $q \equiv 1 \pmod 4$.*

Proof. We have $q \equiv 1 \pmod 4$; i.e., $4 \mid q - 1$. Let g be a generator of the group $\mathbb{F}_q^*$. Then $q - 1$ is the least positive integer such that $g^{q-1} = 1$. We can rewrite this as $g^{q-1} - 1 = (g^{\frac{q-1}{2}} - 1)(g^{\frac{q-1}{2}} + 1) = 0$. Since $g^{\frac{q-1}{2}}$ cannot be equal to 1, it follows that $g^{\frac{q-1}{2}} = (g^{\frac{q-1}{4}})^2 = -1$. This means that $g^{\frac{q-1}{4}}$ is a square root of -1. □

Corollary 2.12 *For $q \equiv 3 \pmod 4$, $-1 \notin \square_q$.*

Corollary 2.13 *For $q \equiv 3 \pmod 4$, $x^2 + 1$ is irreducible.*

The set $\mathbb{F}_q^2$ can be considered as $\mathbb{F}_q[i]$, where i is a root of the polynomial $x^2+1 \in \mathbb{F}_q[x]$. $\mathbb{F}_q[i]$ is considered as a ring since $\mathbb{F}_q[i] \cong \mathbb{F}_q[x]/\langle x^2 + 1\rangle$, and $x^2 + 1$ is reducible for $q \equiv 1 \pmod 4$. The following results, in which we prove for the sake of completeness, are very important for $\mathbb{F}_q[i]$.

We can identify $[(\mathbb{F}_q[i], \cdot)]$ as a monoid under multiplication.

Theorem 2.14 [21] *The norm $N : \mathbb{F}_q[i] \longrightarrow \mathbb{F}_q$ is a monoidal homomorphism*

$$N : (\mathbb{F}_q[i], \cdot) \longrightarrow (\mathbb{F}_q, \cdot).$$

Proof. Let $z = a + bi$ and $z' = c + di$. Then

$$\begin{aligned}
N(zz') &= N[(a+bi)(c+di)] \\
&= N(ac + adi + bci + bdi^2) \\
&= N[ac - bd + (ad + bc)i] = (ac - bd)^2 + (ad + bc)^2 \\
&= a^2c^2 - 2acbd + b^2d^2 + a^2d^2 + 2adbc + b^2c^2 \\
&= a^2(c^2 + d^2) + b^2(d^2 + c^2) \\
&= (a^2 + b^2)(c^2 + d^2) \\
&= N(z)N(z').
\end{aligned}$$

Thus N is a monoidal homomorphism. □

When $q \equiv 3 \pmod 4$, the norm takes a simpler form in the following corollary with a similar proof as that given in [26].

Corollary 2.15 [26] *Let $q \equiv 3 \pmod 4$. Then $N : \mathbb{F}_q[i] \longrightarrow \mathbb{F}_q$ is exactly the map $x \longmapsto x^{q+1}$ so that $N(x - y) = (x - y)^{q+1}$ for all x, y.*

In addition, we give our own proof of the following corollary for completeness.

Corollary 2.16 [21] *An element $z = x + yi \in \mathbb{F}_q[i]$ with $x, y \in \mathbb{F}_q$ is a zero-divisor if and only if $N(z) = 0$.*

Proof. Let $z = x + yi \in \mathbb{F}_q[i]$, $z \neq 0$. Then z is a zero-divisor of $\mathbb{F}_q[i]$ if there exists $z' = x' + y'i \in \mathbb{F}_q[i]$, $z' \neq 0$, such that $zz' = 0$. Then we have

$$\begin{aligned}
N(zz') = 0 &\Rightarrow N(z)N(z') = 0 \\
&\Rightarrow N(z) = 0 \text{ or } N(z') = 0.
\end{aligned}$$

Therefore z and z' are zero-divisors.

Conversely, if $N(z) = 0$, then $N(z)$ can be expressed as $N(z) = z\bar{z}$ with $z = x + yi$ and $\bar{z} = x - yi$; i.e., $z \neq 0$ and $\bar{z} \neq 0$. It follows that z is a zero-divisor. □

If $q \equiv 3 \pmod 4$, $\mathbb{F}_{q^2}$ can be identified with $\mathbb{F}_q[i]$, which is a field.

Corollary 2.17 [21] *If $q \equiv 3 \pmod 4$, then there is no vanishing direction.*

Denote by ω an element of $\mathbb{F}_q$, $q \equiv 1 \pmod 4$, with $\omega^2 = -1$. For completeness, we now analyse ideals in $\mathbb{F}_q[i]$ in the following result with our own proof.

Lemma 2.18 [21] *$\mathbb{F}_q[i]$ is a finite ring with two non trivial ideals $I_1 = \mathbb{F}_q(\omega + i)$ and $I_2 = \mathbb{F}_q(\omega - i)$ if $q \equiv 1 \pmod 4$.*

Proof. Since $-1 \in \square_q$ for $q \equiv 1 \pmod 4$, it follows that

$\omega^2+1 = \omega^2 - i^2 = (\omega - i)(\omega + i)$, and that $\mathbb{F}_q[i]/\langle\omega^2+1\rangle$ admits two non-trivial ideals $\mathbb{F}_q[i]/\langle\omega + i\rangle$ and $\mathbb{F}_q[i]/\langle\omega - i\rangle$. The latter are of the form $\mathbb{F}_q(\omega + i)$ and $\mathbb{F}_q(\omega - i)$. Hence we are done. □

It was observed that there is no vanishing direction in $\mathbb{F}_q[i]$ whenever $q \equiv 3 \pmod 4$ [21]. In the case of $q \equiv 1 \pmod 4$, we have precisely two ideals, and consequently, we get the following with our own proof for completeness.

Proposition 2.19 [21] *$\mathbb{F}_q(\omega + i)$ and $\mathbb{F}_q(\omega - i)$ are exactly vanishing directions and consist of zero-divisors of $\mathbb{F}_q[i]$.*

Proof. Let $P = \alpha(\omega + i)$ and $Q = \beta(\omega - i)$. Then

$$\begin{aligned} N(P) &= N(\alpha(\omega + i)) = N(\alpha\omega + \alpha i) = (\alpha\omega + \alpha i)(\alpha\omega - \alpha i) = \alpha^2\omega^2 - \alpha^2 i^2 \\ &= \alpha^2(\omega^2 + 1) = \alpha^2 \cdot 0. \end{aligned}$$

Thus $N(P) = 0$. By similar argument, we get $N(Q) = 0$.

Therefore P and Q are zero-divisors of $\mathbb{F}_q[i]$. □

Like in complex numbers, for $z = x + yi \in \mathbb{F}_q[i]$ with $\{x, y\} \subseteq \mathbb{F}_q$, we use the notation $\bar{z} = x - yi$. In this case, we get $N(z) = z\bar{z}$.

The following parametric representation of pairs of $\mathbb{F}_q^2$ is very important. It will be a very useful result in most counting arguments in Chapter 4 and Chapter 5.

Theorem 2.20 [21, 32] *Let $c \in \mathbb{F}_q$ and denote $P_c = \{(a, b) \in \mathbb{F}_q^2 : a^2 + b^2 = c^2\}$ for $c \neq 0$. Then*

$$P_0 = \begin{cases} \{(t, \pm t\omega) : t \in \mathbb{F}_q\} & \textit{if } q \equiv 1 \pmod 4, \\ \{(0, 0)\} & \textit{if } q \equiv 3 \pmod 4; \end{cases}$$

and $P_c = \{(\pm c, 0)\} \cup \{(0, \pm c)\} \cup \left\{ \left(\frac{t^2-1}{t^2+1} \cdot c, \frac{2t}{t^2+1} \cdot c, c \right) : t \in \mathbb{F}_q^*, t^2 \neq \pm 1 \right\}.$

Moreover

$$|P_0| = \begin{cases} 2q-1 & \textit{if } q \equiv 1 \pmod 4, \\ 1 & \textit{if } q \equiv 3 \pmod 4; \end{cases} \quad \textit{and } |P_c| = \begin{cases} q-1 & \textit{if } q \equiv 1 \pmod 4, \\ q+1 & \textit{if } q \equiv 3 \pmod 4. \end{cases}$$

This leads to the following corollary with a proof given in [32, Corollary 3.7]

Corollary 2.21 [32] *If* $I_\gamma = \{(\alpha, \beta) \in \mathbb{F}_q^2 : \alpha^2 + \beta^2 = \gamma\}$*, then*

$$|I_0| = \begin{cases} 2q-1 & \textit{if } q \equiv 1 \pmod 4, \\ 1 & \textit{if } q \equiv 3 \pmod 4, \end{cases} \quad \textit{and } |I_\gamma| = \begin{cases} q-1 & \textit{if } q \equiv 1 \pmod 4, \\ q+1 & \textit{if } q \equiv 3 \pmod 4 \end{cases}$$

for $\gamma \neq 0$.

Definition 2.10 By the unit circle in $\mathbb{F}_q^2$, is meant the set

$$\mathcal{C}_q = N^{-1}(1).$$

In the following lemma whose proof is given in [29, Lemma 9], we present an indication that $\mathcal{C}_q$ shares some important properties with the unit circle in the Euclidean plane $\mathbb{R}^2$.

Lemma 2.22 [29] *The unit circle* $\mathcal{C}_q$ *considered as a subset of* $\mathbb{F}_q[i]$ *is a cyclic subgroup of* $\mathbb{F}_q[i]^*$. *The order of* $\mathcal{C}_q$ *is given by*

$$|\mathcal{C}_q| = \begin{cases} q-1 & \textit{if } q \equiv 1 \pmod 4, \\ q+1 & \textit{if } q \equiv 3 \pmod 4. \end{cases}$$

For $q \equiv 1 \pmod 4$, the points $\mathbf{P} \in \mathbb{F}_q^2$ can be represented in another basis of $\mathbb{F}_q^2$ that yields a simple representation of the norm and the vanishing lines. Those points are said to be given in *hyperbolic coordinates*. In this representation, the coordinates (α, β) in which the norm of $\mathbf{P}$ in that new basis is $N(\mathbf{P}) = \alpha\beta$ with vanishing directions $(\mathbb{F}_q, 0)$ and $(0, \mathbb{F}_q)$. (See further details in [21] and Lemma 3.9).

2.3 Basic definitions and properties of Integral distances in $\mathbb{F}_q^m$ $(m > 2)$

At the core of our discussion, we look at integral distances in affine spaces $\mathbb{F}_q^m$. We now present and prove some of their elementary properties to be used in Chapter 4.

Let $\mathbb{F}_q$ be a finite field with $q = p^r$ and consider the m-dimensional affine spaces $\mathbb{F}_q^m$. These spaces are equipped with the natural metric which generalizes the Euclidean.

Definition 2.11 For two points $\mathbf{u} = (u_1, \cdots, u_m)$, $\mathbf{v} = (v_1, \cdots, v_m)$ in $\mathbb{F}_q^m$; the *squared distance* is defined as

$$d^2(\mathbf{u}, \mathbf{v}) = N(\mathbf{u} - \mathbf{v}) = \langle \mathbf{u} - \mathbf{v}, \mathbf{u} - \mathbf{v} \rangle = (\mathbf{u} - \mathbf{v})^T (\mathbf{u} - \mathbf{v}) = \sum_{i=1}^{m} (u_i - v_i)^2 \in \mathbb{F}_q,$$

where $\langle \mathbf{u}, \mathbf{v} \rangle = \mathbf{u}^T \mathbf{v} = \sum_{i=1}^{m} u_i v_i$ is a bilinear form over $\mathbb{F}_q^m$.

The cases where $d^2(\mathbf{u}, \mathbf{v})$ is contained in the set $\square_q$ of squares in $\mathbb{F}_q$ are of the greatest interest in what follows.

Definition 2.12 Two points $\mathbf{u} = (u_1, \cdots, u_m)$, $\mathbf{v} = (v_1, \cdots, v_m)$ in $\mathbb{F}_q^m$ are at *integral distance* if $d^2(\mathbf{u}, \mathbf{v})$ is contained in the set $\square_q = \{\alpha^2 : \alpha \in \mathbb{F}_q\}$ consisting of the squares in $\mathbb{F}_q$. A set $\mathbb{P}$ of points in $\mathbb{F}_q^m$ is called an *integral point set* if all pairs of points are at integral distance; i.e., if $d^2(\mathbf{u}, \mathbf{v}) \in \square_q$ for all $\mathbf{u}, \mathbf{v} \in \mathbb{P}$.

As a shorthand, a map $\Delta : \mathbb{F}_q^m \times \mathbb{F}_q^m \longrightarrow \{0, 1\}$ is defined by

$$\Delta(\mathbf{u}, \mathbf{v}) \longmapsto \begin{cases} 1 & \text{if } \mathbf{u} \text{ and } \mathbf{v} \text{ are at integral distance} \\ 0 & \text{otherwise} \end{cases}$$

As a generalization in m-dimension, similarly to the case of $m = 2$, we need to define these important sets. Again, they are used for counting arguments.

Consider the sets

$$\mathbb{P}_0 = \left\{ \mathbf{u} \in \mathbb{F}_q^m : \sum_{i=1}^{m} u_i^2 = 0 \right\};$$

$$\mathbb{P}^{+} = \left\{ \mathbf{u} \in \mathbb{F}_q^m : \sum_{i=1}^{m} u_i^2 \in \square_q^* \right\};$$

$$\text{and } \mathbb{P}^{-} = \left\{ \mathbf{u} \in \mathbb{F}_q^m : \sum_{i=1}^{m} u_i^2 \notin \square_q \right\}.$$

The following three functions are in consideration.

$\mathcal{S}(m,q) = |\mathbb{P}^{+}|$; $\mathcal{Z}(m,q) = |\mathbb{P}_0|$; and $\mathcal{N}(m,q) = |\mathbb{P}^{-}|$.

The first three functions are given by

$$\mathcal{S}(1,q) = q-1;\ \mathcal{Z}(1,q) = 1;\ \mathcal{N}(1,q) = 0;$$

$$\mathcal{S}(2,q) = \begin{cases} \dfrac{(q-1)^2}{2} & \text{if } q \equiv 1 \pmod 4; \\ \dfrac{q^2-1}{2} & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

$$\mathcal{Z}(2,q) = \begin{cases} 2q-1 & \text{if } q \equiv 1 \pmod 4; \\ 1 & \text{if } q \equiv 3 \pmod 4, \end{cases}$$

and

$$\mathcal{N}(2,q) = \begin{cases} \dfrac{(q-1)^2}{2} & \text{if } q \equiv 1 \pmod 4; \\ \dfrac{q^2-1}{2} & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

For the sake of completeness, we give our own proof of the following equations that determine the relationship between the above three parameters.

Lemma 2.23 [32] *Let* $I_\gamma = \{(a,b) \in \mathbb{F}_q^2 : a^2 + b^2 = \gamma, \gamma \in \mathbb{F}_q\}$ *as defined in* Corollary 2.21. *Then for dimension* $m \geq 3$*, we have*

$\mathcal{Z}(m,q) = \mathcal{Z}(m-2,q)|I_0| + (q^{m-2} - \mathcal{Z}(m-2,q))|I_1|$;

$$\begin{aligned} \mathcal{S}(m,q) = {} & \left(\frac{q-1}{2}\right)(\mathcal{N}(m-2,q) + \mathcal{Z}(m-2,q))|I_1| + \left(\frac{q-3}{2}\right)\mathcal{S}(m-2,q)|I_1| \\ & + \mathcal{S}(m-2,q)|I_0|; \text{ and} \end{aligned}$$

$\mathcal{N}(m,q) = q^m - \mathcal{S}(m,q) - \mathcal{Z}(m,q)$.

Proof. We prove the two first equations:

We rewrite the equation $\sum\limits_{i=1}^{m} u_i^2 = \tau$ as $u_1^2 + u_2^2 = \tau - \sum\limits_{i=3}^{m} u_i^2$.

For $\mathcal{Z}(m, q)$, we have $\sum\limits_{i=1}^{m} u_i^2 = 0$, which gives $\tau = 0$ and $u_1^2 + u_2^2 = -\sum\limits_{i=3}^{m} u_i^2$.

$I_0 = \{(u_1, u_2) : u_1^2 + u_2^2 = 0\}$; i.e., $u_1^2 + u_2^2 = 0$ and so $\sum\limits_{i=3}^{m} u_i^2 = 0$.

We obtain $\mathcal{Z}(m-2, q)|I_0|$ elements.

$I_1 = \{(u_1, u_2) : u_1^2 + u_2^2 = 1\}$: $u_1^2 + u_2^2 = -\sum\limits_{i=3}^{m} u_i^2$.

Let

$$\sum_{i=3}^{m} u_i^2 = \kappa, \quad \kappa \neq 0. \tag{2.1}$$

We have $u_1^2 + u_2^2 = -\kappa$, $\kappa \in \mathbb{F}_q^*$.

By definition of I_γ, we have $q^{m-2} - \mathcal{Z}(m-2, q)$ elements for Equation (2.1) and thus $(q^{m-2} - \mathcal{Z}(m-2, q))|I_1|$ elements.

Therefore $\mathcal{Z}(m, q) = \mathcal{Z}(m-2, q)|I_0| + (q^{m-2} - \mathcal{Z}(m-2, q))|I_1|$.

For $\mathcal{S}(m, q)$, we must have $\tau \in \square_q^*$.

If $u_1^2 + u_2^2 = 0$, we have $\tau = \sum\limits_{i=3}^{m} u_i^2 = \kappa \in \square_q^*$ and we get $\mathcal{S}(m-2, q)|I_0|$.

If $u_1^2 + u_2^2 \neq 0$, we have $u_1^2 + u_2^2 = \tau - \kappa$.

Let $\tau = \nu^2$; i.e., $u_1^2 + u_2^2 = \nu^2 - \kappa$, $\nu^2 \neq \kappa$, and $\nu^2 \neq 0$. So we have different cases.

First, $\kappa = 0$: $u_1^2 + u_2^2 = \nu^2$. This yields to $\left(\dfrac{q-1}{2}\right) \mathcal{Z}(m-2, q)|I_1|$.

Second, $\kappa \neq 0$: $u_1^2 + u_2^2 = \nu^2 - \kappa$. This yields to two cases: $\kappa \in \square_q^*$ and $\kappa \notin \square_q$.

(a) $\kappa \in \square_q^*$: Let $\kappa = \xi^2$ and consider $\nu^2 - \xi^2 = u_1^2 + u_2^2$, $\xi^2 \neq \nu^2$, $\xi^2 \neq 0$. Here we have $\left(\dfrac{q-1}{2} - 1\right) \mathcal{S}(m-2, q)|I_1| = \left(\dfrac{q-3}{2}\right) \mathcal{S}(m-2, q)|I_1|$ solutions.

(b) $\kappa \notin \square_q$: We have the remaining $\dfrac{q-1}{2}$ non-squares for κ yielding to

$\left(\dfrac{q-1}{2}\right)\mathcal{N}(m-2,q)|I_1|$ solutions.

Summing all up, we obtain

$$\mathcal{S}(m,q) = \left(\frac{q-1}{2}\right)(\mathcal{N}(m-2,q)+\mathcal{Z}(m-2,q))|I_1| + \left(\frac{q-3}{2}\right)\mathcal{S}(m-2,q)|I_1| \\ + \mathcal{S}(m-2,q)|I_0|.$$

Therefore $\mathcal{N}(m,q)$ easily follow. □

To facilitate our discussion, we now give our own evaluation of $\mathcal{Z}(m,q)$, $\mathcal{S}(m,q)$, and $\mathcal{N}(m,q)$; with $m \geq 1$ in the following by induction.

Theorem 2.24 [32] *Let $m \geq 1$ be arbitrary.*

For $q \equiv 1 \pmod 4$, we have

$$\mathcal{Z}(m,q) = \begin{cases} q^{m-1} & \text{for } m \text{ odd;} \\ q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}} & \text{for } m \text{ even,} \end{cases}$$

$$\mathcal{S}(m,q) = \begin{cases} \frac{1}{2}\left(q^m - q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right) & \text{for } m \text{ odd;} \\ \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right) & \text{for } m \text{ even,} \end{cases}$$

$$\mathcal{N}(m,q) = \begin{cases} \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m+1}{2}} + q^{\frac{m-1}{2}}\right) & \text{for } m \text{ odd;} \\ \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right) & \text{for } m \text{ even.} \end{cases}$$

For $q \equiv 3 \pmod 4$, we have

$$\mathcal{Z}(m,q) = \begin{cases} q^{m-1} & \text{for } m \text{ odd;} \\ q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}} & \text{for } m \text{ even,} \end{cases}$$

$$\mathcal{S}(m,q) = \begin{cases} \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}}\right) & \text{for } m \text{ odd;} \\ \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right) & \text{for } m \text{ even,} \end{cases}$$

$$\mathcal{N}(m,q) = \begin{cases} \frac{1}{2}\left(q^m - q^{m-1} + (-q)^{\frac{m+1}{2}} + (-q)^{\frac{m-1}{2}}\right) & \text{for } m \text{ odd;} \\ \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right) & \text{for } m \text{ even.} \end{cases}$$

Proof. For $\mathcal{Z}(m,q)$ and $\mathcal{S}(m,q)$, we prove by induction on m and we use Lemma 2.23.

To calculate $\mathcal{Z}(m,q)$, we have the following.

(a) m odd:

(i) $q \equiv 1 \pmod 4$: $|I_0| = 2q-1$ and $|I_1| = q-1$.

Base: $m=1$: $\mathcal{Z}(1,q) = 1$.

Assume that the result holds when $m = 2k-1$.

Hence we have $\mathcal{Z}(2k-1,q) = q^{2k-2}$.

Let us show that it is true for $m = 2k+1$.

We have

$$\begin{aligned}\mathcal{Z}(2k+1,q) &= \mathcal{Z}(2k-1,q)|I_0| + (q^{2k-1} - \mathcal{Z}(2k-1,q))|I_1| \\ &= q^{2k-2}(2q-1) + (q^{2k-1} - q^{2k-2})(q-1) \\ &= q^{2k-2}(2q-1) + q^{2k-2}(q-1)^2 \\ &= q^{2k-2}(2q-1+q^2-2q+1) \\ &= q^{2k-2} \cdot q^2 \\ &= q^{2k}.\end{aligned}$$

Thus $\mathcal{Z}(m,q) = q^{m-1}$.

(ii) $q \equiv 3 \pmod 4$: $|I_0| = 1$ and $|I_1| = q+1$.

Base $m=1$: $\mathcal{Z}(1,q) = 1 = q^0$.

Assume that this is true for $m = 2k-1$. Hence we have $\mathcal{Z}(2k-1,q) = q^{2k-2}$. We show that it is true for $m = 2k+1$.

$$\begin{aligned}\mathcal{Z}(2k+1,q) &= q^{2k-2} \cdot 1 + (q^{2k-1} - q^{2k-2})(q+1) \\ &= q^{2k-2} + q^{2k-2}(q-1)(q+1) \\ &= q^{2k-2} + q^{2k} - q^{2k-2} = q^{2k}.\end{aligned}$$

Thus $\mathcal{Z}(m,q) = q^{m-1}$ for m odd.

(b) m even:

(i) $q \equiv 1 \pmod 4$: $|I_0| = 2q-1$ and $|I_1| = q-1$.

Base $m=2$: $\mathcal{Z}(2,q) = 2q-1 = q+q-1$.

Assume that this holds for $m = 2k$; i.e.,

$\mathcal{Z}(2k, q) = q^{2k-1} + q^{\frac{2k}{2}} - q^{\frac{2k-2}{2}} = q^{2k-1} + q^k - q^{k-1}$.

Now we show that the result holds for $m = 2k + 2 = 2(k + 1)$.

$$\begin{aligned}
\mathcal{Z}(2k+2, q) &= \mathcal{Z}(2k, q)|I_0| + (q^{2k} - \mathcal{Z}(2k, q))|I_1| \\
&= (q^{2k-1} + q^k - q^{k-1})(2q - 1) + (q^{2k} - q^{2k-1} - q^k + q^{k-1})(q - 1) \\
&= q^{2k+1} + q^{k+1} - q^k \\
&= q^{2(k+1)-1} + q^{k+1} - q^{(k+1)-1}.
\end{aligned}$$

Thus $\mathcal{Z}(m, q) = q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}$ if m is even.

(ii) $q \equiv 3 \pmod 4$: $|I_0| = 1$ and $|I_1| = q + 1$.

$\mathcal{Z}(2, q) = 1 = q - q + 1$.

In a similar way as previously, we have $\mathcal{Z}(m, q) = q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}}$.

For the evaluation of $\mathcal{S}(m, q)$ and $\mathcal{N}(m, q)$, we get the following.

(a) m odd:

(i) $q \equiv 1 \pmod 4$: $|I_0| = 2q - 1$; $|I_1| = q - 1$.

Base $m = 1$: $\mathcal{S}(1, q) = q - 1$; $\mathcal{N}(1, q) = 0$.

To show that $\mathcal{S}(m, q) = \dfrac{1}{2}\left(q^m - q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right)$, we find $\mathcal{N}(m, q)$ from $\mathcal{S}(m, q)$ by using Lemma 2.23.

$$\begin{aligned}
\mathcal{N}(m, q) &= q^m - \mathcal{S}(m, q) - \mathcal{Z}(m, q) \\
&= q^m - \frac{1}{2}\left(q^m - q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right) - q^{m-1} \\
&= q^m - \frac{1}{2}q^m + \frac{1}{2}q^{m-1} - \frac{1}{2}q^{\frac{m+1}{2}} + \frac{1}{2}q^{\frac{m-1}{2}} - q^{m-1} \\
&= \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m+1}{2}} + q^{\frac{m-1}{2}}\right).
\end{aligned}$$

Assume that the result is true for $m = 2k - 1$; i.e.,

$\mathcal{S}(2k-1, q) = \dfrac{1}{2}\left(q^{2k-1} - q^{2k-2} + q^k - q^{k-1}\right)$;

$\mathcal{N}(2k-1, q) = \dfrac{1}{2}\left(q^{2k-1} - q^{2k-2} - q^k + q^{k-1}\right)$; and $\mathcal{Z}(2k-1, q) = q^{2k-2}$.

For $m = 2k+1 = 2(k+1)-1$, we show that the result is true.

$$\begin{aligned}
\mathcal{S}(2k+1,q) &= \left(\frac{q-1}{2}\right)(\mathcal{N}(2k-1,q)+\mathcal{Z}(2k-1,q))|I_1| + \left(\frac{q-3}{2}\right)\mathcal{S}(2k-1,q)|I_1| \\
&\quad + \mathcal{S}(2k-1,q)|I_0| \\
&= \left(\frac{q-1}{2}\right)\left[\frac{1}{2}\left(q^{2k-1}-q^{2k-2}-q^k+q^{k-1}\right)+q^{2k-2}\right](q-1) \\
&\quad + \frac{1}{2}\left(\frac{q-3}{2}\right)\left(q^{2k-1}-q^{2k-2}+q^k-q^{k-1}\right)(q-1) \\
&\quad + \frac{1}{2}\left(q^{2k-1}-q^{2k-2}+q^k-q^{k-1}\right)(2q-1) \\
&= \frac{1}{4}(q^2-2q+1)(q^{2k-1}+q^{2k-2}-q^k+q^{k-1}) \\
&\quad + \frac{1}{4}(q^2-4q+3)(q^{2k-1}-q^{2k-2}+q^k-q^{k-1}) \\
&\quad + \frac{1}{2}(q^{2k-1}-q^{2k-2}+q^k-q^{k-1})(2q-1) \\
&= \frac{1}{4}(2q^{2k+1}-2q^{2k}+2q^{k+1}-2q^k) \\
&= \frac{1}{2}(q^{2k+1}-q^{2k}+q^{k+1}-q^k) \\
&= \frac{1}{2}(q^{2(k+1)-1}-q^{2(k+1)-2}+q^{k+1}-q^{(k+1)-1}).
\end{aligned}$$

Thus

$$\mathcal{S}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right);$$

and

$$\mathcal{N}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right).$$

(ii) $q \equiv 3 \pmod 4$: $|I_0| = 1$, $|I_1| = q+1$.

Base $m=1$: $\mathcal{S}(1,q) = q-1$, $\mathcal{N}(1,q) = 0$.

To show that $\mathcal{S}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}}\right)$, we find first $\mathcal{N}(m,q)$

from $\mathcal{S}(m,q)$:

$$\begin{aligned}\mathcal{N}(m,q) &= q^m - \mathcal{S}(m,q) - \mathcal{Z}(m,q)\\ &= q^m - \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}}\right) - q^{m-1}\\ &= \frac{1}{2}\left(q^m - q^{m-1} + (-q)^{\frac{m+1}{2}} + (-q)^{\frac{m-1}{2}}\right).\end{aligned}$$

Assume that the result holds for $m = 2k-1$; i.e.,

$\mathcal{S}(2k-1,q) = \dfrac{1}{2}(q^{2k-1} - q^{2k-2} - (-q)^k - (-q)^{k-1})$; $\mathcal{Z}(2k-1,q) = q^{2k-2}$;

and $\mathcal{N}(2k-1,q) = \dfrac{1}{2}(q^{2k-1} - q^{2k-2} + (-q)^k + (-q)^{k-1})$.

Now we show that it holds for $m = 2k+1$.

$$\begin{aligned}\mathcal{S}(2k+1,q) &= \left(\frac{q-1}{2}\right)(\mathcal{N}(2k-1,q) + \mathcal{Z}(2k-1,q))|I_1|\\ &\quad + \left(\frac{q-3}{2}\right)\mathcal{S}(2k-1,q)|I_1| + \mathcal{S}(2k-1,q)|I_0|\\ &= \left(\frac{q-1}{2}\right)\left[\frac{1}{2}(q^{2k-1} - q^{2k-2} + (-q)^k + (-q)^{k-1}) + q^{2k-2}\right](q+1)\\ &\quad + \frac{1}{2}\left(\frac{q-3}{2}\right)(q^{2k-1} - q^{2k-2} - (-q)^k - (-q)^{k-1})(q+1)\\ &\quad + \frac{1}{2}(q^{2k-1} - q^{2k-2} - (-q)^k - (-q)^{k-1}) \cdot 1\\ &= \frac{1}{4}(q^2-1)(q^{2k-1} - q^{2k-2} + (-q)^k + (-q)^{k-1} + 2q^{2k-2})\\ &\quad + \frac{1}{4}(q^2 - 2q - 3)(q^{2k-1} - q^{2k-2} - (-q)^k - (-q)^{k-1})\\ &\quad + \frac{1}{2}(q^{2k-1} - q^{2k-2} - (-q)^k - (-q)^{k-1})\\ &= \frac{1}{4}(2q^{2k+1} - 2q^{2k} - 2(-q)^{k+1} - 2(-q)^k)\\ &= \frac{1}{2}(q^{2k+1} - q^{2k} - (-q)^{k+1} - (-q)^k)\\ &= \frac{1}{2}(q^{2(k+1)-1} - q^{2(k+1)-2} - (-q)^{k+1} - (-q)^{(k+1)-1}).\end{aligned}$$

Thus

$$\mathcal{S}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}}\right);$$

and

$$\mathcal{N}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} + (-q)^{\frac{m+1}{2}} + (-q)^{\frac{m-1}{2}}\right).$$

(b) m even:

(i) $q \equiv 1 \pmod 4$: $|I_0| = 2q-1$, $|I_1| = q-1$.

Base $m=2$: $\mathcal{S}(2,q) = \dfrac{(q-1)^2}{2}$ and $\mathcal{N}(2,q) = \dfrac{(q-1)^2}{2}$.

That is, $\mathcal{S}(2,q) = \dfrac{1}{2}(q^2 - q - q + 1) = \mathcal{N}(2,q)$.

To show that $\mathcal{S}(m,q) = \dfrac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right)$, we first find $\mathcal{N}(m,q)$ from $\mathcal{S}(m,q)$.

$$\begin{aligned}\mathcal{N}(m,q) &= q^m - \mathcal{S}(m,q) - \mathcal{Z}(m,q)\\ &= q^m - \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right) - \left(q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}\right)\\ &= \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right).\end{aligned}$$

Assume that the result holds for $m = 2k$; i.e.,

$\mathcal{S}(2k,q) = \dfrac{1}{2}(q^{2k} - q^{2k-1} - q^k + q^{k-1})$; $\mathcal{Z}(2k,q) = q^{2k-1} + q^k - q^{k-1}$;

and $\mathcal{N}(2k,q) = \dfrac{1}{2}\left(q^{2k} - q^{2k-1} - q^k + q^{k-1}\right)$.

Then we show that it is true for $m = 2k+2$.

$$\begin{aligned}
\mathcal{S}(2k+2,q) &= \left(\frac{q-1}{2}\right)(\mathcal{N}(2k,q)+\mathcal{Z}(2k,q))|I_1| \\
&\quad + \left(\frac{q-3}{2}\right)\mathcal{S}(2k,q)|I_1| + \mathcal{S}(2k,q)|I_0| \\
&= \left(\frac{q-1}{2}\right)\left[\frac{1}{2}(q^{2k}-q^{2k-1}-q^k+q^{k-1})+q^{2k-1}+q^k-q^{k-1}\right](q-1) \\
&\quad + \frac{1}{2}\left(\frac{q-3}{2}\right)(q^{2k}-q^{2k-1}-q^k+q^{k-1})(q-1) \\
&\quad + \frac{1}{2}(q^{2k}-q^{2k-1}-q^k+q^{k-1})(2q-1) \\
&= \frac{1}{4}(q^2-2q+1)(q^{2k}+q^{2k-1}+q^k-q^{k-1}) \\
&\quad + \frac{1}{4}(q^2-4q+3)(q^{2k}-q^{2k-1}-q^k+q^{k-1}) \\
&\quad + \frac{1}{2}(q^{2k}-q^{2k-1}-q^k+q^{k-1})(2q-1) \\
&= \frac{1}{4}(2q^{2k+2}-2q^{2k+1}-2q^{k+1}+2q^k) \\
&= \frac{1}{2}(q^{2k+2}-q^{2k+1}-q^{k+1}+q^k) \\
&= \frac{1}{2}(q^{2(k+1)}-q^{2(k+1)-1}-q^{k+1}+q^{(k+1)-1}).
\end{aligned}$$

Thus

$$\mathcal{S}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right);$$

and

$$\mathcal{N}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right).$$

(ii) $q \equiv 3 \pmod 4$: $|I_0| = 1$, $|I_1| = q+1$.

Base $m=2$: $\mathcal{S}(2,q) = \dfrac{q^2-1}{2}$ and $\mathcal{N}(2,q) = \dfrac{q^2-1}{2}$.

That is, $\mathcal{S}(2,q) = \dfrac{1}{2}(q^2-q+q-1) = \mathcal{N}(2,q)$.

To show that $\mathcal{S}(m,q) = \dfrac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right)$, again we first find

$\mathcal{N}(m,q)$ given $\mathcal{S}(m,q)$.

$$\begin{aligned}\mathcal{N}(m,q) &= q^m - \mathcal{S}(m,q) - \mathcal{Z}(m,q)\\ &= q^m - \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right) - \left(q^{m-1} + (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right)\\ &= \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right).\end{aligned}$$

Again by induction hypothesis, the result holds for $m = 2k$; i.e.,

$\mathcal{S}(2k,q) = \frac{1}{2}(q^{2k} - q^{2k-1} - (-q)^k - (-q)^{k-1})$; $\mathcal{Z}(2k,q) = q^{2k-1} + (-q)^k + (-q)^{k-1}$;

and $\mathcal{N}(2k,q) = \frac{1}{2}(q^{2k} - q^{2k-1} - (-q)^k - (-q)^{k-1})$.

For $m = 2k+2$ we show that the result holds.

$$\begin{aligned}\mathcal{S}(2k+2,q) &= \left(\frac{q-1}{2}\right)\Big[\frac{1}{2}(q^{2k} - q^{2k-1} - (-q)^k - (-q)^{k-1})\\ &\quad + q^{2k-1} + (-q)^k + (-q)^{k-1}\Big](q+1)\\ &\quad + \frac{1}{2}\left(\frac{q-3}{2}\right)(q^{2k} - q^{2k-1} - (-q)^k - (-q)^{k-1})(q+1)\\ &\quad + \frac{1}{2}(q^{2k} - q^{2k-1} - (-q)^k - (-q)^{k-1}) \cdot 1\\ &= \frac{1}{4}(q^2-1)(q^{2k} + q^{2k-1} + (-q)^k + (-q)^{k-1})\\ &\quad + \frac{1}{4}(q^2 - 2q - 3)(q^{2k} - q^{2k-1} - (-q)^k - (-q)^{k-1})\\ &\quad + \frac{1}{2}(q^{2k} - q^{2k-1} - (-q)^k - (-q)^{k-1})\\ &= \frac{1}{4}(2q^{2k+2} - 2q^{2k+1} - 2(-q)^{k+1} - 2(-q)^k)\\ &= \frac{1}{2}(q^{2k+2} - q^{2k+1} - (-q)^{k+1} - (-q)^k)\\ &= \frac{1}{2}(q^{2(k+1)} - q^{2(k+1)-1} - (-q)^{k+1} - (-q)^{(k+1)-1}).\end{aligned}$$

Thus

$$\mathcal{S}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right);$$

and

$$\mathcal{N}(m,q) = \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right).$$

□

2.4 Primitive groups, examples and characterization

In this section, we collect all definitions and results related to finite primitive permutation groups, that will be used in Chapter 5. As an example of a permutation group, we begin with a very important type of group in this thesis, namely, the affine group over a field F. See [11,38,40] for further details on all notations, concepts, and useful facts related to abstract groups and Permutation Group Theory, that will be used throughout this section and Chapter 5.

Definition 2.13 An automorphism of the affine space $\mathrm{AG}_m(F)$ is a permutation of the set of points which maps each affine subspace to an affine subspace (of the same dimension). In other words, an *affine automorphism* is a permutation of the points that preserves or respects the affine geometry. By the *affine geometry* (denoted by $\mathrm{AG}_m(F)$), is meant the set consisting of points and affine subspaces constructed from the vector subspaces of F^m of row vectors of dimension m over the field F.

An *affine transformation* is an affine automorphism of an especially simple form. For each linear transformation $A \in \mathrm{GL}_m(F)$ and vector $\mathbf{v} \in F^m$, the affine transformation $\lambda_{A,\mathbf{v}} : F^m \longrightarrow F^m$ is defined by $\lambda_{A,\mathbf{v}} : \mathbf{u} \longmapsto \mathbf{u}A + \mathbf{v}$.

Each of the mapping is an automorphism of the affine geometry $\mathrm{AG}_m(F)$. The set of all $\lambda_{A,\mathbf{v}}$ ($A \in \mathrm{GL}_m(F)$ and $\mathbf{v} \in F^m$) forms the *affine group* denoted by $\mathrm{AGL}_m(F)$ of dimension $m \geq 1$ over F. It is a classical result that $\mathrm{AGL}_m(F)$ is a 2-transitive subgroup of the symmetric group S_{F^m}.

For any vector $\mathbf{v} \in \mathbb{F}_q^m$, the associated translation $\lambda_{I,\mathbf{v}}$ with I the $m \times m$ identity matrix, is a permutation, mapping the vector $\mathbf{u}$ to the vector $\mathbf{u} + \mathbf{v}$. Denote by Λ the set of such elements called the *translation group* of F^m. For any $\lambda_{I,\mathbf{v}} \in \Lambda$ and any $\lambda_{A,\mathbf{0}}$, an element of $\mathrm{GL}_m(F)$ mapping the vector $\mathbf{u}$ to $\mathbf{u}A$, it is easy to show that $\lambda_{A,\mathbf{0}}^{-1}\lambda_{I,\mathbf{v}}\lambda_{A,\mathbf{0}} = \lambda_{I,\mathbf{v}A} \in \Lambda$ so that $\Lambda \lhd \mathrm{AGL}_m(F)$. It follows that $\mathrm{AGL}_m(F) = \Lambda(\mathrm{GL}_m(F))$. Clearly, the stabilizer in $\mathrm{AGL}_m(F)$ of the zero vector is $\mathrm{GL}_m(F)$ since no non-trivial element of Λ fixes this vector; thus $\Lambda \cap \mathrm{GL}_m(F) = 1$. In summary, $\mathrm{AGL}_m(F)$ is the semi-direct product of Λ by $\mathrm{GL}_m(F)$.

Further affine automorphisms are derived from the automorphisms of the field F. For each field automorphism $\sigma \in \mathrm{Aut}(F)$, there is a permutation of F^m defined by $\lambda_\sigma : \mathbf{u} \longmapsto \mathbf{u}^\sigma$, where σ acts componentwise on the vector $\mathbf{u}$. The mappings λ_σ ($\sigma \in \mathrm{Aut}(F)$) form a subgroup of S_{F^m} isomorphic to $\mathrm{Aut}(F)$. This subgroup, together with $\mathrm{AGL}_m(F)$, generates the group $\mathrm{A\Gamma L}_m(F)$ of *affine semi-linear transformations.* The elements of $\mathrm{A\Gamma L}_m(F)$ are precisely the permutations of F^m of the form $\lambda_{A,\mathbf{v},\sigma} : \mathbf{u} \longmapsto \mathbf{u}^\sigma A + \mathbf{v}$, where $A \in \mathrm{GL}_m(F)$, $\mathbf{v} \in F^m$, and $\sigma \in \mathrm{Aut}(F)$. When $m \geq 2$, it turns out that the group $\mathrm{A\Gamma L}_m(F)$ is the full automorphism group of the affine geometry $\mathrm{AG}_m(F)$. (See [11, Exercises 2.8.10 and 2.8.12]). It can be easily shown that the subgroup isomorphic to $\mathrm{Aut}(F)$ normalizes $\mathrm{AGL}_m(F)$, so that $\mathrm{A\Gamma L}_m(F) \cong \mathrm{AGL}_m(F) \rtimes \mathrm{Aut}(F)$. In the case that $\mathrm{Aut}(F) = 1$ (For example, if $|F|$ is a prime or if $F = \mathbb{R}$ or $\mathbb{Q}$), we have $\mathrm{A\Gamma L}_m(F) = \mathrm{AGL}_m(F)$.

In particular, if $F = \mathbb{F}_q$ a finite field defined in Section 2.2 with $q = p^r$, p prime, then by [33], it has been shown that the only automorphisms of $\mathbb{F}_q$ are those called *Frobenius automorphisms.* Those automorphisms are of the form $\xi \longmapsto \xi^p$ so that the order of $\mathrm{Aut}(\mathbb{F}_q)$ is r. Since Λ is isomorphic to the additive group $\mathbb{F}_q^m$, then $|\Lambda| = q^m$. Clearly, it can be deduced that the order of $\mathrm{A\Gamma L}_m(\mathbb{F}_q)$ is $rq^m|\mathrm{GL}_m(\mathbb{F}_q)|$ with $|\mathrm{GL}_m(\mathbb{F}_q)| = (q^m - 1)(q^m - q)\cdots(q^m - q^{m-1})$. (See [38, 3.2.7] for the latter equality).

The group $\mathrm{AGL}_m(F)$ has several important classes of subgroups. One of them is the subgroup denoted by $\mathrm{ASL}_m(F)$ [11], namely, the *affine special linear group* defined by

$$\mathrm{ASL}_m(F) = \{\lambda_{A,\mathbf{v}} \in \mathrm{AGL}_m(F) : \det(A) = 1\}.$$

From the linear groups $\mathrm{GL}_m(F)$ and $\mathrm{SL}_m(F)$, the center of each of them has been defined in [38, 3.2.6]. The former has center Z which consists of scalar matrices αI, $\alpha \in F \setminus \{0\}$ with I the $n \times n$ identity matrix. The latter has center $Z \cap \mathrm{SL}_m(F)$. From there, the groups; namely, the *projective general linear groups* $\mathrm{PGL}_m(F)$, and $\mathrm{PSL}_m(F)$ of dimension m over a field F, were defined to be the quotient groups $\mathrm{GL}_m(F)/Z$ and $\mathrm{SL}_m(F)Z/Z$ (see [38, 1.4.4 and 3.2.6] and [11]). The latter projective groups have been shown to be non-abelian simple groups if $d \geq 2$ and $|F| > 3$. See [38, 3.2.9].

Finally, we present some definitions and results related to primitive groups. These will be the main tools that will be mostly used in Chapter 5.

The action of G on Ω can be extended to subsets of Ω by defining $\Gamma^x = \{\gamma^x : \gamma \in \Gamma\}$ for each $\Gamma \subseteq \Omega$.

Definition 2.14 Let G be a group acting transitively on a set Ω. A non-empty subset Δ of Ω is called a *block* for G if for each $x \in G$, either $\Delta^x = \Delta$ or $\Delta^x \cap \Delta = \varnothing$.

If G is a group acting transitively on the set Ω, it is clear that Ω and the singletons $\{\alpha\}$ ($\alpha \in \Omega$) are blocks for G. These are called the *trivial blocks.* Any other block is called *non-trivial* or *system of imprimitivity.* A block which is minimal in the set of blocks of size greater than 1 is called a *minimal block.*

The importance of blocks arises from the following observation. (See [11, Exercise 1.5.3]).

Proposition 2.25 [11] *Suppose that G acts transitively on Ω and that Δ is a block for G. Put $\Sigma := \{\Delta^x : x \in G\}$. Then the sets in Σ form a partition of Ω, and each element of Σ is a block for G.*

We call Σ in Proposition 2.25 the *system of blocks* containing Δ. Now G acts on Σ in an obvious way, and this new action may give useful information about G provided Δ is a non-trivial block.

Definition 2.15 Let G be a group which acts transitively on a set Ω. The group G is said to be *primitive* if it has no non-trivial blocks on Ω; otherwise, G is called *imprimitive.*

To describe relation between blocks and subgroups, the following notation which extends the notation for a point-stabilizer is required.

If G is a group acting on a set Ω and $\Delta \subseteq \Omega$, then the *elementwise stabilizer* of Δ in G is defined by

$$G_{\Delta} = \{x \in G : \delta^x = \delta \text{ for all } \delta \in \Delta\},$$

and the *setwise stabilizer* of Δ in G by

$$G_{\{\Delta\}} = \{x \in G : \Delta^x = \Delta\}.$$

It is easily shown that G_{Δ} and $G_{\{\Delta\}}$ are both subgroups of G, and that $G_{\Delta} \lhd G_{\{\Delta\}}$. Note that $G_{\{\alpha\}} = G_{\alpha}$ for each $\alpha \in \Omega$. More generally, for a finite set $\Delta = \{\alpha_1 \cdots, \alpha_k\}$, G_{Δ} is often written as $G_{\alpha_1, \cdots, \alpha_k}$ instead of $G_{\{\alpha_1 \cdots, \alpha_k\}}$.

Now we have a very important result with a proof given in [11, Theorem 1.5A], which is useful in Chapter 5. This represents the relation between blocks and subgroups.

Theorem 2.26 [11] *Let G be a group which acts transitively on a set Ω and let $\alpha \in \Omega$. Let $\mathcal{B}$ be the set of all blocks Δ for G with $\alpha \in \Delta$, and let $\mathcal{S}$ denote the set of all subgroups H of G with $G_{\alpha} \leqslant H$. Then there is a bijection Ψ of $\mathcal{B}$ onto $\mathcal{S}$ given by $\Psi(\Delta) = G_{\{\Delta\}}$, whose inverse mapping Φ is given by $\Phi(H) = \alpha^H$. The* *mapping Ψ is order-preserving in the sense that, if $\Delta, \Gamma \in \mathcal{B}$, then $\Delta \subseteq \Gamma$ if and only if $\Psi(\Delta) \leqslant \Psi(\Gamma)$.*

Note that from Theorem 2.26, it can be deduced that G is primitive if and only if each point-stabilizer is a maximal subgroup of G. In addition, it has been shown by [11, Lemma 1.6A(i)] that the orbits of elements for a normal subgroup of any transitive permutation group G on Ω are blocks for G. It follows that every non-trivial normal subgroup of a primitive permutation group is transitive, see [11, Lemma 1.6(v)] and [38, 7.2.5].

In terms of wreath products, we have the other examples of primitive and imprimitive actions which are very important in this chapter and Chapter 5. These are the two standard actions of a wreath product.

Let H act transitively on Δ, and let K act transitively on $\Gamma = \{1, 2, \cdots, r\}$ a finite set. Then $H \wr_\Gamma K$ acts on Δ^r by sending $(\delta_1, \delta_2, \cdots, \delta_r)$ to $(\delta_{1^\kappa}^{h_1^\kappa}, \delta_{2^\kappa}^{h_2^\kappa}, \cdots, \delta_{r^\kappa}^{h_r^\kappa})$ for every $(\delta_1, \delta_2, \cdots, \delta_r) \in \delta^r$ and $(h_1, h_2, \cdots, h_r)\kappa^{-1} \in H \wr_\Gamma K$. This is called the *product action* [11,13]. If H is primitive but not regular on Δ and K is transitive on Γ, then the product action is primitive [11, Lemma 2.7A].

On the other hand, $H \wr_\Gamma K$ acts on $\Delta \times \Gamma$ by sending (δ, i) to (δ^{h^i}, i^κ) for every (δ, i) in $\Delta \times \Gamma$, and $(h_1, h_2, \cdots, h_r)\kappa \in H \wr_\Gamma K$. This action is transitive, and the sets $\Gamma_i = \{(\delta, i) : \delta \in \Delta\}$ for $i \in \Gamma$ are blocks that partition $\Delta \times \Gamma$, so this action is imprimitive. Indeed, let $\Gamma_i = \{(\delta, i) : \delta \in \Delta\}$ and $\Gamma_j = \{(\delta, j) : \delta \in \Delta\}$.

If $(\delta^{h_i}, i^\kappa) = (\delta^{h_j}, j^\kappa)$ for some $i, j \in \Gamma$, then $\delta^{h_i} = \delta^{h_j}$ and $i^\kappa = j^\kappa \Leftrightarrow i = j$. This is because κ is a permutation of Γ. Thus $h_i = h_j$ so that $\delta^{h_i} = \delta^{h_j}$. Hence $\Gamma_i^{(h_1, \cdots, h_r)\kappa} = \Gamma_j^{(h_1, \cdots, h_r)\kappa}$, so that Γ_i is a block for $H \wr_\Gamma K$. Therefore this action is imprimitive.

In fact, if H is any imprimitive subgroup of $S_{[n]}$ with r blocks of size m, then H is permutation isomorphic to a subgroup of $S_{[m]} \wr_{[r]} S_{[r]}$ in its imprimitive action on $[m] \times [r]$ with $[m] = \{1, 2, \cdots, m\}$ and $[r] = \{1, 2, \cdots, r\}$. (See [11,13]).

Now we look at the definitions and results related to the analysis of finite primitive groups, which will be most useful in Chapter 5.

The *socle* of a group denoted by $\mathrm{Soc}(G)$, is the subgroup of G generated by all its minimal normal subgroups. By usual convention, $\mathrm{Soc}(G) = 1$ if G has no minimal normal subgroups.

Since the set of all minimal normal subgroups of G is mapped into itself by every automorphism of G, the socle $\mathrm{Soc}(G)$ is a characteristic subgroup of G. Every non-trivial finite group has at least one minimal normal subgroup, so it has a non-trivial socle.

It is a classical result that the socle of a group is a direct product of some of its minimal normal subgroups [11, Theorem 4.3A]. If the latter are all non-abelian, then they are the only minimal normal subgroups. In addition, every minimal normal subgroup K of a group G is a direct product of some of its simple subgroups, which are conjugate under G. If the latter are also non-abelian, then they are the only minimal normal subgroups of K. Consequently, it follows that every minimal normal subgroup of a finite group is either an elementary abelian p-group for some prime p, or its centre is trivial. (See [11, Corollary 4.3B] and [38, 7.2.6]). All the above leads to the following general result on socles in the special case of finite primitive group with a proof given in [11, Theorem 4.3B].

Theorem 2.27 [11] *If G is a finite primitive permutation group acting on Ω, and K is a minimal normal subgroup of G, then exactly one of the following holds:*

(i) *For some prime p and some integer d, K is a regular elementary abelian group of order p^d, and $\mathrm{Soc}(G) = K = C_G(K)$;*

(ii) *K is a regular non-abelian group, $C_G(K)$ is a minimal normal subgroup of G which is isomorphic to K, and $\mathrm{Soc}(G) = K \times C_G(K)$;*

(iii) *K is non-abelian, $C_G(K) = 1$ and $\mathrm{Soc}(G) = K$.*

Consequently, this leads in turn to the following with a proof given in [11, Corollary 4.3B].

Corollary 2.28 [11] *If G is a finite primitive group, then $H = \mathrm{Soc}(G)$ is a direct product of isomorphic simple groups. If N denotes the normalizer of H in the symmetric group, then H is a minimal normal subgroup of N. Moreover, if H is not regular, then it is the only minimal normal subgroups of N.*

With the above results, we have the main central theorem related to the analysis of finite primitive permutation groups in terms of their socles. This is known as the *O'Nan Scott Theorem.*

Theorem 2.29 [11,26] (O'Nan Scott Theorem) *Let G be a finite primitive permutation group acting on a set Ω, and let H be the socle of G. Then $H \cong T \times \cdots \times T = T^m$ for some simple group T, $m \geq 1$, and one of the following holds:*

(1) Affine type (A)*: H is an elementary abelian p-group of order p^m, it acts regularly on Ω, and $G \leqslant \mathrm{AGL}_m(\mathbb{F}_p)$ is an affine group.*

(2) Regular non-abelian type (RN)*: H is non-abelian, it acts regularly on Ω and $m \geq 6$.*

(3) Almost simple type (AS)*: $H = T$ is non-abelian, it acts non-regularly on Ω, and $G \leqslant \mathrm{Aut}(H)$.*

(4) Diagonal type (D)*: H is non-abelian, $m \geq 2$, and G is a subgroup of a wreath product with the diagonal action, and $|\Omega| = |T|^{m-1}$.*

(5) Product type (P)*: H is non-abelian, $m = rs$ and $s > 1$. The group G is isomorphic to a subgroup of the wreath $U \wr S_{[s]}$ with the product action, where U is a primitive permutation group of degree d such that $|\Omega| = d^s$, U has socle T^r, and U is of type AS or D.*

The proof of the above theorem has been done in various parts through [11, Sections 4.5, 4,6 and 4.7].

In summary, the types A and RN are characterized by regular socles. The former is related to Theorem 2.27(i), and turns to a problem in Linear Algebra (see [11, Theorem 4.7A]). The latter corresponds to Theorem 2.27 (ii), where the socle is regular and a direct product of non-abelian simple factors. Such a group has a point-stabilizer with no non-trivial soluble normal subgroup, so that its action by conjugation on the set of factors is transitive and faithful. So the point-stabilizer is isomorphic to a subgroup of $S_{[m]}$. The normalizer of one factor in the point-stabilizer must contain a composition factor isomorphic to a finite non-abelian subgroup T. (See [11, Theorem 4.7B]).

The remaining types; namely, AS, D, and P, are related to non-regular socles. They correspond to Theorem 2.27 (iii). For the product type, namely P, the socle H is non-regular and a direct product of non-regular simple groups. For that, the normalizer of H in S_Ω must be equal to the wreath product in (5) from Theorem 2.29 with a product action. (See [11, Lemma 4.5A]). For the type D, the construction is again from the product action of a wreath product, but the simple non-abelian group T, for which all factors of H are isomorphic to, is taken as a regular subgroup. It has been shown that the normalizer $N_{S_\Omega}(H)$ of H in the symmetric group S_Ω is the extension of $T \wr S_{[m]}$ by $\mathrm{Out}(T) = \mathrm{Aut}(T)/\mathrm{Inn}(T)$. (See [11, Lemma 4.5B]). Further details are in [11, Theorems 4.5A and 4.6A]. The former type is related to $m = 1$. The details of the proof for the three last cases of Theorem 2.29 are found in [11, Theorem 4.6A].

It has been shown that a transitive permutation group can be seen to act as groups of automorphisms of a directed graph.

Let G denote a finite group which acts transitively on a set Ω. Then G acts on

$\Omega \times \Omega$ coordinatewise, and the respective orbits are called the *orbitals* of G. Since G is transitive on Ω, the set $\{(\omega, \omega) : \omega \in \Omega\}$ is an orbital, also called the *diagonal orbital* of G. Given an orbital Δ of G, the *orbital digraph* Graph(Δ) is defined to have vertex set Ω and arc set Δ. The number of orbits of the stabilizer G_ω is equal to the number of the orbitals of G for any $\omega \in \Omega$. This number is called the *rank* of G. In addition, the sizes of the G_ω-orbits do not depend on ω, and these parameters are called the *subdegrees* of Ω. The set $\{\omega\}$ is trivially a G_ω-orbit, and we refer to the sizes of the remaining G_ω-orbits as the non-trivial subdegrees.

The following theorem with a proof given in [11, Theorem 3.2A] gives another characterisation of primitivity to be used in Chapter 5.

Theorem 2.30 [11] *Let G be a group acting transitively on a set Ω. Then G acts primitively if and only if* Graph(Δ) *is connected for each non-diagonal orbital Δ.*

In addition, from the above definitions, we shall use the following theorem about transitive actions of simple groups proved by R.M. Guralnick [17, Corollary 2].

Theorem 2.31 [17, 26] *Let G be a non-abelian simple group acting transitively on Ω with $|\Omega| = p^a$, p prime. Then G acts 2-transitively on Ω unless $G \cong PSU_4(\mathbb{F}_2)$, and $|\Omega| = 27$, in which case G has rank 3, whose subdegrees are 1, 10 and 16.*

Finally, one cornerstone of the proof will be the following classification of finite primitive affine permutation groups of rank 3 obtained by M. W. Liebeck [34, Theorem 1.1]

Theorem 2.32 [26, 34] *Let G be a finite primitive affine permutation group of rank 3 and of degree $n = p^d$, with socle $V \cong \mathbb{Z}_p^d$ for some prime p, and let G_0 be the stabilizer of the zero vector in V. Then one of the following holds:*

(i) Infinite classes (A)*: G is in one of 11 infinite classes of permutation groups labelled by* (A1)-(A11)*. If G is in class* (A1)*, then G_0 is isomorphic to a subgroup of $\Gamma L_1(\mathbb{F}_{p^n})$; and if G is in class* (A2)-(A11) (*see* Table 1 *from* Appendix A)*, then $d = 2r$ and G has non-trivial subdegrees listed in* Table 2 *from* Appendix B*.*

(ii) 'Extraspecial' classes (B)*: G is in one of a finite set of permutation groups whose degree is equal to one of the following numbers* (*see* [34, Table 1])*:*

$$2^6, 3^4, 3^6, 3^8, 5^4, 7^2, 7^4, 13^2, 17^2, 19^2, 23^2, 29^2, 31^2, 47^2. \qquad (2.2)$$

(iii) 'Exceptional' classes (C)*: G is one of a finite set of permutation groups whose* *degree is equal to one of the following numbers* (*see* [34, Table 2])*:*

$$2^6, 2^8, 2^{11}, 2^{12}, 3^4, 3^5, 3^6, 3^{12}, 5^4, 5^6, 7^4, 31^2, 41^2, 71^2, 79^2, 89^2. \qquad (2.3)$$

Chapter 3

Constituent graphs of integral distance graphs as Cayley graphs

3.1 Introduction

In this chapter, before we define the integral distance graph and explore it as a Cayley graph, we shall first consider the constituent graphs of integral distances graphs in two dimensions over a finite field $\mathbb{F}_q$, $q \equiv 1 \pmod 4$. We will also explore them as Cayley graphs and deduce that the integral distance graph for the above case is a Cayley graph. By defining and exploring the integral distance graph as a Cayley graph in all dimensions, we shall also deduce that it is Cayley for $q \equiv 3 \pmod 4$ in two dimensions.

It is going to be shown that the integral distance graph is contained in a certain set of graphs. The class of Cayley graphs containing the integral distance graph has it that the Cayley sets form a concrete Boolean algebra. The latter is generated by the two base Cayley sets of the constituent graphs that we are going to define in this chapter.

As alluded to in Chapter 1, it turns out that it is useful to model integral point sets as cliques of certain graphs. The graphs in question are generalizations of graphs called *Paley graphs* in certain cases. We now first present Paley graphs as follows.

Definition 3.1 By the *Paley graph* $P(q)$ with q a prime power, $q \equiv 1 \pmod 4$, is

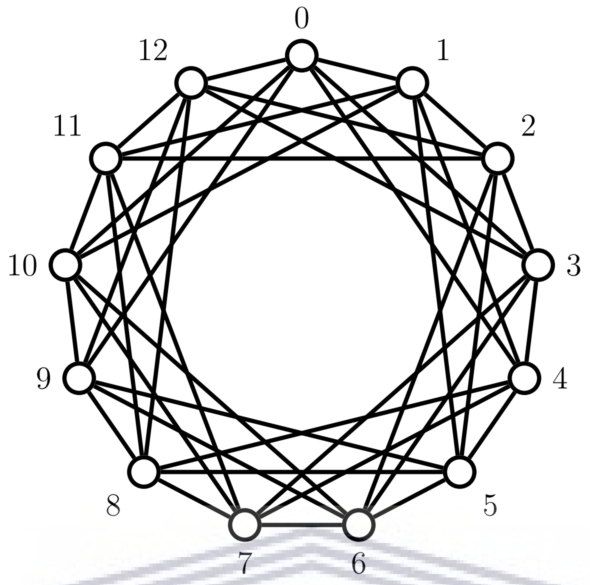


Figure 3.1: Paley graph of order 13.

meant the graph given by

$$\begin{aligned} V(P(q)) &= \mathbb{F}_q; \\ E(P(q)) &= \{\{x,y\} : x, y \in \mathbb{F}_q, x - y \in \square_q^*\}. \end{aligned}$$

Example 4 Let $P(13) = (V, E)$ be the Paley graph of order 13. Here we have $q = 13$. Then

$$V(P(13)) = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\};$$

and

$$\square_{13}^* = \{1, 3, 4, 9, 10, 12\}.$$

It follows that each vertex in $V(P(13))$ (see Figure 3.1) is adjacent to exactly six vertices $x + 1$, $x + 3$, $x + 4$, $x + 9$, $x + 10$, and $x + 12$. So

$$E(P(13)) = \{\{x, x{+}1\}, \{x, x{+}3\}, \{x, x{+}4\}, \{x, x{+}9\}, \{x, x{+}10\}, \{x, x{+}12\} \text{ for all } x \in \mathbb{F}_{13}\}.$$

It remains to see that the Paley graph is another example of a Cayley graph.

Lemma 3.1 *The Paley graph $P(q)$ defined in* Definition 3.1 *is a Cayley graph.*

Proof. For $\mathbb{F}_q$, consider it as an additive group and let $S = \square_q^*$. Since $-1 \in \square_q^*$ for $q \equiv 1 \pmod 4$ and $\square_q^*$ is a subgroup of $\mathbb{F}_q^*$, we deduce that $-s \in S$ for all $s \in S$. Thus the Paley graph $P(q) = (V, E)$ is a Cayley graph $\mathrm{Cay}(\mathbb{F}_q, \square_q^*)$. □

Having defined the Paley graphs, we now define graphs of integral distances. From the definition, it will be seen that the latter are indeed generalization of the former.

Before graphs of integral distances are defined in general, we begin with a particular case of constituent graphs of integral distance graphs in two dimensions for $q \equiv 1 \pmod 4$.

3.2 Constituent graphs of integral distance graphs in two dimensions as Cayley graphs

In this section, we shall consider the case of integral distance graphs in two dimensions and show that they are Cayley graphs. First of all, we introduce a set of Cayley graphs whose Cayley sets constitute a concrete boolean algebra of sets. We will form a boolean algebra of two base subsets S_1 and S_2 of $\mathbb{F}_q^2$, $q \equiv 1 \pmod 4$, that we are going to define. After proving that each of the latter sets is Cayley, we shall deduce that the integral distance graph with a connecting set contained in the boolean algebra of those Cayley sets is a Cayley graph. Finally, after defining the Cayley sets of integral distance graphs in all dimensions, we shall deduce that the two dimensional integral distance graph is Cayley for $q \equiv 3 \pmod 4$.

The two base sets of $\mathbb{F}_q^2$ mentioned above are defined as follows:

$$S_1 = \{(x_1, x_2) \in \mathbb{F}_q^2 \setminus \{(0,0)\} : x_1 x_2 = 0\} = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*); \tag{3.1}$$

and

$$S_2 = \{(x_1, x_2) \in \mathbb{F}_q^2 : x_1 x_2 \in \square_q^*\}. \tag{3.2}$$

Let $U = \mathbb{F}_q^2 \setminus \{\mathbf{0}\}$ be the universal set for Cayley sets and

$$S_3 = U \setminus S, \; S = S_1 \cup S_2. \tag{3.3}$$

Now we consider the boolean algebra $\mathfrak{B} = \langle S_1, S_2 \rangle$ generated by the sets S_1 and S_2 defined above. Clearly, $S_1 \cap S_2 = \varnothing$ since from Equation (3.1) and Equation (3.2) we can not have $xy \in \square_q \setminus \{0\}$ and $xy = 0$ at the same time. It follows that S is a disjoint union of S_1 and S_2. The elements of $\mathfrak{B}$ are $\varnothing$, S_1, S_2, S_3, S, $U \setminus S_1$, $U \setminus S_2$, and U, since $S_3 = U \setminus S$ and $S = S_1 \cup S_2$.

In view of Theorem 2.7, it is enough to show that S_1 and S_2 are Cayley sets.

Lemma 3.2 *Let $\mathbb{F}_q$ be a finite field with $q \equiv 1 \pmod 4$. Then S_1 and S_2 defined by* Equation (3.1) *and* Equation (3.2)*, respectively, are Cayley sets.*

Proof. (i) For S_1, it is clear that $(0,0) \notin S_1$. Let $\mathbf{s} = (s_1, s_2) \in S_1$. Then by Equation (3.1), $s_1 s_2 = 0$; i.e., $s_1 = 0$ or $s_2 = 0$, and $-\mathbf{s} = (-s_1, -s_2)$. Thus

$$(-s_1)(-s_2) = s_1 s_2 = 0.$$

Hence $-\mathbf{s} \in S_1$ and therefore S_1 is a Cayley set.

(ii) For S_2, since xy is a non-zero square by Equation (3.2), it follows that $x \neq 0$ and $y \neq 0$; and hence $(0,0) \notin S_2$.

Let $\mathbf{s} = (s_1, s_2) \in S_2$; i.e., $s_1 s_2 \in \square_q^*$.

Then $-\mathbf{s} = (-s_1, -s_2)$, which implies that

$$(-s_1)(-s_2) = (-1)^2 s_1 s_2 = s_1 s_2 \in \square_q^*.$$

Thus $-\mathbf{s} \in S_2$ and hence S_2 is a Cayley set. □

This leads immediately to the following result.

Corollary 3.3 *Let Γ_i be the graphs whose connecting sets are generated by the base sets S_i, $i = 1, 2$, of $\mathfrak{B}$ defined in* Equation (3.1) *and* Equation (3.2)*. Then*

(i) *every element in $\mathfrak{B}$ is a Cayley set;*

(ii) *every graph $\Gamma_i = \mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2$, is a Cayley graph; and*

(iii) *any graph with a connecting set in $\mathfrak{B}$ is a Cayley graph.*

Proof. (i) and (iii) follow immediately by Theorem 2.7 and Proposition 2.4, (ii) follows from Lemma 3.2. □

We illustrate the above results by the following.

Example 5 Let $q = 5$. Then $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ and $\square_5^* = \{1, 4\}$.

The connecting sets are

$$S_1 = \{(0,1); (0,2); (0,3); (0,4); (1,0); (2,0); (3,0); (4,0)\};$$

and

$$S_2 = \{(1,1); (1,4); (2,2); (2,3); (3,2); (3,3); (4,1); (4,4)\}.$$

For each graph $\Gamma_i = \mathrm{Cay}(\mathbb{F}_q^2, S_i)$; $i = 1, 2$; in Figure 3.2, vertices are labelled by vectors (a, b) of $\mathbb{F}_q^2$.

As we have seen the constituent graphs of a two dimensional integral distance graph over $\mathbb{F}_q$, $q \equiv 1 \pmod 4$, as Cayley graph, now we define the integral distance graphs in all dimensions. We will show that the latter is also a Cayley graph for any odd prime power q.

Definition 3.2 By the *graph of integral distances* $\mathfrak{G}_{m,q}$ for a prime power q and a given dimension m, is meant the graph given by

$$\begin{aligned} V(\mathfrak{G}_{m,q}) &= \mathbb{F}_q^m; \\ E(\mathfrak{G}_{m,q}) &= \{\{\mathbf{x}, \mathbf{y}\} : \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^m, d^2(\mathbf{x}, \mathbf{y}) = N(\mathbf{x} - \mathbf{y}) \in \square_q\}. \end{aligned}$$

Graphs of integral distances can be considered as Cayley graphs in the following way.

First we define Cayley sets of the graphs in question.

Lemma 3.4 *Let $S^{(m)} = \{\mathbf{s} \in \mathbb{F}_q^m : N(\mathbf{s}) \in \square_q,\ \mathbf{s} \neq \mathbf{0}\}$ be a subset of $\mathbb{F}_q^m$. Then $S^{(m)}$ is a Cayley set in $\mathbb{F}_q^m$, where $\mathbb{F}_q^m$ is considered as an abelian group under addition.*

Proof. Consider $\mathbb{F}_q^m$ as an abelian group under addition.

(a) Clearly from the definition of $S^{(m)}$, $\mathbf{0} \notin S^{(m)}$.

(b) Let $\mathbf{s} \in S^{(m)}$; i.e., $N(\mathbf{s}) \in \square_q$.

Then $N(-\mathbf{s}) = N(-1 \cdot \mathbf{s}) = (-1)^2 \cdot N(\mathbf{s}) = N(\mathbf{s}) \in \square_q$.

Thus $-\mathbf{s} \in S^{(m)}$ and hence $S^{(m)}$ is a Cayley set. □

The following theorem will be used in Chapter 4.

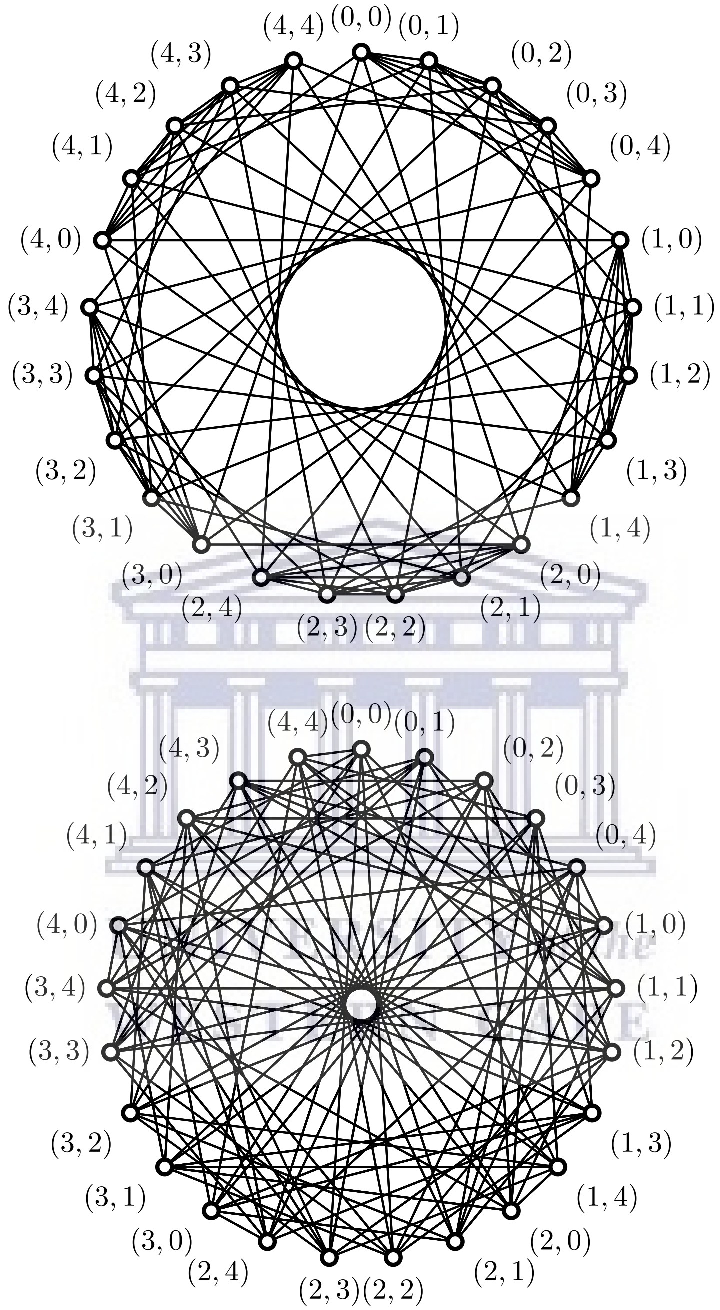


Figure 3.2: Constituent graphs $\Gamma_1 = \mathrm{Cay}(\mathbb{F}_5^2, S_1)$ (above) and $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_5^2, S_2)$ (below).

Theorem 3.5 *Let $\mathbb{F}_q$ be a field and ρ a generator of $\mathbb{F}_q^*$. Let $S_k = \langle \rho^k \rangle$. For $\omega \in \mathbb{F}_q$, if $\omega^k = -1$ has a solution, then*

(i) *S_k is a Cayley set in $\mathbb{F}$; and*

(ii) *S_k is a connecting set if $(k, |\mathbb{F}_q|) = 1$.*

Proof. $S_k = \langle \rho^k \rangle \leqslant \mathbb{F}_q^*$.

Let $-s$ be the additive inverse of $s \in S_k$; i.e., $s = (\rho^k)^l$. If $\omega^k = -1$ for $\omega \in \mathbb{F}_q$; i.e., $\omega^k = (\rho^k)^{l'} = -1$, then $-s = -1 \cdot s \in S_k$. The rest is clear. □

Corollary 3.6 *Let $\mathbb{F}_q$ be an additive group with q an odd prime power. Then*

(i) *for $q \equiv 1 \pmod 4$, the set $\square_q^*$ of all non-zero perfect squares in $\mathbb{F}_q$ is closed under taking inverses under addition; and,*

(ii) *for $q \equiv 3 \pmod 4$, $\square_{q^2}^*$ is a Cayley set.*

Proof. (i) follows from Lemma 3.1.

(ii) For $q \equiv 3 \pmod 4$, since $\mathbb{F}_{q^2}^*$ is a cyclic group by Lemma 2.22; i.e., $\mathbb{F}_{q^2}^* = \langle \rho \rangle$ for some $\rho \in \mathbb{F}_{q^2}^*$, it follows that $\square_{q^2}^* \leqslant \mathbb{F}_{q^2}^*$ is also cyclic and $\square_{q^2}^* = \langle \rho^2 \rangle$. Clearly, $q^2 \equiv 1 \pmod 4$. It follows from (i) that $\square_{q^2}^*$ is a Cayley set, and hence $S = \square_{q^2}^*$ for $q \equiv 3 \pmod 4$. □

Consider the Cayley graph $\mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})$ defined by

$$\begin{aligned} V(\mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})) &= \mathbb{F}_q^m; \\ E(\mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})) &= \{\{\mathbf{x}, \mathbf{y}\} : \mathbf{x}, \mathbf{y} \in \mathbb{F}_q^m, \mathbf{y} = \mathbf{x} + \mathbf{s}, N(\mathbf{s}) \in \square_q\}. \end{aligned}$$

We will show that the graphs of integral distances defined in Definition 3.2 and the Cayley graphs defined above are isomorphic.

3.3 Isomorphism between $\mathfrak{G}_{m,q}$ and $\mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})$

In this section, we are going to show the isomorphism between $\mathfrak{G}_{m,q}$ and $\mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})$. First, we need the following technical lemma.

Lemma 3.7 *$N(\mathbf{x} - \mathbf{y}) \in \square_q$ if and only if there exists $\mathbf{s} \in \mathbb{F}_q^m$ such that $\mathbf{y} = \mathbf{x} + \mathbf{s}$ and $N(\mathbf{s}) \in \square_q$.*

Proof. Assume that $N(\mathbf{x}-\mathbf{y}) \in \square_q$. Then there exists $\mathbf{s}' \in \mathbb{F}_q^m$ such that

$\mathbf{x}-\mathbf{y} = \mathbf{s}' \Leftrightarrow \mathbf{y} = \mathbf{x}-\mathbf{s}'$, and $N(\mathbf{x}-\mathbf{y}) = N(\mathbf{s}') \in \square_q$.

Put $\mathbf{s} = -\mathbf{s}'$; i.e., $\mathbf{s}' = -\mathbf{s}$. Then $\mathbf{y} = \mathbf{x}+\mathbf{s}$ and $N(\mathbf{s}') = N(-\mathbf{s}) = N(\mathbf{s}) \in \square_q$ by Lemma 3.4

Conversely, assume that there exists $\mathbf{s} \in \mathbb{F}_q^m$ such that $\mathbf{y} = \mathbf{x}+\mathbf{s}$, and $N(\mathbf{s}) \in \square_q$.

Then $\mathbf{y} = \mathbf{x}+\mathbf{s} \Leftrightarrow \mathbf{s} = \mathbf{y}-\mathbf{x}$, and

$N(\mathbf{s}) = N(\mathbf{y}-\mathbf{x}) = N(-(\mathbf{x}-\mathbf{y})) = N(\mathbf{x}-\mathbf{y}) \in \square_q$ by Lemma 3.4. □

We now prove the isomorphism between $\text{Cay}(\mathbb{F}_q^m, S^{(m)})$ and $\mathfrak{G}_{m,q}$.

Theorem 3.8 $\Gamma = \text{Cay}(\mathbb{F}_q^m, S^{(m)})$ *as given in* Definition 3.2 *is isomorphic to* $\mathfrak{G}_{m,q}$.

Proof. Define $\sigma : V(\mathfrak{G}_{m,q}) \longrightarrow V(\Gamma)$ by $\sigma(x) = x$.

Clearly, σ is a bijection. It follows immediately that

$$\begin{aligned} \{\mathbf{x},\mathbf{y}\} \in E(\mathfrak{G}_{m,q}) &\Leftrightarrow N(\mathbf{x}-\mathbf{y}) = N(\mathbf{s}) \in \square_q \\ &\Leftrightarrow \mathbf{y} = \mathbf{x}+\mathbf{s}, N(\mathbf{s}) \in \square_q \text{ by Lemma 3.7} \\ &\Leftrightarrow \{\mathbf{x},\mathbf{y}\} \in E(\Gamma). \end{aligned}$$

Therefore $\text{Cay}(\mathbb{F}_q^m, S^{(m)}) \cong \mathfrak{G}_{m,q}$. □

Now, consider the set $\mathbb{S} = S^{(2)} = \{\mathbf{x} \in \mathbb{F}_q^2 : \mathbf{x} \neq \mathbf{0} \text{ and } N(\mathbf{x}) \in \square_q\}$, $q \equiv 1 \pmod 4$. In order to prove that the two dimensional integral distance graph is a Cayley graph for $q \equiv 1 \pmod 4$, we consider the following result.

Lemma 3.9 *Let* ϕ *be an* $\mathbb{F}_q$*-linear mapping defined by*

$\phi : (x_1, x_2) \mapsto (x_1 + \omega x_2, x_1 - \omega x_2)$ *with* $\omega^2 = -1$. *Then*

(i) ϕ *is a switch to hyperbolic coordinates; and*

(ii) ϕ *is an isomorphism between the sets* $\mathbb{S}$ *and* $S = S_1 \cup S_2$, *where* S_1 *and* S_2 *are the two base sets of* $\mathbb{F}_q^2$ *defined by* Equation (3.1) *and* Equation (3.2), *respectively. Hence* $\mathbb{S}$ *is a Cayley set.*

Proof. (i) We show that $\phi : (x_1, x_2) \mapsto (x_1 + \omega x_2, x_1 - \omega x_2)$,$\omega^2 = -1$, is a switch to hyperbolic coordinates.

Put $a = x_1 + \omega x_2$ and $b = x_1 - \omega x_2$. Then it follows that

$x_1 = \dfrac{1}{2}(a+b)$ and $x_2 = -\dfrac{\omega}{2}(a-b)$.

Thus $N(x_1, x_2) = ab$ (see [21]), and hence ϕ is a switch to hyperbolic coordinates.

(ii)Put $N^{\phi}(x_1, x_2) = x_1 x_2$. Then we have

$$\mathbb{S}^{\phi} = \{\mathbf{x} \in \mathbb{F}_q^2 : \mathbf{x} = (x_1, x_2) \neq \mathbf{0} : x_1 x_2 \in \square_q\}.$$

Clearly, ϕ is a bijection of $\mathbb{F}_q^2$ over itself, and $\mathbb{S}^{\phi} = S_1 \cup S_2 = S$ by combining Equation (3.1) and Equation (3.2). It follows that ϕ is an isomorphism between $\mathbb{S}$ and S. The rest follows from Corollary 3.3(i) and Proposition 2.6. □

In particular, all the above results lead to the main result of this chapter in the following.

Proposition 3.10 *The integral distance graph $\mathfrak{G}_{2,q}$ is a Cayley graph for every prime power q.*

Proof. (i) For $q \equiv 1 \pmod 4$, $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$ is a Cayley graph in view of Corollary 3.3(iii). By Lemma 3.9, it follows that $\mathbb{S}$ is a connecting set, and Γ is isomorphic to $\mathrm{Cay}(\mathbb{F}_q^2, \mathbb{S})$ by Proposition 2.6.

(ii) For $q \equiv 3 \pmod 4$, the result follows immediately from Corollary 3.6(ii).

Finally, in both cases for q, the result follows immediately from Theorem 3.8 □

By combining the two Cayley graphs Γ_i, $i = 1, 2$, in Example 5, we obtain $S = S_1 \cup S_2$ as a Cayley set. Now we have the following example of an integral distance graph in two dimensions.

Example 6 Let $q = 5$. We have $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ and $\square_5 = \{0, 1, 4\}$. The vertices of the integral distances graph $\Gamma = \mathrm{Cay}(\mathbb{F}_5^2, S) \cong \mathfrak{G}_{2,5}$ in Figure 3.3 are labelled as in Example 5.

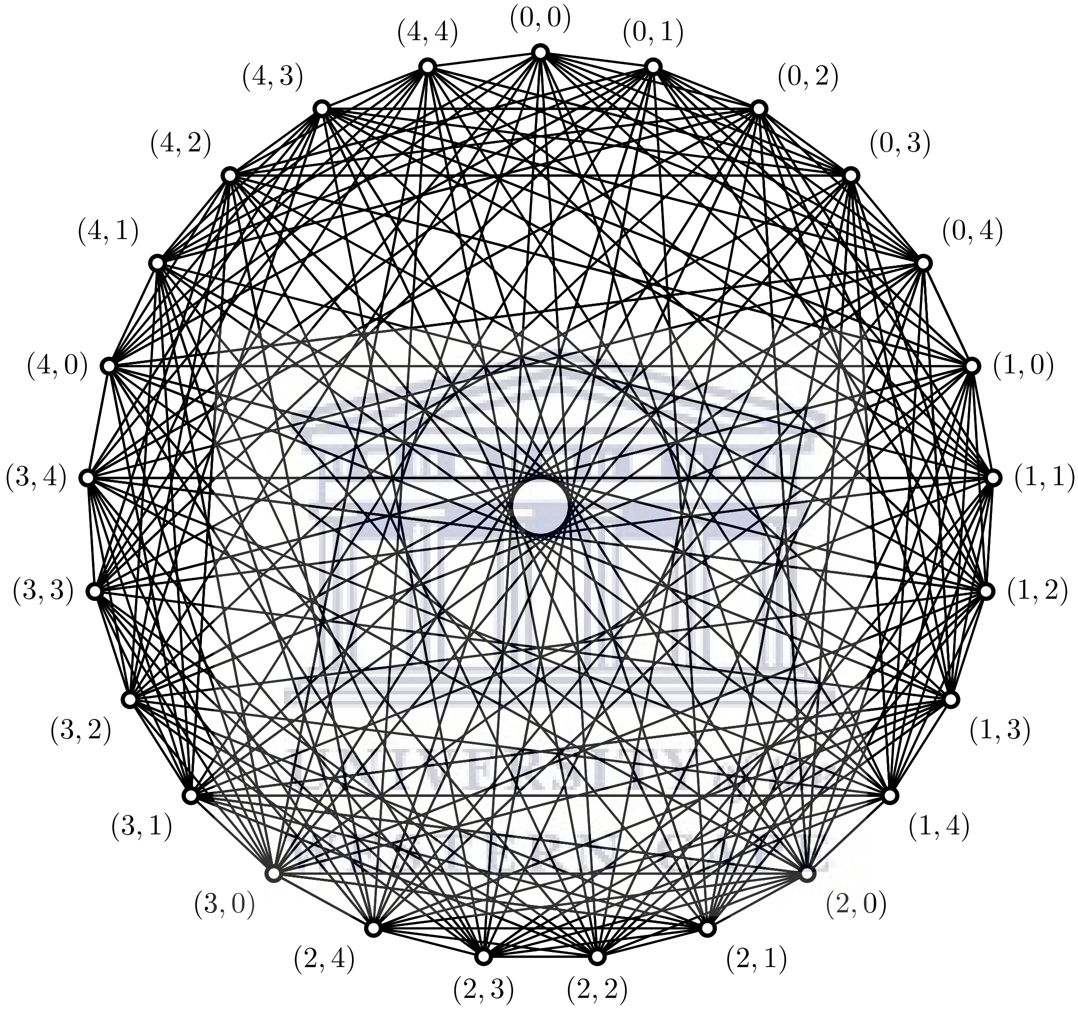


Figure 3.3: Integral distance graph $\Gamma = \mathrm{Cay}(\mathbb{F}_5^2, S) \cong \mathfrak{G}_{2,5}$.

Chapter 4

Constituent graphs of integral distances graphs as strongly regular graphs

In this chapter, we shall explore the integral distance graph as a strongly regular graph. First, we begin with the case of two dimensions. In this case, we explore the three constituent graphs Γ_i, $i = 1, 2, 3$, defined in Chapter 3 as strongly regular graphs. The latter are constituent graphs of the integral distance graph over the finite field $\mathbb{F}_q$ with $q \equiv 1 \pmod 4$. We also determine the strong regularity of the integral distance graph for each case of q in two dimensions.

Finally, we consider the case of the higher dimension. In [32], it was verified for small values using computer calculations that integral distance graphs of orders $p \leq 2029$, $p \leq 283$, $p \leq 97$, $p \leq 59$, $p \leq 31$ for $m = 3, 4, 5, 6, 7$; respectively, are strongly regular.

Inevitably, it was conjectured that all integral distance graphs of even dimensions are strongly regular. In this chapter, we prove this conjecture.

4.1 Constituent graphs of $\mathfrak{G}_{2,q}$ as strongly regular graphs

To show that the graph $\mathfrak{G}_{2,q}$ of integral distances is a strongly regular graph, we begin with the case of $q \equiv 1 \pmod 4$ in hyperbolic coordinates. In this case, we shall begin with constituent graphs $\Gamma_i = \mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2$, defined in Chapter 3.

In addition, we consider another graph $\Gamma_3 = \mathrm{Cay}(\mathbb{F}_q^2, S_3)$ with $S_3 = \mathbb{F}_q^2 \setminus (S \cup \{\mathbf{0}\})$, where $S = S_1 \cup S_2$. Obviously, Γ_3 is the complement of the integral distance graph Γ defined in Chapter 3, and thus a Cayley graph by Theorem 2.7.

To show that Γ is strongly regular, first we show that each constituent graph Γ_i is strongly regular for $i = 1, 2$. After this, we show that Γ is strongly regular. It will therefore follow that Γ_3 is strongly regular since it is the complement of Γ by Theorem 2.3. Because of the isomorphism established in Lemma 3.9, we will have that $\mathfrak{G}_{2,q}$ with $q \equiv 1 \pmod 4$, is a strongly regular graph. Finally, we show the same for $\mathfrak{G}_{2,q}$ with the remaining case $q \equiv 3 \pmod 4$.

Now we begin with the constituent graph $\Gamma_1 = \mathrm{Cay}(\mathbb{F}_q^2, S_1)$.

Theorem 4.1 *Let $\Gamma_1 = \mathrm{Cay}(\mathbb{F}_q^2, S_1)$ be a constituent graph of an integral distance graph Γ with $S_1 = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*)$, $q \equiv 1 \pmod 4$. Then Γ_1 is a strongly regular graph with parameters $(v, k, \lambda, \mu) = (q^2, 2(q-1), q-2, 2)$.*

Proof. Obviously, $v = |\mathbb{F}_q| = q^2$. To evaluate the degree $k = |S_1|$ of each vertex in Γ_1, we have $S_1 = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*)$. The sets $(\mathbb{F}_q^*, 0)$ and $(0, \mathbb{F}_q^*)$ are disjoint, and each of them is of size $q - 1$. Thus it follows that $k = |S_1| = 2(q-1)$.

To calculate λ, we first consider the vertex $(0, 0)$ and its neighbor $(x, 0)$ with $x \in \mathbb{F}_q^*$ since Γ_1 is Cayley, and hence by Theorem 2.5 vertex-transitive. Let $\mathbf{s} \in \mathbb{F}_q^2$ be the common neighbor to $(0, 0)$ and $(x, 0)$. Since $\mathbf{s} \in S_1$, then it is of the form $(s, 0)$ or $(0, s)$ because it is adjacent to $(0, 0)$.

In addition, $\mathbf{s} = (x, 0) + \mathbf{s}_1$ for some $\mathbf{s}_1 \in S_1$ since Γ_1 is Cayley. Either $\mathbf{s}_1 = (s_1, 0)$ or $\mathbf{s}_1 = (0, s_1)$; i.e., $\mathbf{s} = (x + s_1, 0)$ or $\mathbf{s} = (x, s_1) \notin S_1$. Thus the common neighbor to $(0, 0)$ and $(x, 0)$ can only be of the form $\mathbf{s} = (s, 0)$ with $s \in \mathbb{F}_q^* \setminus \{x\}$, and hence $\lambda = q - 2$.

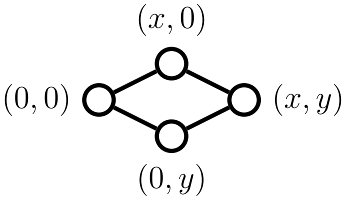
To evaluate μ, we consider the non-adjacent vertices $(0, 0)$ and (x, y), where $x, y \in \mathbb{F}_q^*$.

We have that $(x, y) = \mathbf{s}_i + \mathbf{s}_j$, $i, j = 1, 2$. If $\mathbf{s}_i, \mathbf{s}_j \in (\mathbb{F}_q^*, 0)$, then $(x, y) = (x', 0)$ for some $x' \in \mathbb{F}_q^*$. Similarly, if $\mathbf{s}_i, \mathbf{s}_j \in (0, \mathbb{F}_q^*)$, then $(x, y) = (0, y')$ for some $y' \in \mathbb{F}_q^*$. To each case, (x, y) becomes a neighbor of $(0, 0)$ because either $x = 0$ or $y = 0$.

Thus we should have, without loss of generality, $(x, y) = \mathbf{s}_i + \mathbf{s}_j$ with $\mathbf{s}_i \in (\mathbb{F}_q^*, 0)$ and $\mathbf{s}_j \in (0, \mathbb{F}_q^*)$, $i, j = 1, 2$.

In the following diagram, it follows that the common neighbors to non-adjacent vertices $(0, 0)$ and (x, y), with x and y non-zero fixed elements of $\mathbb{F}_q$, are $(x, 0)$ and

$(0, y)$. Hence $\mu = 2$ elements.



Therefore the result follows. $\square$

For the constituent graph $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$ with $S_2 = \{(x, y) \in \mathbb{F}_q^2 : xy \in \square_q^*\}$, since $v = |\mathbb{F}_q^2| = q^2$, each of the remaining parameters is dealt with separately in the following lemmas.

Lemma 4.2 *Let* $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$ *be the constituent graph of the two-dimensional integral distance graph* Γ *for* $q \equiv 1 \pmod 4$ *with* S_2 *defined as in* Equation (3.2). *Then the degree of* Γ_2 *is* $\dfrac{(q-1)^2}{2}$.

Proof. Let $\deg \Gamma_2 = k$. This is the same as the size of the Cayley set S_2 to be evaluated.

Because of the isomorphism of Cayley graphs $\mathrm{Cay}(\mathbb{F}_q^2, \mathbb{S})$ and $\mathrm{Cay}(\mathbb{F}_q^2, \mathbb{S}^{\phi})$, where a switch to hyperbolic coordinates $\phi : (x, y) \mapsto (x + \omega y, x - \omega y)$, $\omega^2 = -1$, is an automorphism of the vector space $\mathbb{F}_q^2$, it follows that the size of S_2 is the same as the size of $\{(x, y) \in \mathbb{F}_q^2 : N(x, y) \in \square_q^*\}$ equal to $\frac{1}{2}(q-1)^2$ by Corollary 2.21 and Theorem 2.9 in Chapter 2. Thus $k = |S_2| = \frac{1}{2}(q-1)^2$. $\square$

Because of vertex-transitivity, to determine λ and μ, we focus on the neighborhood of the vertex $(0, 0)$.

Lemma 4.3 *Let* (α, β) *be the neighbor of the vertex* $(0, 0)$ *in* Γ_2.

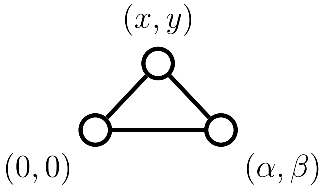
Then the number of common neighbors to $(0, 0)$ *and* (α, β) *is*

$$\lambda = \frac{(q-1)(q-3)}{4} + 1.$$

Proof. Let (x, y) be a common neighbor to the adjacent vertices $(0, 0)$ and (α, β) in Γ_2.

From the hypothesis, it follows that $(\alpha, \beta) \in S_2$; i.e., $\alpha\beta \in \square_q^*$.

To evaluate the number λ of choices for (x, y) in $\mathbb{F}_q^2$, we have the following.



We have $(x, y) = (\alpha, \beta) + \mathbf{s}$, where $\mathbf{s} \in S_2$. In addition, $(x, y) \in S_2$; i.e., $xy \in \square_q^*$. It follows that $\mathbf{s} = (x - \alpha, y - \beta)$ and $(x - \alpha)(y - \beta) \in \square_q^*$.

Put $xy = a^2$, $(x - \alpha)(y - \beta) = b^2$, and $\alpha\beta = \gamma^2$; $a, b, \gamma \in \mathbb{F}_q^*$.

Then we have the system

$$\begin{aligned} xy &= a^2; &(4.1)\\ (x - \alpha)(y - \beta) &= b^2. &(4.2)\end{aligned}$$

which implies that

$$\begin{aligned} xy &= a^2; &(4.3)\\ xy - \beta x - \alpha y + \gamma^2 &= b^2. &(4.4)\end{aligned}$$

with $a^2 \neq 0$ and $b^2 \neq 0$. Substracting Equation (4.4) from Equation (4.3), we obtain

$$\beta x + \alpha y - \gamma^2 = a^2 - b^2; \tag{4.5}$$

and Equation 4.3 becomes

$$y = \frac{a^2}{x}. \tag{4.6}$$

Substituting Equation (4.6) in Equation (4.5) becomes

$$\beta x + \alpha\frac{a^2}{x} - \gamma^2 = a^2 - b^2 \Leftrightarrow \beta x^2 + \alpha a^2 - \gamma^2 x - x(a^2 - b^2) = 0;$$

which is equivalent to

$$\beta x^2 - (a^2 - b^2 + \gamma^2)x + \alpha a^2 = 0. \tag{4.7}$$

Put $A = \beta$, $B = -(a^2 - b^2 + \gamma^2)$, $C = \alpha a^2$, and $\Delta = B^2 - 4AC$.

Then

$$\Delta = (a^2 - b^2 + \gamma^2)^2 - 4a^2\gamma^2. \tag{4.8}$$

Equation (4.7) has solutions in $\mathbb{F}_q$ if and only if $\Delta \in \square_q$.

We have two cases: $\Delta = 0$ and $\Delta \in \square_q^*$. Note that to each ordered pair (a^2, b^2) corresponds two solutions for $\Delta \in \square_q^*$, and only one solution for $\Delta = 0$.

(a) $\Delta = 0$.

From Equation (4.8), we have $(a^2 - b^2 + \gamma^2)^2 = 4a^2\gamma^2 \Rightarrow a^2 - b^2 + \gamma^2 = \pm 2a\gamma$, $a, \gamma \in \mathbb{F}_q^*$, and $x = -\dfrac{B}{2a}$.

We must have the two following sub-cases: (i) $a^2 = b^2$

Equation (4.8) becomes $\Delta = \gamma^4 - 4a^2\gamma^2 = \gamma^2(\gamma^2 - 4a^2)$, which implies that

$$\gamma^2 - 4a^2 = 0 \Leftrightarrow a^2 = \frac{\gamma^2}{4} \text{ since } \gamma^2 \neq 0.$$

Then $x = \dfrac{\gamma^2}{2\beta} = \dfrac{\alpha}{2}$; and $y = \dfrac{a^2}{x} = \dfrac{\gamma^2}{4}\dfrac{2}{\alpha} \Rightarrow y = \dfrac{\beta}{2}$.

Thus we have only one solution $\left(\dfrac{\alpha}{2}, \dfrac{\beta}{2}\right)$.

(ii) $a^2 \neq b^2$.

For this case we have

$$x = -\frac{B}{2A} = \frac{a^2 - b^2 + \gamma^2}{2\beta} = \pm\frac{2a\gamma}{2\beta} = \pm\frac{a\gamma}{\beta};$$

and

$$y = \frac{a^2}{x} = \frac{2a^2\beta}{a^2 - b^2 + \gamma^2} = \pm\frac{2a^2\beta}{2a\gamma} = \pm\frac{a\beta}{\gamma}$$

with $a \in \mathbb{F}_q^*$, $\pm\dfrac{a\gamma}{\beta} \neq \dfrac{\alpha}{2}$, and $\pm\dfrac{a\beta}{\gamma} \neq \dfrac{\beta}{2}$; i.e., $a \neq \pm\dfrac{\gamma}{2}$ and hence $q - 3$ solutions.

Summing up all obtained solutions for $\Delta = 0$, we get $q - 2$ solutions.

(b) $\Delta \in \square_q^*$.

Here, Equation (4.8) becomes

$$\Delta = (a^2 - b^2 + \gamma^2)^2 - 4a^2\gamma^2 = c^2 \tag{4.9}$$

for some $c \in \mathbb{F}_q^*$. With this case, we must also consider the two following sub-cases for a^2 and b^2.

(i) $a^2 = b^2$.

Equation (4.9) becomes $\gamma^4 - 4a^2\gamma^2 = c^2$.

Then we have $\gamma^2(\gamma^2 - 4a^2) = c^2 \Leftrightarrow \gamma^2 - 4a^2 = \dfrac{c^2}{\gamma^2}$.

Put $d^2 = \dfrac{c^2}{\gamma^2} \in \square_q^*$.

Then

$$\begin{aligned}\gamma^2 - 4a^2 = d^2 \Leftrightarrow 4a^2 &= \gamma^2 - d^2;\\ \Leftrightarrow \left(\frac{\gamma - d}{2a}\right)\left(\frac{\gamma + d}{2a}\right) &= 1.\end{aligned}$$

Let $t = \dfrac{\gamma + d}{2a}$ and $t^{-1} = \dfrac{\gamma - d}{2a}$.

Then $t + t^{-1} = \dfrac{\gamma}{a}$ and $t - t^{-1} = \dfrac{d}{a}$.

We obtain

$$a = \frac{\gamma}{t + t^{-1}} = \frac{\gamma t}{t^2 + 1}; t \neq 0 \text{ and } t^2 \neq \pm 1;$$

and

$$d = a(t - t^{-1}) = \gamma\left(\frac{t^2 - 1}{t^2 + 1}\right); t^2 \neq \pm 1.$$

Let $X = \left\{i : \rho^i = \gamma\left(1 - \dfrac{2}{t^2 + 1}\right); t^2 \neq 0; t^2 \neq \pm 1\right\}$.

Clearly, $|X| = |\square_q^*| - 2 = \dfrac{q-1}{2} - 2 = \dfrac{q-5}{2}$, and

$$\begin{aligned}\left|\left\{d^2 : d = \gamma\left(1 - \frac{2}{t^2 + 1}\right); t^2 \neq 0; t^2 \neq \pm 1\right\}\right| &= |\{2i : i \in X\}|\\ &= \frac{1}{2}|X|\\ &= \frac{q-5}{4}.\end{aligned}$$

Thus we obtain for this sub-case $2\left(\dfrac{q-5}{4}\right) = \dfrac{q-5}{2}$ solutions since $\Delta \in \square_q^*$ and hence there is no solution.

(ii) $a^2 \neq b^2$.

This sub-case is also further subdivided in the following sub-cases.

(1) $(a^2 - b^2 - \gamma^2)^2 = 0$ or $4a^2\gamma^2 = 0$.

For $4a^2\gamma^2 = 0$, we have a contradiction since $a^2, \gamma^2 \in \Box_q^*$.

For $(a^2 - b^2 + \gamma^2)^2 = 0 \Leftrightarrow a^2 - b^2 + \gamma^2 = 0$, we have

$$-4a^2\gamma^2 = c^2 \Leftrightarrow a^2 = -\frac{c^2}{4\gamma^2}.$$

Then

$$\begin{aligned} a^2 - b^2 + \gamma^2 = 0 &\Leftrightarrow a^2 = b^2 - \gamma^2; \\ &\Leftrightarrow 1 = \left(\frac{b-\gamma}{a}\right)\left(\frac{b+\gamma}{a}\right). \end{aligned}$$

Let $t = \dfrac{b+\gamma}{a}$. Then $t^{-1} = \dfrac{b-\gamma}{a}$. We have

$$t + t^{-1} = \frac{2b}{a} \text{ and } t - t^{-1} = \frac{2\gamma}{a};$$

which simplifies to

$$a = \frac{2\gamma}{t - t^{-1}} = \frac{2\gamma t}{t^2 - 1};\ t \neq 0;\ t^2 \neq 1;$$

and

$$b = \frac{a}{2}(t + t^{-1}) = \gamma\left(\frac{t^2+1}{t^2-1}\right);\ t^2 \neq \pm 1.$$

Let $X = \left\{ i : \rho^i = \gamma\left(1 + \dfrac{2}{t^2-1}\right); t^2 \neq \pm 1; t^2 \neq 0 \right\}$.

Clearly, $|X| = |\Box_q^*| - 2 = \dfrac{q-1}{2} - 2 = \dfrac{q-5}{2}$, and

$$\begin{aligned} \left| \left\{ b^2 : b = \gamma\left(1 + \frac{2}{t^2-1}\right); t^2 \neq \pm 1; t^2 \neq 0 \right\} \right| &= |\{2i : i \in X\}|; \\ &= \frac{1}{2}|X| \\ &= \frac{q-5}{4}. \end{aligned}$$

(2) $(a^2-b^2+\gamma^2)^2 \neq 0$ and $4a^2\gamma^2 \neq 0$. Here, Equation (4.9) leads to

$$\begin{aligned}(a^2-b^2+\gamma^2)^2-4a^2\gamma^2=c^2 &\Leftrightarrow (a^2-b^2+\gamma^2-2a\gamma)(a^2-b^2+\gamma^2+2a\gamma)=c^2;\\ &\Leftrightarrow [(a-\gamma)^2-b^2][(a+\gamma)^2-b^2]=c^2;\\ &\Leftrightarrow (a-b-\gamma)(a+b-\gamma)(a-b+\gamma)(a+b+\gamma)=c^2.\end{aligned}$$

Put $c^2=k^2l^2$, $k^2 \neq 0$, and $l^2 \neq 0$.

Then we have

$$\begin{gathered}(a+b-\gamma)(a-b-\gamma)(a+b+\gamma)(a-b+\gamma)=k^2l^2;\\ \Leftrightarrow \left(\frac{a+b-\gamma}{k}\right)\left(\frac{a-b-\gamma}{l}\right)\left(\frac{a+b+\gamma}{k}\right)\left(\frac{a-b+\gamma}{l}\right)=1.\end{gathered}$$

Let $t=\left(\frac{a+b+\gamma}{k}\right)\left(\frac{a-b+\gamma}{l}\right)$, and $t^{-1}=\left(\frac{a+b-\gamma}{k}\right)\left(\frac{a-b-\gamma}{l}\right)$.

Put $t=uv$ with $u=\dfrac{a+b+\gamma}{k}$ and $v=\dfrac{a-b+\gamma}{l}$.

Then $t^{-1}=u^{-1}v^{-1}$ with $u^{-1}=\dfrac{a+b-\gamma}{k}$, and $v^{-1}=\dfrac{a-b-\gamma}{l}$. It follows that

$$\begin{gathered}u+u^{-1}=\frac{2(a+b)}{k} \text{ and } u-u^{-1}=\frac{2\gamma}{k};\\ v+v^{-1}=\frac{2(a-b)}{l} \text{ and } v-v^{-1}=\frac{2\gamma}{l}.\end{gathered}$$

We obtain

$$a+b = \frac{k}{2}(u+u^{-1}); \tag{4.10}$$

$$a-b = \frac{l}{2}(v+v^{-1}); \tag{4.11}$$

and

$$k=\frac{2\gamma}{u-u^{-1}}; \quad l=\frac{2\gamma}{v-v^{-1}} \tag{4.12}$$

with $u,v \notin \{0,1\}$.

By inserting Equations (4.12) into Equations (4.10) and (4.11), we obtain

$$a+b = \gamma\left(\frac{u^2+1}{u^2-1}\right)=\gamma\left(1+\frac{2}{u^2-1}\right); \tag{4.13}$$

$$a-b = \gamma\left(\frac{v^2+1}{v^2-1}\right)=\gamma\left(1+\frac{2}{v^2-1}\right); \tag{4.14}$$

$$\tag{4.15}$$

where $u^2 \neq \pm 1$ and $v^2 \neq \pm 1$.

Adding Equation (4.14) to Equation (4.13) and dividing both sides by 2, we get

$$a = \gamma \left(1 + \frac{1}{u^2 - 1} + \frac{1}{v^2 - 1} \right). \tag{4.16}$$

Substracting Equation (4.14) from Equation (4.13) and dividing both sides by 2, we obtain

$$b = \gamma \left(\frac{1}{u^2 - 1} - \frac{1}{v^2 - 1} \right). \tag{4.17}$$

Note that the last two equations, (4.16) and (4.17), are valid only for $u^2, v^2 \notin \{0, \pm 1\}$; $v^2 \neq u^{\pm 2}$. We must also set up conditions for u^2 and v^2 so that $a^2 \neq 0$ and $b^2 \neq 0$. This simplifies to

$$1 + \frac{1}{u^2 - 1} + \frac{1}{v^2 - 1} \neq 0 \text{ and } \frac{1}{u^2 - 1} - \frac{1}{v^2 - 1} \neq 0.$$

Solving each of the above inequalities for v^2 gives us solutions $v^2 \neq u^{\pm 2}$.

Thus $a^2, b^2 \in \square_q^*$ if and only if $v^2 \neq u^{\pm 2}$.

Let $A = \left\{ (a, b) : a = \gamma \left(1 + \frac{1}{u^2 - 1} + \frac{1}{v^2 - 1} \right); b = \gamma \left(\frac{1}{u^2 - 1} - \frac{1}{v^2 - 1} \right) \right\}$,

with $u^2, v^2 \notin \{0, \pm 1\}$; $v^2 \neq u^{\pm 2}$, and $\gamma \in \mathbb{F}_q^*$.

By counting we observe that

$$\begin{aligned}
|A| &= |\{(u^2, v^2) \in (\square_q)^2 : u^2, v^2 \notin \{0, \pm 1\}; v^2 \neq u^{\pm 2}\}| \\
&= |\{(u^2, v^2) \in (\square_q)^2 : u^2, v^2 \notin \{0, \pm 1\}\}| - |\{(u^2, u^{\pm 2}) : u^2 \notin \{0, \pm 1\}\}| \\
&= |\{u^2 \in \square_q^* : u^2 \neq \pm 1\}| \cdot |\{v^2 \in \square_q^* : v^2 \neq \pm 1\}| \\
&\quad - |\{(u^2, u^2); (u^2, u^{-2}) : u^2 \notin \{0, \pm 1\}\}| \\
&= \left(\frac{q+1}{2} - 3 \right) \left(\frac{q+1}{2} - 3 \right) - 2 \left(\frac{q+1}{2} - 3 \right) \\
&= \left(\frac{q-5}{2} \right)^2 - 2 \left(\frac{q-5}{2} \right) \\
&= \left(\frac{q-5}{2} \right) \left(\frac{q-9}{2} \right).
\end{aligned}$$

Let $B = \{(a^2, b^2) : (a, b) \in A\}$.

Then

$$\begin{aligned}|B| &= |\{(2i,2j) : (\rho^i,\rho^j) \in A\}| \\ &= \frac{1}{2}|\{(i,2j) : (\rho^i,\rho^j) \in A\}| \\ &= \frac{1}{4}|\{(i,j) : (\rho^i,\rho^j) \in A\}| \\ &= \frac{1}{4}|A|.\end{aligned}$$

Thus $|B| = \left(\frac{q-5}{4}\right)\left(\frac{q-9}{4}\right)$.

Since $\Delta = (a-b-\gamma)(a+b-\gamma)(a-b+\gamma)(a+b+\gamma)$, we have the symmetry of Δ; i.e., the same is obtained by swapping a and b and thus a^2 and b^2. It follows that we obtain $2\left[\left(\frac{q-5}{4}\right)\left(\frac{q-9}{4}\right)+\left(\frac{q-5}{4}\right)\right] = 2\left(\frac{q-5}{4}\right)^2$ solutions for ordered pairs (a^2, b^2) by combining (1) and (2), and hence $4\left(\frac{q-5}{4}\right)^2 = \left(\frac{q-5}{2}\right)^2$ solutions whenever $\Delta \in \square_q^*$.

Therefore, combining all cases for $\Delta \in \square_q$, we obtain

$$\begin{aligned}\lambda &= q-2+\frac{q-5}{2}+\left(\frac{q-5}{2}\right)^2 \\ &= \frac{4q-8+2q-10+q^2-10q+25}{4} \\ &= \frac{q^2-4q+7}{4} \\ &= \frac{(q-1)(q-3)}{4}+1.\end{aligned}$$

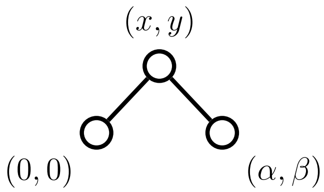
□

Lemma 4.4 *Let $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$ and let (α,β) be a non-adjacent vertex to $(0,0)$ in Γ_2.*

Then the number of common neighbours to $(0,0)$ and (α,β) is given by

$$\mu = \frac{(q-1)(q-3)}{4}.$$

Proof. Consider again (x, y) the common neighbour to both $(0, 0)$ and (α, β). Again, to evaluate the number μ of choices of (x, y) in Γ_2, we consider the following.



Here, $(x, y) = (\alpha, \beta) + \mathbf{s} \Leftrightarrow \mathbf{s} = (x - \alpha, y - \beta)$ with $(x, y); \mathbf{s} \in S_2$ and $(\alpha, \beta) \notin S_2$; i.e., $xy, (x - \alpha)(y - \beta) \in \square_q^*$ and $\alpha\beta \notin \square_q^*$.

For $\alpha\beta \notin \square_q^*$, we consider two cases: $\alpha\beta = 0$ and $\alpha\beta \notin \square_q$.

(a) $\alpha\beta = 0$; i.e., $\alpha = 0$ or $\beta = 0$.

Take $\beta = 0$. The system of Equations (4.3) and (4.4) becomes

$$\begin{aligned} xy &= a^2; && (4.18)\\ (x - \alpha)y &= b^2. && (4.19) \end{aligned}$$

Substracting Equation (4.19) from Equation (4.18), we obtain

$$\alpha y = a^2 - b^2. \qquad (4.20)$$

We consider the following sub-cases for non-zero a^2 and b^2:

(i) $a^2 = b^2$. Here, Equation (4.20) simplifies to $\alpha y = 0 \Leftrightarrow y = 0$ since $\alpha \neq 0$. So $(x, y) \notin S_2$, a contradiction, and thus we have no solution.

(ii) $a^2 \neq b^2$. From Equation (4.20), we get $y = \dfrac{a^2 - b^2}{\alpha}$ and so $x = \dfrac{a^2}{y} = \dfrac{a^2\alpha}{a^2 - b^2}$ (Equation (4.18)).

Thus we have solutions of the form $\left(\dfrac{a^2\alpha}{a^2 - b^2}, \dfrac{a^2 - b^2}{\alpha}\right)$, and hence

$\left(\dfrac{q-1}{2}\right)^2 - \left(\dfrac{q-1}{2}\right) = \left(\dfrac{q-1}{2}\right)\left(\dfrac{q-3}{2}\right)$ solutions.

Therefore $\mu = \dfrac{(q-1)(q-3)}{4}$ is the number of common neighbours to non-adjacent vertices in Γ_2 for $\alpha\beta = 0$.

(b) $\alpha\beta \neq 0$; i.e. $\alpha\beta \notin \square_q$. Put $\alpha\beta = k$, $k \notin \square_q$.

Then we have from Equations (4.1) and (4.2) the system of equations

$$\begin{aligned} xy &= a^2; & (4.21)\\ xy - \beta x - \alpha y + k &= b^2. & (4.22) \end{aligned}$$

Substracting Equation (4.22) from Equation (4.21) simplifies to

$$\beta x + \alpha y - k = a^2 - b^2. \tag{4.23}$$

Additionally we must have from (4.21)

$$y = \frac{a^2}{x}. \tag{4.24}$$

Then substituting Equation (4.24) in Equation (4.23) gives us

$$\beta x + \alpha \frac{a^2}{x} - k = a^2 - b^2 \Leftrightarrow \beta x^2 + \alpha a^2 - kx - x(a^2 - b^2) = 0;$$

which is equivalent to

$$\beta x^2 - (a^2 - b^2 + k)x + \alpha a^2 = 0. \tag{4.25}$$

Put $A = \beta$, $B = -(a^2 - b^2 + k)$, $C = \alpha a^2$, and $\Delta = B^2 - 4AC$.

Then,

$$\Delta = (a^2 - b^2 + k)^2 - 4\alpha\beta a^2 = (a^2 - b^2 + k)^2 - 4a^2 k. \tag{4.26}$$

We examine different cases for $\Delta \in \square_q$; namely, $\Delta = 0$ and $\Delta \in \square_q^*$, so that Equation (4.25) have solutions in $\mathbb{F}_q$.

(i) $\Delta = 0$.

Here we have from Equation (4.26) $(a^2 - b^2 + k)^2 = 4a^2 k \notin \square_q$, which is a contradiction and thus there is no solution for $\Delta = 0$.

(ii) $\Delta \neq 0$; i.e., $\Delta \in \square_q^*$.

From Equation (4.26), we have for some $c \neq 0$

$$(a^2 - b^2 + k)^2 - 4a^2 k = c^2. \tag{4.27}$$

Now for this last case, we have to examine the two following sub-cases.

(1) $a^2 = b^2$.

This leads to (Equation (4.27)) $k^2 - 4a^2 k = c^2$ so that $\Delta \in \square_q$.

Let $X = \{i : \rho^i = k^2 - 4a^2k; a^2 \neq 0\}$, k fixed. Clearly, $|X| = \dfrac{q-1}{2}$.

Put $c = \rho^j$ for some j. Then $\rho^i = c^2 \Rightarrow i = 2j$.

Thus

$$\begin{aligned} |\{\rho^i = c^2 : i \in X\}| &= |\{2j : j \in X\}| \\ &= \frac{1}{2}|X| \\ &= \frac{q-1}{4}. \end{aligned}$$

Recall from Lemma 4.3 that to each value of $\Delta \in \Box_q^*$ corresponds exactly two solutions. Thus we obtain $2\left(\dfrac{q-1}{4}\right) = \dfrac{q-1}{2}$ solutions.

(2) $a^2 \neq b^2$.

For this last case, Equation (4.27) cannot be factorized for $k \notin \Box_q$. Let (α, β) an element of $\mathbb{F}_q^2 \setminus \{(0,0)\}$, be adjacent to (x, y), which is in turn adjacent to $(0,0)$. That is, $(\alpha, \beta) \in S_2$ or $(\alpha, \beta) \notin S_2$; i.e., $\alpha\beta \in \mathbb{F}_q$. Then $(x, y) = (\alpha, \beta) + \mathbf{s}$ for some $\mathbf{s} \in S_2$ and $(x, y) \in S_2$; i.e., $xy \in \Box_q^*$.

It follows that $(\alpha, \beta) \in \mathbb{F}_q^2$; $(\alpha, \beta) \neq (0,0)$; and $(\alpha, \beta) \neq (x, y)$.

Let $A = \{(a^2, b^2) : 0 \neq a^2 \neq b^2 \neq 0\}$.

Then clearly, $|A| = \left(\dfrac{q-1}{2}\right)^2 - \left(\dfrac{q-1}{2}\right) = \left(\dfrac{q-1}{2}\right)\left(\dfrac{q-3}{2}\right)$.

For each case of A we have

$\Delta(a^2, b^2, \alpha\beta) \in \Box_q^*$; $\Delta(a^2, b^2, \alpha\beta) = 0$; and $\Delta(a^2, b^2, \alpha\beta) \notin \Box_q$.

In fact, $\Delta(a^2, b^2, \alpha\beta) = 0$ if and only if $\alpha\beta \in \Box_q^*$; i.e., $(\alpha, \beta) \in S_2$.

Let $A_0 = \{(a^2, b^2) \in A : \Delta(a^2, b^2, \alpha\beta) = 0\}$.

From the proof for λ in S_2 by Lemma 4.3, we have $|A_0| = q - 3$.

Let $A^* = A \setminus A_0 = \{(a^2, b^2) \in A : \Delta(a^2, b^2, \alpha\beta) \neq 0\}$.

Then

$$\begin{aligned}|A^*| = |A \setminus A_0| &= |A| - |A_0| \\ &= \left(\frac{q-1}{2}\right)\left(\frac{q-3}{2}\right) - (q-3) \\ &= \left(\frac{q-3}{2}\right)\left(\frac{q-1}{2} - 2\right) \\ &= \left(\frac{q-3}{2}\right)\left(\frac{q-5}{2}\right)\end{aligned}$$

and $B = \{(a^2, b^2) \in A^* : (\alpha, \beta) \in S_2; (x, y)_{(a^2,b^2)} \in S_2\}$.

As λ was determined in Lemma 4.3, we have $|B| = 2\left(\frac{q-5}{4}\right)^2$ because of the symmetry of Δ for λ.

Then $A^* \setminus B$ consists of elements corresponding to $(x, y) \in S_2$, but $(\alpha, \beta) \notin S_2$. Thus

$$\begin{aligned}|A^* \setminus B| &= |A^*| - |B| \\ &= \left(\frac{q-3}{2}\right)\left(\frac{q-5}{2}\right) - 2\left(\frac{q-5}{2}\right)^2 \\ &= \left(\frac{q-5}{4}\right)\left(q - 3 - \frac{q-5}{2}\right) \\ &= \left(\frac{q-5}{4}\right)\left(\frac{q-1}{2}\right).\end{aligned}$$

Hence this corresponds to exactly $2\left(\frac{q-5}{4}\right)\left(\frac{q-1}{2}\right) = \left(\frac{q-5}{2}\right)\left(\frac{q-1}{2}\right)$ solutions for $0 \neq a^2 \neq b^2 \neq 0$.

Because of vertex-transitivity of the graph in question, the number μ of common neighbours to non adjacent vertices in Γ_2 is therefore

$$\begin{aligned}\mu &= \frac{q-1}{2} + \left(\frac{q-5}{2}\right)\left(\frac{q-1}{2}\right) \\ &= \left(\frac{q-1}{2}\right)\left(\frac{q-5}{2} + 1\right) \\ &= \frac{(q-1)(q-3)}{4}.\end{aligned}$$

□

Summing up all results for Γ_2, we have now the strong regularity of Γ_2 in the following terms.

Theorem 4.5 *Let* $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$*, where* $S_2 = \{(x,y) \in \mathbb{F}_q^2 : xy \in \Box_q^*\}$.
Then Γ_2 *is strongly regular with parameters*

$$(v, k, \lambda, \mu) = \left(q^2, \frac{(q-1)^2}{2}, \frac{(q-1)(q-3)}{4} + 1, \frac{(q-1)(q-3)}{4}\right).$$

Proof. In this case, $\mathbb{F}_q^2$ is a vertex set with size q^2. Thus $v = |\mathbb{F}_q^2| = q^2$. For the remaining parameters k, λ, and μ; the result follows from Lemma 4.2, Lemma 4.3, and Lemma 4.4. □

In order to show that the integral distance graph $\mathfrak{G}_{2,q}$ is a strongly regular graph for $q \equiv 1 \pmod 4$, we must use the above results for Γ_1 and Γ_2. As alluded to, it is sufficient to show that the graph $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$ with $S = S_1 \cup S_2$ is a strongly regular graph since $\mathfrak{G}_{2,q}$ is isomorphic to $\mathrm{Cay}(\mathbb{F}_q^2, S)$ for $q \equiv 1 \pmod 4$. (See Chapter 3).

Now we shall determine all the four parameters of Γ as was done with Γ_2 in the following lemmas.

Lemma 4.6 *Let* $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$*, where* $S = S_1 \cup S_2$*. Then*

$$\deg \Gamma = \frac{(q-1)(q+3)}{2}.$$

Proof. Put $k = \deg \Gamma$.

In fact, $S = S_1 \cup S_2 = \{(x,y) \in (\mathbb{F}_q^2) \setminus \{(0,0)\} : xy \in \Box_q\}$ and $v = |\mathbb{F}_q^2| = q^2$. Clearly, S is a disjoint union of S_1 and S_2 since we cannot have $xy \in \Box_q^*$ and $xy = 0$ at the same time.

From Theorem 4.1 and Lemma 4.2, we have $|S_1| = 2(q-1)$ and $|S_2| = \dfrac{(q-1)^2}{2}$.

Thus

$$\begin{aligned} k = |S| &= |S_1 \cup S_2| \\ &= |S_1| + |S_2| \\ &= 2(q-1) + \frac{(q-1)^2}{2} \\ &= (q-1)\left(2 + \frac{q-1}{2}\right) \\ &= \frac{(q-1)(q+3)}{2}. \end{aligned}$$

□

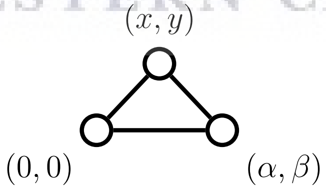
Following a similar argument as that used for Γ_2, we shall focus again on the neighborhood of the vertex $(0,0)$ because of vertex-transitivity of Γ to determine λ and μ.

Lemma 4.7 *Let (α,β) be a neighbor of the vertex $(0,0)$ in $\Gamma = \mathrm{Cay}(\mathbb{F}_q, S)$ with $S = S_1 \cup S_2$.*

Then the number of common neighbors to the above vertices is given by

$$\lambda = \frac{(q+1)(q+3)}{4} - 3.$$

Proof. Let (x,y) be the common neighbor to both $(0,0)$ and (α,β) as shown in the following diagram.



Let us evaluate the number λ of choices for (x,y) in the above triangle.

We have $(x,y) = (\alpha,\beta) + \mathbf{s}$, where $(x,y); (\alpha,\beta); s \in S$; i.e., $xy, \alpha\beta, (x-\alpha)(y-\beta) \in \square_q$.

Let $a, b, \gamma \in \mathbb{F}_q$ such that $xy = a^2$, $(x-\alpha)(y-\beta) = b^2$, and $\alpha\beta = \gamma^2$.

Now we must examine the two cases for γ^2: (a) $\gamma^2 = 0$ and (b) $\gamma^2 \neq 0$.

(a) $\gamma^2 = 0$; i.e., $\alpha = 0$ or $\beta = 0$.

Take $\beta = 0$. From Equations (4.3) and (4.4), the system reduces again to Equations (4.18)-(4.19).

This case has also the following four sub-cases for a^2 and b^2 to be examined.

(i) $a^2 = b^2 = 0$.

This sub-case is related to Γ_1 and thus, by Theorem 4.1, we have $q-2$ solutions.

(ii) $a^2 \neq 0$ and $b^2 = 0$.

Now, Equation (4.18) and Equation (4.19) reduce to

$$\begin{aligned} xy &= a^2; \qquad (4.28)\\ (x-\alpha)y &= 0. \qquad (4.29)\end{aligned}$$

Equation (4.29) implies that $x - \alpha = 0$ or $y = 0$. Thus $x = \alpha$ since $xy = a^2 \neq 0$ and $y = \dfrac{a^2}{\alpha}$ from Equation (4.28). Hence we have solutions of the form $\left(\alpha, \dfrac{a^2}{\alpha}\right)$, and therefore $\dfrac{q-1}{2}$ solutions.

(iii) $a^2 = 0$ and $b^2 \neq 0$. To this case, Equation (4.18) and Equation (4.19) reduce to the system

$$\begin{aligned} xy &= 0; \qquad (4.30)\\ (x-\alpha)y &= b^2. \qquad (4.31)\end{aligned}$$

Equation (4.30) reduces immediately to $x = 0$ or $y = 0$. From Equation (4.31), we have

$$x = 0 \Rightarrow -\alpha y = b^2 \Leftrightarrow y = -\frac{b^2}{\alpha};$$

and

$$y = 0 \Rightarrow b^2 = 0, \text{ a contradiction.}$$

Thus we have solutions of the form $\left(0, -\dfrac{b^2}{\alpha}\right)$ and hence $\dfrac{q-1}{2}$ of them.

(iv) $a^2 \neq 0$ and $b^2 \neq 0$.

To this sub-case, we return back to Equations (4.18) and (4.19).

Now we have two sub-cases for a^2 and b^2: $a^2 = b^2$ and $a^2 \neq b^2$.

(1) $a^2 = b^2$.

Equation (4.18) and Equation (4.19) become

$$\begin{aligned} xy &= a^2; & (4.32)\\ (x-\alpha)y &= a^2. & (4.33)\end{aligned}$$

Substracting Equation (4.33) from Equation (4.32), we get

$$xy-(x-\alpha)y=0 \Leftrightarrow \alpha y=0 \Leftrightarrow y=0, \text{ a contradiction.}$$

Thus there are no solutions for this case.

(2) $0 \neq a^2 \neq b^2 \neq 0$.

Substracting Equation (4.19) from Equation (4.18), we obtain

$$\begin{aligned} xy-(x-\alpha)y=a^2-b^2 &\Leftrightarrow \alpha y=a^2-b^2\\ &\Leftrightarrow y=\frac{a^2-b^2}{\alpha}\end{aligned}$$

and

$$x=\frac{a^2}{y}=\frac{a^2\alpha}{a^2-b^2} \text{ (From Equation (4.34)).}$$

Thus we have solutions of the form $\left(\frac{a^2\alpha}{a^2-b^2}, \frac{a^2-b^2}{\alpha}\right)$ and hence

$$\left(\frac{q-1}{2}\right)^2-\left(\frac{q-1}{2}\right)=\left(\frac{q-1}{2}\right)\left(\frac{q-3}{2}\right) \text{ solutions.}$$

Therefore, summing up the obtained results from all cases (i), (ii), (iii), and (iv); we obtain for the case $\gamma^2=0$

$$\begin{aligned}\lambda &= q-2+2\left(\frac{q-1}{2}\right)+\left(\frac{q-1}{2}\right)\left(\frac{q-3}{2}\right)\\ &= 2q-3+\frac{q^2-4q+3}{4}\\ &= \frac{q^2+4q-9}{4}\\ &= \frac{(q+1)(q+3)}{4}-3.\end{aligned}$$

(b) $\gamma^2 \neq 0$.

To this last case, we shall use the system of Equations (4.3) and (4.4) that we used in Lemma 4.3. Similar to the previous case, for γ^2, we must examine again the four cases for a^2 and b^2.

(i) $a^2 = b^2 = 0$.

Using Equations (4.3) and (4.4) from Lemma 4.3, we have the system

$$\begin{aligned} xy &= 0; & (4.34)\\ xy - \beta x - \alpha y + \gamma^2 &= 0. & (4.35) \end{aligned}$$

Equation (4.35), taken from Equation (4.34), gives $\beta x + \alpha y - \gamma^2 = 0$. In addition, we have $x = 0$ or $y = 0$ from Equation (4.34). Then,

$$x = 0 \Rightarrow \alpha y - \gamma^2 = 0 \Leftrightarrow y = \frac{\gamma^2}{\alpha} = \beta;$$

and

$$y = 0 \Rightarrow \beta x - \gamma^2 = 0 \Leftrightarrow x = \frac{\gamma^2}{\beta} = \alpha.$$

Thus we get solutions of the form $(\alpha, 0)$ and $(0, \beta)$; and hence 2 solutions.

(ii) $a^2 = 0$ and $b = 0$.

Using the same equations as those used in (i), we obtain

$$\begin{aligned} xy &= a^2; & (4.36)\\ xy - \beta x - \alpha y + \gamma^2 &= 0. & (4.37) \end{aligned}$$

Equation (4.37) becomes $(x - \alpha)(y - \beta) = 0$, giving $x = \alpha$ or $y = \beta$.

Then $x = \alpha \Rightarrow y = \dfrac{a^2}{\alpha}$ and $y = \beta \Rightarrow x = \dfrac{a^2}{\beta}$ by Equation (4.36).

Thus we obtain solutions of the form $\left(\alpha, \dfrac{a^2}{\alpha}\right)$; and $\left(\dfrac{a^2}{\beta}, \beta\right)$ with $a^2 \neq \gamma^2$ (since $\gamma^2 = \alpha\beta$ and $(x, y) \neq (\alpha, \beta)$); and hence $2\left(\dfrac{q-1}{2} - 1\right) = q - 3$ solutions.

(iii) $a^2 = 0$ and $b^2 \neq 0$. In addition, using the same equations as in the two previous cases, we have the system

$$\begin{aligned} xy &= 0; & (4.38)\\ xy - \beta x - \alpha y + \gamma^2 &= b^2. & (4.39) \end{aligned}$$

Equation (4.38) reduces to $x = 0$ or $y = 0$. So

$$x = 0 \Rightarrow -\alpha y + \gamma^2 = b^2 \Leftrightarrow y = \frac{\gamma^2 - b^2}{\alpha};$$

and

$$y = 0 \Rightarrow -\beta x + \gamma^2 = b^2 \Leftrightarrow y = \frac{\gamma^2 - b^2}{\beta}.$$

Thus we get solutions of the form $\left(0, \dfrac{\gamma^2 - b^2}{\alpha}\right)$; and $\left(\dfrac{\gamma^2 - b^2}{\beta}, 0\right)$ with $b^2 \neq \gamma^2$ (since $(x, y) \neq (0, 0)$); and hence $2\left(\dfrac{q-1}{2} - 1\right) = q - 3$ solutions.

(iv) $a \neq 0$ and $b \neq 0$.

This last case for a^2 and b^2 is related to Γ_2 and thus, by Lemma 4.3, we obtain $\dfrac{(q-1)(q-3)}{4} + 1$ solutions.

Finally, by summing up the results from all cases studied above for $\gamma^2 \neq 0$, we obtain

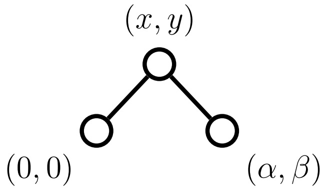
$$\begin{aligned}
\lambda &= 2 + 2(q-3) + \frac{(q-1)(q-3)}{4} + 1 \\
&= \frac{8 + 8q - 24 + q^2 - 4q + 7}{4} \\
&= \frac{q^2 + 4q - 9}{4} \\
&= \frac{(q+1)(q+3)}{4} - 3.
\end{aligned}$$

□

Lemma 4.8 *Let (α, β) be a non-adjacent vertex to $(0, 0)$ in $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$. Then the number of vertices adjacent to both $(0, 0)$ and (α, β) is given by*

$$\mu = \frac{(q+1)(q+3)}{4}.$$

Proof. Let (x, y) be any vertex adjacent to both $(0, 0)$ and (α, β) as shown in the following diagram.



The instance above shows that $(x, y) = (\alpha, \beta) + \mathbf{s}$ with $(x, y); \mathbf{s} \in S$ and $(\alpha, \beta) \notin S$; i.e., we have $xy, (x - \alpha)(y - \beta) \in \Box_q$ and $\alpha\beta \notin \Box_q$; i.e., $\alpha \neq 0$ and $\beta \neq 0$.

Put $xy = a^2$, $(x - \alpha)(y - \beta) = b^2$, and $\alpha\beta = k \notin \Box_q$; $a, b \in \mathbb{F}_q$.

In this case, we shall use Equation (4.21) and Equation (4.22) from Lemma 4.4. Now we have different cases for a^2 and b^2. Moreover, the cases $a^2 = b^2 = 0$ and $a^2 \neq 0, b^2 \neq 0$ are related to Γ_2, and hence they correspond to exactly 2 and $\dfrac{(q-1)(q-3)}{4}$ solutions respectively. So we shall deal only with the cases for exactly one of a^2 and b^2 being non-zero.

(a) $a^2 \neq 0, b^2 = 0$.

Using Equation (4.21) and Equation (4.22) from Lemma 4.4, we get the following system of equations

$$\begin{aligned} xy &= a^2; && (4.40) \\ xy - \beta x - \alpha y + k &= 0. && (4.41) \end{aligned}$$

Since $k = \alpha\beta$, Equation (4.41) reduces to $(x - \alpha)(y - \beta) = 0$; i.e., $x = \alpha$ or $y = \beta$.

Then from Equation (4.40), we obtain

$$x = \alpha \Rightarrow y = \frac{a^2}{\alpha} \text{ and } y = \beta \Rightarrow x = \frac{a^2}{\beta};$$

so that we have solutions of the forms $\left(\alpha, \dfrac{a^2}{\alpha}\right)$ and $\left(\dfrac{a^2}{\beta}, \beta\right)$; and thus $2\left(\dfrac{q-1}{2}\right) = q - 1$ solutions.

(b) $a^2 = 0, b^2 \neq 0$.

Using the same equations as those we used in (a), we have

$$\begin{aligned} xy &= 0; && (4.42) \\ xy - \beta x - \alpha y + k &= b^2. && (4.43) \end{aligned}$$

Equation (4.42) gives us $x = 0$ or $y = 0$, and hence we get

$$x = 0 \Rightarrow -\alpha y = b^2 - k \Leftrightarrow y = \frac{k - b^2}{\alpha};$$

or

$$y = 0 \Rightarrow -\beta x = b^2 - k \Leftrightarrow x = \frac{k - b^2}{\beta}.$$

This gives us solutions of the forms $\left(0, \frac{k-b^2}{\alpha}\right)$ and $\left(\frac{k-b^2}{\beta}, 0\right)$; and thus $2\left(\frac{q-1}{2}\right) = q - 1$ solutions.

Summing up all cases for μ, we obtain

$$\begin{aligned}\mu &= 2 + 2(q-1) + \frac{(q-1)(q-3)}{4} \\ &= \frac{8 + 8q - 8 + q^2 - 4q + 3}{4} \\ &= \frac{q^2 + 4q + 3}{4} \\ &= \frac{(q+1)(q+3)}{4}.\end{aligned}$$

□

Combining all the results obtained from the three last lemmas, we get the following.

Theorem 4.9 *Let* $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$, $q \equiv 1 \pmod 4$ *with* $S = S_1 \cup S_2$.
Then Γ *is a strongly regular graph with parameters*

$$(v, k, \lambda, \mu) = \left(q^2, \frac{(q-1)(q+3)}{2}, \frac{(q+1)(q+3)}{4} - 3, \frac{(q+1)(q+3)}{4}\right).$$

Proof. Again, it is clear that the vertex set $\mathbb{F}_q^2$ of Γ is of size $v = q^2$. For the remaining parameters, the result follows exactly from Lemma 4.6, Lemma 4.7, and Lemma 4.8. □

This completes the case $q \equiv 1 \pmod 4$.

Now we deduce the strong regularity of the remaining graph Γ_3. Finally, we summarize all the obtained results above to form a complete Boolean algebra of Cayley sets S_1 and S_2 for strong regularity of $\mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2$, in the following.

Corollary 4.10 *Let* $\Gamma_3 = \mathrm{Cay}(\mathbb{F}_q^2, S_3)$*, where* $S_3 = \mathbb{F}_q^2 \setminus (S \cup \{\mathbf{0}\})$*,* $S = S_1 \cup S_2$*. Then:*

(i) Γ_3 *is a strongly regular graph.*

(ii) *Given* $\langle S_1, S_2\rangle$*, a complete Boolean algebra of Cayley sets, the set* $\mathfrak{S} = \{T \in \langle S_1, S_2\rangle : \mathrm{Cay}(\mathbb{F}_q^2, T)$ *is strongly regular*$\}$ *forms a complete Boolean algebra of sets.*

Proof. (i) Consider $\Gamma_3 = \mathrm{Cay}(\mathbb{F}_q^2, S_3)$ with $S_3 = \mathbb{F}_q^2 \setminus (S_1 \cup S_2 \cup \{\mathbf{0}\})$, where $S_1 \cup S_2 = S$ defined above as a Cayley set for $\Gamma \cong \mathfrak{G}_{m,q}$ with $q \equiv 1 \pmod 4$. It follows that $\Gamma_3 = \mathrm{Cay}(\mathbb{F}_q^2, \mathbb{F}_q^2 \setminus (S \cup \{\mathbf{0}\})) = \Gamma^C$; and that it is a strongly regular graph with parameters $(v, v-k-1, v-2-2k+\mu, v-2k+\lambda)$ by Theorem 2.3. Using the parameters of Γ obtained from Theorem 4.9 in order to evaluate the parameters of Γ_3, it can easily be determined that

$$\begin{aligned} v-k-1 &= \frac{(q-1)^2}{2} \\ v-2-2k+\mu &= \frac{(q-1)(q-3)}{4}+1 \\ v-2k+\lambda &= \frac{(q-1)(q-3)}{4}. \end{aligned}$$

(ii) follows immediately from (i); by Theorems 4.1, 4.5 and 4.9; and by Proposition 2.3. $\Box$

For the other case $q \equiv 3 \pmod 4$, the constituent graphs similar to the previous case are only two: $\Gamma_1 = \mathrm{Cay}(\mathbb{F}_q^2, S_1)$ and $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$, with $S_1 = \{(x,y) \in \mathbb{F}_q^2 : N(x,y) \in \Box_q^*\}$ and $S_2 = \{(x,y) \in \mathbb{F}_q^2 : N(x,y) \notin \Box_q\}$; since $N(\mathbf{x}) = \mathbf{0}$ if and only if $\mathbf{x} = \mathbf{0}$.

Similar to the proof of the Corollary 4.10(i), it can be deduced that Γ_1 and Γ_2 are isomorphic. Moreover, $\Gamma_2 = \Gamma^C$ (since $S_2 = \mathbb{F}_q^2 \setminus (S_1 \cup \{\mathbf{0}\})$ by Proposition 2.4), and $|S_1| = |S_2|$ (to be seen in next Lemmas).

Thus $\Gamma_1 \cong \mathfrak{G}_{2,q}$ is self-complementary for $q \equiv 3 \pmod 4$, and hence we shall only consider the graph $\Gamma = \Gamma_1 = \mathrm{Cay}(\mathbb{F}_q^2, S^{(2)})$ with $S^{(2)} = S_1$. We have the following.

Lemma 4.11 *Let* $\mathfrak{G}_{2,q}$ *be the integral distance graph with* $q \equiv 3 \pmod 4$*. Then*

$$\deg\ \mathfrak{G}_{2,q} = \frac{q^2-1}{2}.$$

Proof. Put $k = \deg \mathfrak{G}_{2,q}$; i.e., the degree of each vertex of $\mathfrak{G}_{2,q}$.

By Theorem 3.8, $\mathfrak{G}_{2,q}$ is isomorphic to $\mathrm{Cay}(\mathbb{F}_q^2, S^{(2)})$, where $S^{(2)} = \{\mathbf{s} \in \mathbb{F}_q^2 : N(\mathbf{s}) \in \Box_q; s \neq 0\}$ a connecting set. Since $k = |S^{(2)}|$, it is sufficient to determine the value of $|S^{(2)}|$.

It is obvious that $N(s) = 0 \Leftrightarrow s = 0$ for $q \equiv 3 \pmod 4$, and hence

$$S^{(2)} = \{\mathbf{s} \in \mathbb{F}_q^2 : N(\mathbf{s}) \in \Box_q^*\}.$$

Let $S_1^{(2)} = \{\mathbf{s} \in \mathbb{F}_q^2 : N(\mathbf{s}) = 1\} = N^{-1}(1)$. By Lemma 2.22, we have that

$$|S_1^{(2)}| = |N^{-1}(1)| = q + 1 \text{ for } q \equiv 3 \pmod 4.$$

If $N(\mathbf{s}) = 1$, then $N(\lambda\mathbf{s}) = \lambda^2 \cdot 1 = \lambda^2, \lambda \neq 0$.

Let $S_\lambda^{(2)} = \{\lambda\mathbf{s} \in \mathbb{F}_q^2 : N(\lambda\mathbf{s}) = \lambda^2, \lambda \neq 0\}$. Then

$$\begin{aligned} |S_\lambda^{(2)}| &= |\lambda S_1^{(2)}| \\ &= |S_1^{(2)}| \\ &= q + 1. \end{aligned}$$

In our case, since $q \equiv 3 \pmod 4$, then $q^2 \equiv 1 \pmod 4$ and $\mathbb{F}_q^2 \cong \mathbb{F}_{q^2}$ is a field. Thus

$$\begin{aligned} k &= |S^{(2)}| \\ &= |\Box_q^*||S_1^{(2)}| \\ &= \left(\frac{q-1}{2}\right)(q+1) \\ &= \frac{q^2-1}{2} \\ &= |\Box_{q^2}^*|. \end{aligned}$$

□

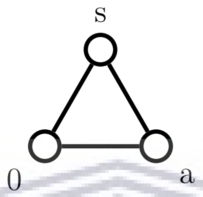
Since $\mathbb{F}_q^2$ is isomorphic to $\mathbb{F}_{q^2}$ for $q \equiv 3 \pmod 4$, we shall consider the elements of $\mathbb{F}_{q^2}$ as vertices of $\mathfrak{G}_{2,q}$. Because of the vertex-transitivity of $\mathfrak{G}_{2,q}$, we shall focus on the neighbors of the vertex 0 of $\mathbb{F}_{q^2}$ as we did for $q \equiv 1 \pmod 4$.

Lemma 4.12 *Let $a \in \mathbb{F}_{q^2}$ be the neighbor of the vertex $0 \in \mathbb{F}_{q^2}$ in $\mathfrak{G}_{2,q}$, $q \equiv 3 \pmod 4$.*

Then the number of vertices adjacent to both 0 and a is

$$\lambda = \frac{q^2-1}{4} - 1.$$

Proof. Let $s \in \mathbb{F}_{q^2}$ be a common neighbour to the two adjacent vertices 0 and a of $\mathfrak{G}_{2,q}$ as shown in the triangle below.



We have $s = a + s'$, where $a, s, s' \in S^{(2)} = \Box^*_{q^2}$.

Put $a = \alpha^2$, $s' = x^2$, and $s = y^2$; $\alpha^2 \neq 0$, $x^2 \neq 0$, and $y^2 \neq 0$. Then $s = a + s'$ implies that $y^2 = \alpha^2 + x^2$ (α^2 fixed).

Let $A_{\alpha^2} = \{y^2 : y^2 = \alpha^2 + x^2;\ y^2 \neq 0;\ \alpha^2 \neq 0;\ x^2 \neq 0\}$ so that $|A_{\alpha^2}| = \lambda$.

Then

$$\begin{aligned} y^2 = \alpha^2 + x^2 &\Leftrightarrow x^2 = y^2 - \alpha^2 \\ &\Leftrightarrow 1 = \left(\frac{y-\alpha}{x}\right)\left(\frac{y+\alpha}{x}\right). \end{aligned}$$

Let $t = \dfrac{y+\alpha}{x}$. Then we have $t^{-1} = \dfrac{y-\alpha}{x}$.

Thus

$$t + t^{-1} = \frac{2y}{x} \tag{4.44}$$

and

$$t - t^{-1} = \frac{2\alpha}{x}. \tag{4.45}$$

Equation (4.45) implies that

$$x = \frac{2\alpha}{t-t^{-1}} = \frac{2\alpha t}{t^2-1}\ (t \neq 0; t^2 \neq 1 \text{ since } x^2 \neq 0; \alpha^2 \neq 0).$$

In addition, Equation (4.44) implies that

$$\begin{aligned} y &= \frac{x}{2}(t+t^{-1}) \\ &= \alpha\left(\frac{t+t^{-1}}{t-t^{-1}}\right) \\ &= \alpha\left(\frac{t^2+1}{t^2-1}\right) \\ &= \alpha\left(1+\frac{2}{t^2-1}\right) \\ &= \alpha(1+2(t^2-1)^{-1});\ t^2 \neq \pm 1 \text{ since } y^2 \neq 0, \alpha^2 \neq 0. \end{aligned}$$

Let $B = \{i : \rho^i = \alpha(1+2(t^2-1)^{-1});\ t^2 \neq 0;\ t^2 \neq \pm 1\}$.
Then

$$\begin{aligned} |B| &= |\alpha(1+2\square^*_{q^2})| - 2 \\ &= |\square^*_{q^2}| - 2 \\ &= \frac{q^2-1}{2} - 2. \end{aligned}$$

Thus

$$|B| = \frac{q^2-5}{2}.$$

Hence we now have that

$$\begin{aligned} \lambda &= |A_{\alpha^2}| \\ &= |\{y^2 : y^2 = \alpha^2 + x^2, y^2 \neq 0, \alpha^2 \neq 0, x^2 \neq 0\}| \\ &= |\{2i : \rho^i = \alpha(1+2(t^2-1)^{-1}), t^2 \neq 0, t^2 \neq \pm 1\}|. \end{aligned}$$

Therefore

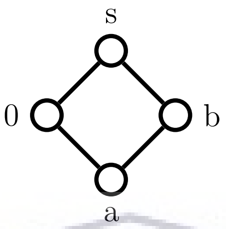
$$\begin{aligned} \lambda &= \frac{1}{2}|B| \\ &= \frac{1}{2}\frac{q^2-5}{2} \\ &= \frac{q^2-5}{4} \\ &= \frac{q^2-1}{4} - 1. \end{aligned}$$

$\square$

Lemma 4.13 *Let $b \in \mathbb{F}_{q^2}$ be a non-adjacent vertex to* 0 *in $\mathfrak{G}_{2,q}$, $q \equiv 3 \pmod 4$. Then the number of common neighbours to* 0 *and a in $\mathfrak{G}_{2,q}$ is*

$$\mu = \frac{q^2-1}{4}.$$

Proof. Let $a, s \in \mathbb{F}_{q^2}$ be common neighbours to both 0 and b as shown in the diagram below.



We have $b = a + s'$ and $s = b + s'' = a + s' + s''$, where $a, s, s', s'' \in \square^*_{q^2}$.

Let $a = \alpha^2$, $s' = \beta^2$, $s'' = x^2$, and $s = y^2$; with $\alpha^2 \neq 0$, $\beta^2 \neq 0$, $x^2 \neq 0$, and $y^2 \neq 0$.

Then $s = a + s' + s''$ implies that $y^2 = \alpha^2 + \beta^2 + x^2$; $\alpha^2 + \beta^2 \notin \square^*_{q^2}$ (α^2, β^2 fixed).

Let $A_{\alpha^2,\beta^2} = \{y^2 : y^2 = \alpha^2 + \beta^2 + x^2;\ \alpha^2, \beta^2, x^2, y^2 \in \square^*_{q^2};\ \alpha^2 + \beta^2 \notin \square^*_{q^2}\}$ so that $|A_{\alpha^2,\beta^2}| = \mu$.

Then $y^2 = \alpha^2 + \beta^2 + x^2$ if and only if $y^2 - x^2 = \alpha^2 + \beta^2 \notin \square^*_{q^2}$.

Let $B = \{y^2 : y^2 \neq 0;\ y^2 \neq \alpha^2\}$ and $C = \{y^2 : y^2 - x^2 \in \square^*_{q^2};\ y^2 \neq 0;\ x^2 \neq 0\}$.

Then $B = \{y^2 \in \square^*_{q^2};\ y^2 \neq \alpha^2\}$.

Therefore

$$\begin{aligned} |B| &= |\square^*_{q^2}| - 1 \\ &= \frac{q^2-1}{2} - 1 \\ &= \frac{q^2-3}{2}. \end{aligned}$$

Since $y^2 - x^2 \in \square^*_{q^2}$, we have $y^2 - x^2 = \gamma^2$ for some $\gamma \in \mathbb{F}^*_{q^2}$. Hence $y^2 = \gamma^2 + x^2$ and so C has a one-to-one correspondence with the set A_{α^2} for λ. Thus $|C| = \lambda = \dfrac{q^2-5}{4}$.

In this case, $A_{(\alpha^2,\beta^2)} = \{y^2 : y^2 - x^2 \notin \square^*_{q^2};\ y^2 \neq 0;\ x^2 \neq 0\} = B \setminus C$; and thus

$$\begin{aligned}
\mu &= |A_{\alpha^2,\beta^2}| \\
&= |B \setminus C| \\
&= |B| - |C| \\
&= \frac{q^2-3}{2} - \frac{q^2-5}{4} \\
&= \frac{2q^2-6-q^2+5}{4}.
\end{aligned}$$

Hence

$$\mu = \frac{q^2-1}{4}.$$

□

Combining all the results obtained in this section, we have the following.

Theorem 4.14 [21] *The graph $\mathfrak{G}_{2,q}$ is strongly regular with parameters*

$$(v,k,\lambda,\mu) = \left(q^2, \frac{(q-1)(q+3)}{2}, \frac{(q+1)(q+3)}{4} - 3, \frac{(q+1)(q+3)}{4}\right)$$

for $q \equiv 1 \pmod 4$; and

$$(v,k,\lambda,\mu) = \left(q^2, \frac{q^2-1}{2}, \frac{q^2-1}{4} - 1, \frac{q^2-1}{4}\right)$$

for $q \equiv 3 \pmod 4$.

Proof. In both cases, we have $\mathbb{F}_q^2$ as vertex set whose size is q^2. Thus $v = |V(\mathfrak{G}_{2,q})| = |\mathbb{F}_q^2| = q^2$. For the remaining parameters k, λ, and μ we have two different cases:

For $q \equiv 1 \pmod 4$, the result follows from Theorem 4.9, and by the isomorphism of the Cayley graph $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$ defined in Chapter 3 with $\mathfrak{G}_{2,q}$, $q \equiv 1 \pmod 4$, by the switch to hyperbolic coordinates.

On the other hand, if $q \equiv 3 \pmod 4$, then the result follows from Lemma 4.11, Lemma 4.12, and Lemma 4.13. □

Hence we shall conclude that the graph of integral distances $\mathfrak{G}_{2,q}$ is a strongly regular graph. Next, we consider the case of dimension $m > 2$.

4.2 The graphs $\mathfrak{G}_{m,q}$ for $m > 2$

In this section, we study the properties of $\mathfrak{G}_{m,q}$ for $m > 2$. We shall prove that the graph $\mathfrak{G}_{m,q}$ is a strongly regular graph if and only if $m \equiv 0 \pmod 2$.

We will first look at the valency (or degree) of $\mathfrak{G}_{m,q}$. Denote the degree of $\mathfrak{G}_{m,q}$ by $\mathcal{D}(m,q)$.

We first consider $m = 3$. For completeness, we determine the degree of the integral distance graph for this case in the following.

Lemma 4.15 [32] *The degree of $\mathfrak{G}_{3,q}$ is given by*

$$\mathcal{D}(3,q) = \begin{cases} (q-1)\dfrac{(q+2)(q+1)}{2} & \textit{if } q \equiv 1 \pmod 4; \\ (q-1)\left(\dfrac{q^2+q+2}{2}\right) & \textit{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. It suffices to determine the number of vectors $(\alpha,\beta,\gamma) \neq 0$ such that $\alpha^2 + \beta^2 + \gamma^2 \in \square_q$; i.e., $\alpha^2 + \beta^2 + \gamma^2 = \nu^2$ for some $\nu \in \mathbb{F}_q$.

If $\nu = 0$, we have $\alpha^2 + \beta^2 = -\gamma^2$ and we obtain $q^2 - 1$ vectors.

If $\nu \neq 0$, we have $\alpha^2 + \beta^2 = \nu^2 - \gamma^2$. As we have $\dfrac{q-1}{2}$ cases for ν^2 and q for γ, we obtain $\left(\dfrac{q-1}{q}\right) q$ cases for $\nu \neq 0$.

We therefore obtain

$$\begin{aligned} \mathcal{D}(3,q) &= |S| \\ &= q^2 - 1 + (q-1)\left(\frac{q-1}{2}\right) q \\ &= (q-1)\left(q+1+\frac{q^2-q}{2}\right) \\ &= (q-1)\left(\frac{q^2+q+2}{2}\right) \end{aligned}$$

for $q \equiv 1 \pmod 4$; and

$$\begin{aligned}\mathcal{D}(3,q) &= |S| \\ &= q^2 - 1 + (q+1)\left(\frac{q-1}{2}\right)q \\ &= (q-1)(q+1)\left(1+\frac{q}{2}\right) \\ &= (q-1)\frac{(q+1)(q+2)}{2}\end{aligned}$$

for $q \equiv 3 \pmod 4$. □

To determine the degree $\mathcal{D}(m,q)$ of the integral distance graph $\mathfrak{G}_{m,q}$ in arbitrary dimension m, we shall use the obtained values of $\mathcal{Z}(m,q)$, $\mathcal{S}(m,q)$, and $\mathcal{N}(m,q)$ from Theorem 2.24 in Chapter 2.

Since $\mathfrak{G}_{m,q} \cong \mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})$, so that its degree equal the size of the Cayley set $S^{(m)}$ defined in Chapter 3 as the set of all non-zero vectors $s \in \mathbb{F}_q^m$ with $N(s) \in \square_q$, it follows that

$$\mathcal{D}(m,q) = \mathcal{Z}(m,q) + \mathcal{S}(m,q) - 1. \tag{4.46}$$

Now we have the following result about $\mathcal{D}(m,q)$ with our own proof for the sake of completeness.

Lemma 4.16 [32] *Let $m \geq 1$ be arbitrary.*

The degree $\mathcal{D}_{m,q}$ of the integral distance graph $\mathfrak{G}_{m,q}$ for $q \equiv 1 \pmod 4$ is given by

$$\mathcal{D}(m,q) = \begin{cases} \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right) - 1 & \textit{for } m \textit{ odd;} \\ \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}\right) - 1 & \textit{for } m \textit{ even;} \end{cases}$$

and for $q \equiv 3 \pmod 4$,

$$\mathcal{D}(m,q) = \begin{cases} \frac{1}{2}\left(q^m + q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}}\right) - 1 & \textit{for } m \textit{ odd;} \\ \frac{1}{2}\left(q^m + q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}}\right) - 1 & \textit{for } m \textit{ even.} \end{cases}$$

Proof. Using the results from Theorem 2.24 in Equation (4.46), we obtain the following.

(a) m odd:

(i) $q \equiv 1 \pmod 4$:

$$\begin{aligned}\mathcal{D}(m,q) &= \frac{1}{2}\left(q^m - q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right) + q^{m-1} - 1\\ &= \frac{1}{2}q^m - \frac{1}{2}q^{m-1} + \frac{1}{2}q^{\frac{m+1}{2}} - \frac{1}{2}q^{\frac{m-1}{2}} + q^{m-1} - 1.\end{aligned}$$

Thus

$$\mathcal{D}(m,q) = \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right) - 1.$$

(ii) $q \equiv 3 \pmod 4$:

$$\begin{aligned}\mathcal{D}(m,q) &= \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}}\right) + q^{m-1} - 1\\ &= \frac{1}{2}q^m - \frac{1}{2}q^{m-1} - \frac{1}{2}(-q)^{\frac{m+1}{2}} - \frac{1}{2}(-q)^{\frac{m-1}{2}} + q^{m-1} - 1.\end{aligned}$$

Thus

$$\mathcal{D}(m,q) = \frac{1}{2}\left(q^m + q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}}\right) - 1.$$

(b) m even:

(i) $q \equiv 1 \pmod 4$

$$\begin{aligned}\mathcal{D}(m,q) &= \frac{1}{2}\left(q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right) + q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}} - 1\\ &= \frac{1}{2}q^m - \frac{1}{2}q^{m-1} - \frac{1}{2}q^{\frac{m}{2}} + \frac{1}{2}q^{\frac{m-2}{2}} + q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}} - 1.\end{aligned}$$

Thus

$$\mathcal{D}(m,q) = \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}\right) - 1.$$

(ii) $q \equiv 3 \pmod 4$

$$\begin{aligned}\mathcal{D}(m,q) &= \frac{1}{2}\left(q^m - q^{m-1} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right) + q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}} - 1\\ &= \frac{1}{2}q^m - \frac{1}{2}q^{m-1} - \frac{1}{2}(-q)^{\frac{m}{2}} - \frac{1}{2}(-q)^{\frac{m-2}{2}} + q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}} - 1.\end{aligned}$$

Thus

$$\mathcal{D}(m,q) = \frac{1}{2}\left(q^m + q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}}\right) - 1.$$

□

For completeness with strongly regular graphs in mind, we give the proof of the following result in order to determine the number of common neighbors to adjacent vertices by our own computations.

Theorem 4.17 [32] *If $\lambda = \mathcal{A}(m,q)$ is the number of neighbors of $\mathbf{0}$ and $\mathbf{e}^{(1)} = (1,0,\cdots,0)$ in $\mathbb{F}_q^m \setminus \{\mathbf{0},\mathbf{e}^{(1)}\}$; then for $m \geq 1$ we have*

$$\mathcal{A}(m,q) = \begin{cases} \dfrac{q^{m-2}(q+1)^2 + (-1)^{\frac{(m-1)(q-1)}{4}} q^{\frac{m-3}{2}}(3q^2-2q-1)}{4} - 2 & \textit{for } m \textit{ odd;} \\ \dfrac{q^{m-2}(q+1)^2 + 2(-1)^{\frac{m(q-1)}{4}} q^{\frac{m-2}{2}}(q-1)}{4} - 2 & \textit{for } m \textit{ even.} \end{cases}$$

Proof. Clearly, we have $\mathcal{A}(1,q) = q-2$. For $m \geq 1$, we count the number of solutions $(x_1, x_2, \cdots, x_m)$ of the system of equations

$$x_1^2 + \sum_{i=2}^{m} x_i^2 = \alpha^2; \tag{4.47}$$

$$(x_1-1)^2 + \sum_{i=2}^{m} x_i^2 = \beta^2. \tag{4.48}$$

Substracting Equation (4.48) from Equation (4.47), we obtain

$$2x_1 - 1 = \alpha^2 - \beta^2 \Leftrightarrow x_1 = \frac{\alpha^2-\beta^2+1}{2}.$$

Hence Equation (4.47) becomes

$$\sum_{i=2}^{m} x_i^2 = \alpha^2 - \left(\frac{\alpha^2-\beta^2+1}{2}\right)^2 = \tau; \ \tau \in \mathbb{F}_q.$$

Let a_ν be the number of (α^2, β^2) resulting in $\tau = \nu$.

Then $\displaystyle\sum_{\nu\in\mathbb{F}_q} a_\nu = \left(\frac{q+1}{2}\right)^2$. Denote by $b_{m,\nu}$, the number of vectors $(x_2,\cdots,x_m) \in \mathbb{F}_q^{m-1}$ with $\displaystyle\sum_{j=2}^{m} x_j^2 = \nu$. Then we have

$$\mathcal{A}(m,q) = \sum_{\nu\in\mathbb{F}_q} a_\nu b_{m,\nu} - 2.$$

Since $\mathcal{A}(1,q) = q-2$, we have $b_{1,\nu} = 0$ for $\nu \neq 0$ and $a_0 = q$.
If $\nu, \mu \in \square_q^*$ or $\nu, \mu \notin \square_q$, then $b_{m,\nu} = b_{m,\mu}$.
Let $a_+ = \displaystyle\sum_{\nu \in \square_q^*} a_\nu$ and $a_- = \displaystyle\sum_{\nu \notin \square_q} a_\nu$.

If we use the results for $\mathcal{A}(2,q)$; i.e., $\lambda = \mathcal{A}(2,q) = \dfrac{q^2-1}{4} - 1$ for $q \equiv 3 \pmod 4$, and $\lambda = \mathcal{A}(2,q) = \dfrac{(q+1)(q+3)}{4} - 3$ for $q \equiv 1 \pmod 4$; then

$$\begin{aligned}\mathcal{A}(2,q) &= a_0 \cdot 1 + a_+ \cdot 2 + a_- \cdot 0 - 2\\ &= a_0 + 2a_+ - 2.\end{aligned}$$

(i) $q \equiv 3 \pmod 4$:

$$\begin{aligned}\frac{q^2-1}{4} - 1 = q + 2a_+ - 2 &\Leftrightarrow 2a_+ = \frac{q^2-5}{4} - q + 2\\ &\Leftrightarrow 2a_+ = \frac{q^2-5-4q+8}{4} = \frac{q^2-4q+3}{4}\\ &\Rightarrow a_+ = \frac{(q-1)(q-3)}{8}.\end{aligned}$$

(ii) $q \equiv 1 \pmod 4$:

$$\begin{aligned}\frac{(q+1)(q+3)}{4} - 3 = q + 2a_+ - 2 &\Leftrightarrow 2a_+ = \frac{q^2+4q-9}{4} - q + 2\\ &\Leftrightarrow 2a_+ = \frac{q^2+4q-9-4q+8}{4}\\ &\Leftrightarrow a_+ = \frac{q^2-1}{8} = \frac{(q-1)(q+1)}{8}.\end{aligned}$$

To find a_-, we have

$$\sum_{\nu \in \mathbb{F}_q} a_\nu = a_0 + \sum_{\nu \in \square_q^*} a_\nu + \sum_{\nu \notin \square_q} a_\nu = a_0 + a_+ + a_-.$$

Then

$$\left(\frac{q+1}{2}\right)^2 = q + a_+ + a_- \Leftrightarrow a_- = \left(\frac{q+1}{2}\right)^2 - a_+ - q.$$

(i) $q \equiv 3 \pmod 4$:

$$\begin{aligned} a_- &= \left(\frac{q+1}{2}\right)^2 - q - \frac{(q-1)(q-3)}{8} \\ &= \frac{2q^2+4q+2-8q-q^2+4q-3}{8} \\ &= \frac{q^2-1}{8} \\ &= \frac{(q-1)(q+1)}{8}. \end{aligned}$$

(ii) $q \equiv 1 \pmod 4$:

$$\begin{aligned} a_- &= \left(\frac{q+1}{2}\right)^2 - q - \left(\frac{q^2-1}{8}\right) \\ &= \frac{2q^2+4q+2-8q-q^2+1}{8} \\ &= \frac{q^2-4q+3}{8} \\ &= \frac{(q-1)(q-3)}{8}. \end{aligned}$$

As $b_{m,0} = \mathcal{Z}(m-1,q)$, $b_{m,\nu} = \dfrac{2}{q-1}\mathcal{S}(m-1,q)$ for $\nu \in \square_q^*$, and

$b_{m,\nu} = \dfrac{2}{q-1}\mathcal{N}(m-1,q)$ for $\nu \notin \square_q$; then

$$\begin{aligned} \lambda &= \mathcal{A}(m,q) \\ &= \sum_{\nu\in\mathbb{F}_q} a_\nu b_{m,\nu} - 2 \\ &= a_0 b_{m,0} + a_+ \cdot \frac{2}{q-1}\mathcal{S}(m-1,q) + a_- \cdot \frac{2}{q-1}\mathcal{N}(m-1,q) - 2 \\ &= a_0\mathcal{Z}(m-1,q) + a_+\frac{2}{q-1}\mathcal{S}(m-1,q) + a_-\frac{2}{q-1}\mathcal{N}(m-1,q) - 2. \end{aligned}$$

(a) m even ($m-1$ odd):

(i) $q \equiv 1 \pmod 4$:

$b_{m,0} = \mathcal{Z}(m-1,q) = q^{m-2}$; $\mathcal{S}(m-1,q) = \dfrac{1}{2}\left(q^{m-1} - q^{m-2} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}\right)$;

and $\mathcal{N}(m-1,q) = \dfrac{1}{2}\left(q^{m-1} - q^{m-2} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right)$.

Then

$$\begin{aligned}
\lambda &= q \cdot q^{m-2} + \frac{(q-1)(q+1)}{8} \cdot \frac{2}{q-1} \cdot \frac{1}{2}\left(q^{m-1} - q^{m-2} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}\right) \\
&\quad + \frac{(q-1)(q-3)}{8} \cdot \frac{2}{q-1} \cdot \frac{1}{2}\left(q^{m-1} - q^{m-2} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}\right) - 2 \\
&= \left(\frac{4q^{m-1} + q^{m} - 2q^{m-1} + q^{m-2} + 2q^{\frac{m}{2}} - 2q^{\frac{m-2}{2}}}{4}\right) - 2.
\end{aligned}$$

Thus

$$\lambda = \mathcal{A}(m,q) = \frac{q^{m-2}(q+1)^2 + 2q^{\frac{m-2}{2}}(q-1)}{4} - 2.$$

(ii) $q \equiv 3 \pmod 4$:

$b_{m,0} = \mathcal{Z}(m-1,2) = q^{m-2}$; $\mathcal{S}(m-1,q) = \dfrac{1}{2}\left(q^{m-1} - q^{m-2} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right)$;

and $\mathcal{N}(m-1,q) = \dfrac{1}{2}\left(q^{m-1} - q^{m-2} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}}\right)$.

Then

$$\begin{aligned}
\lambda &= q \cdot q^{m-2} + \frac{(q-1)(q-3)}{8} \cdot \frac{2}{q-1} \cdot \frac{1}{2}\left(q^{m-1} - q^{m-2} - (-q)^{\frac{m}{2}} - (-q)^{\frac{m-2}{2}}\right) \\
&\quad + \frac{(q-1)(q+1)}{8} \cdot \frac{2}{q-1} \cdot \frac{1}{2}\left(q^{m-1} - q^{m-2} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}}\right) - 2 \\
&= \left(\frac{4q^{m-1} + q^{m} - 2q^{m-1} + q^{m-2} + 2(-1)^{\frac{m}{2}}q^{\frac{m}{2}} - 2(-1)^{\frac{m}{2}}q^{\frac{m-2}{2}}}{4}\right) - 2.
\end{aligned}$$

Thus

$$\lambda = \mathcal{A}(m,q) = \frac{q^{m-2}(q+1)^2 + 2(-1)^{\frac{m}{2}}q^{\frac{m-2}{2}}(q-1)}{4} - 2.$$

For $q \equiv 1 \pmod 4$; $q-1 \equiv 0 \pmod 4$ if and only if $\dfrac{q-1}{2} \equiv 0 \pmod 2$, and $(-1)^{\frac{q-1}{2}} = 1$.

For $q \equiv 3 \pmod 4$, $q-1 \equiv 2 \pmod 4$; i.e., $\dfrac{q-1}{2} \equiv 1 \pmod 2$ and $(-1)^{\frac{q-1}{2}} = -1$.

Therefore $\lambda = \mathcal{A}(m,q) = \dfrac{q^{m-2}(q+1)^2 + 2(-1)^{\frac{m(q-1)}{4}}q^{\frac{m-2}{2}}(q-1)}{4} - 2$.

(b) m odd ($m-1$ even):

(i) $q \equiv 1 \pmod 4$:

$b_{m,0} = \mathcal{Z}(m-1,q) = q^{m-2} + q^{\frac{m-1}{2}} - q^{\frac{m-3}{2}}$;

$\mathcal{S}(m-1,q) = \dfrac{1}{2}\left(q^{m-1} - q^{m-2} - q^{\frac{m-1}{2}} + q^{\frac{m-3}{2}}\right)$;

and $\mathcal{N}(m-1,q) = \dfrac{1}{2}\left(q^{m-1} - q^{m-2} - q^{\frac{m-1}{2}} + q^{\frac{m-3}{2}}\right)$.

Then

$$\begin{aligned}
\lambda &= \mathcal{A}(m,q) \\
&= q(q^{m-2} + q^{\frac{m-1}{2}} + q^{\frac{m-3}{2}}) \\
&\quad + \frac{(q-1)(q+1)}{8} \cdot \frac{2}{q-1} \cdot \frac{1}{2}\left(q^{m-1} - q^{m-2} - q^{\frac{m-1}{2}} + q^{\frac{m-3}{2}}\right) \\
&\quad + \frac{(q-1)(q-3)}{8} \cdot \frac{2}{q-1} \cdot \frac{1}{2}\left(q^{m-1} - q^{m-2} - q^{\frac{m-1}{2}} + q^{\frac{m-3}{2}}\right) - 2 \\
&= \frac{4q^{m-1} + 4q^{\frac{m+1}{2}} - 4q^{\frac{m-1}{2}} + q^{m} - 2q^{m-1} + q^{m-2} - q^{\frac{m+1}{2}} + 2q^{\frac{m-1}{2}} - q^{\frac{m-3}{2}}}{4} - 2.
\end{aligned}$$

Thus

$$\lambda = \mathcal{A}(m,q) = \frac{q^{m-2}(q+1)^2 + q^{\frac{m-3}{2}}(3q^2 - 2q - 1)}{4} - 2.$$

(ii) $q \equiv 3 \pmod 4$:

$b_{m,0} = \mathcal{Z}(m-1,q) = q^{m-2} + (-q)^{\frac{m-1}{2}} + (-q)^{\frac{m-3}{2}}$;

$\mathcal{S}(m-1,q) = \dfrac{1}{2}\left(q^{m-1} - q^{m-2} - (-q)^{\frac{m-1}{2}} - (-q)^{\frac{m-3}{2}}\right)$;

and $\mathcal{N}(m-1,q) = \dfrac{1}{2}\left(q^{m-1} - q^{m-2} - (-q)^{\frac{m-1}{2}} - (-q)^{\frac{m-3}{2}}\right)$.

Then

$$\begin{aligned}
\lambda &= \mathcal{A}(m,q); \\
&= q\left(q^{m-2} + (-q)^{\frac{m-1}{2}} + (-q)^{\frac{m-3}{2}}\right) \\
&\qquad + \frac{(q-1)(q-3)}{8}\cdot\frac{2}{q-1}\cdot\frac{1}{2}\left(q^{m-1} - q^{m-2} - (-q)^{\frac{m-1}{2}} - (-q)^{\frac{m-3}{2}}\right) \\
&\qquad + \frac{(q-1)(q+1)}{8}\cdot\frac{2}{q-1}\cdot\frac{1}{2}\left(q^{m-1} - q^{m-2} - (-q)^{\frac{m-1}{2}} - (-q)^{\frac{m-3}{2}}\right) - 2 \\
&= \frac{1}{4}\left(4q^{m-1} + 4(-1)^{\frac{m-1}{2}}q^{\frac{m+1}{2}} - 4(-1)^{\frac{m-1}{2}}q^{\frac{m-1}{2}} + q^m - 2q^{m-1} + q^{m-2}\right. \\
&\qquad \left. - (-1)^{\frac{m-1}{2}}q^{\frac{m+1}{2}} + 2(-1)^{\frac{m-1}{2}}q^{\frac{m-1}{2}} - (-1)^{\frac{m-1}{2}}q^{\frac{m-3}{2}}\right) - 2.
\end{aligned}$$

Thus

$$\lambda = \mathcal{A}(m,q) = \frac{q^{m-2}(q+1)^2 + (-1)^{\frac{m-1}{2}}q^{\frac{m-3}{2}}(3q^2-2q-1)}{4} - 2.$$

Hence

$$\lambda = \mathcal{A}(m,q) = \frac{q^{m-2}(q+1)^2 + (-1)^{\frac{(m-1)(q-1)}{4}}q^{\frac{m-3}{2}}(3q^2-2q-1)}{4} - 2.$$

□

Therefore, for dimension $m = 3$, again by the same process as above, we have for completeness

$$\begin{aligned}
\mathcal{A}(3,q) &= \frac{q(q+1)^2 + (-1)^2q^0(3q^2-2q-1)}{4} - 2 \\
&= \frac{q^3 + 2q^2 + q + 3q^2 - 2q - 1 - 8}{4} \\
&= \frac{q^3 + 5q^2 - q - 9}{4} \qquad\qquad \text{for } q \equiv 1 \pmod 4
\end{aligned}$$

and

$$\begin{aligned}
\mathcal{A}(3,q) &= \frac{q(q+1)^2 + (-1)q^0(3q^2-2q-1)}{4} - 2 \\
&= \frac{q^3 + 2q^2 + q - 3q^2 + 2q + 1 - 8}{4} \\
&= \frac{q^3 - q^2 + 3q - 7}{4} \qquad\qquad \text{for } q \equiv 3 \pmod 4.
\end{aligned}$$

Again with our own calculations, we use the above results and Theorem 2.2 to determine the number of common neighbors to non-adjacent vertices in the following for completeness. This is done in order to check the strong regularity in all dimensions for each case of q.

Lemma 4.18 [32] *For odd dimension $m \geq 3$, the graph of integral distances $\mathfrak{G}_{m,q}$ is not a strongly regular graph.*

Proof. We prove by contradiction. Let us assume that $\mathfrak{G}_{m,q}$ is strongly regular. Then there exists the corresponding parameters (v, k, λ, μ) with $v = q^m$, $k = \mathcal{D}(m, q)$, and $\lambda = \mathcal{A}(m, q)$.

For a strongly regular graph we have from Theorem 2.2 the identity

$(v - k - 1)\mu = k(k - \lambda - 1)$.

Using Lemma 4.16 and Theorem 4.17, we can use this identity to determine μ.

For $q \equiv 1 \pmod 4$ and m odd, we have

$k = \mathcal{D}(m, q) = \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right) - 1$; and

$\lambda = \mathcal{A}(m, q) = \frac{q^{m-2}(q+1)^2 + q^{\frac{m-3}{2}}(3q^2 - 2q - 1)}{4} - 2.$

$$\begin{aligned} k - \lambda - 1 &= \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m+1}{2}} - q^{\frac{m-1}{2}}\right) - 1 \\ &\quad - \frac{q^{m-2}(q+1)^2 + q^{\frac{m-3}{2}}(3q^2 - 2q - 1)}{4} + 2 - 1 \\ &= \frac{q^m - q^{m-2} - q^{\frac{m+1}{2}} + q^{\frac{m-3}{2}}}{4} \\ &= \frac{q^{\frac{m-3}{2}}(q-1)(q+1)(q^{\frac{m-1}{2}} - 1)}{4}. \end{aligned}$$

$$k(k-\lambda-1)=\frac{q^{\frac{m-3}{2}}(q-1)(q+1)(q^{\frac{m-1}{2}}-1)\left[\left(q^m+q^{m-1}+q^{\frac{m+1}{2}}-q^{\frac{m-1}{2}}\right)-2\right]}{8}.$$

$$\begin{aligned}
v-k-1 &= q^m-\frac{1}{2}\left(q^m+q^{m-1}+q^{\frac{m+1}{2}}-q^{\frac{m-1}{2}}\right)+1-1\\
&= \frac{2q^m-q^m-q^{m-1}-q^{\frac{m+1}{2}}+q^{\frac{m-1}{2}}}{2}\\
&= \frac{q^m-q^{m-1}-q^{\frac{m+1}{2}}+q^{\frac{m-1}{2}}}{2}\\
&= \frac{q^{\frac{m-1}{2}}(q-1)(q^{\frac{m-1}{2}}-1)}{2}.
\end{aligned}$$

Thus

$$\mu=\frac{k(k-\lambda-1)}{v-k-1}=\frac{(q+1)\left(q^m+q^{m-1}+q^{\frac{m+1}{2}}-q^{\frac{m-1}{2}}-2\right)}{4q}.$$

For $q\equiv 3 \pmod 4$ and m odd, we obtain:

$k=\mathcal{D}(m,q)=\frac{1}{2}\left(q^m+q^{m-1}-(-q)^{\frac{m+1}{2}}-(-q)^{\frac{m-1}{2}}\right)-1$; and

$\lambda=\mathcal{A}(m,q)=\frac{q^{m-2}(q+1)^2+(-1)^{\frac{m-1}{2}}q^{\frac{m-3}{2}}(3q^2-2q-1)}{4}-2.$

$$\begin{aligned}
k-\lambda-1 &= \frac{1}{2}\left(q^m+q^{m-1}-(-q)^{\frac{m+1}{2}}-(-q)^{\frac{m-1}{2}}\right)-1\\
&\quad -\frac{q^{m-2}(q+1)^2+(-1)^{\frac{m-1}{2}}q^{\frac{m-3}{2}}(3q^2-2q-1)}{4}+2-1\\
&= \frac{q^m-q^{m-2}+(-q)^{\frac{m+1}{2}}+(-1)^{\frac{m-1}{2}}q^{\frac{m-3}{2}}}{2}\\
&= \frac{q^m-q^{m-2}-(-1)^{\frac{m-1}{2}}q^{\frac{m+1}{2}}+(-1)^{\frac{m-1}{2}}q^{\frac{m-3}{2}}}{4}\\
&= \frac{q^{\frac{m-3}{2}}(q-1)(q+1)\left(q^{\frac{m-1}{2}}-(-1)^{\frac{m-1}{2}}\right)}{4}.
\end{aligned}$$

$$k(k-\lambda-1) = \frac{q^{\frac{m-3}{2}}(q-1)(q+1)(q^{\frac{m-1}{2}} - (-1)^{\frac{m-1}{2}})(q^m + q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}} - 2)}{8}.$$

$$\begin{aligned} v-k-1 &= q^m - \frac{1}{2}\left(q^m + q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}}\right) + 1 - 1 \\ &= \frac{2q^m - q^m - q^{m-1} + (-q)^{\frac{m+1}{2}} + (-q)^{\frac{m-1}{2}}}{2} \\ &= \frac{q^{m-1}(q-1) - (-1)^{\frac{m-1}{2}}q^{\frac{m+1}{2}} - (-1)^{\frac{m-1}{2}}q^{\frac{m-1}{2}}}{2} \\ &= \frac{q^{\frac{m-1}{2}}(q-1)(q^{\frac{m-1}{2}} - (-1)^{\frac{m-1}{2}})}{2}. \end{aligned}$$

Thus

$$\mu = \frac{k(k-\lambda-1)}{v-k-1} = \frac{(q+1)\left(q^m + q^{m-1} - (-q)^{\frac{m+1}{2}} - (-q)^{\frac{m-1}{2}} - 2\right)}{4q}.$$

As for odd $m \geq 3$, the denominator of μ is divisible by q, and the numerator is not divisible by q, the graph of integral distances $\mathfrak{G}_{m,q}$ is not a strongly regular graph in these cases.

If the same computations are done for $m \equiv 0 \pmod 2$, then for $q \equiv 1 \pmod 4$ we get

$k = \mathcal{D}(m,q) = \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}\right) - 1$; and

$\lambda = \mathcal{A}(m,q) = \frac{q^{m-2}(q+1)^2 + 2q^{\frac{m-2}{2}}(q-1)}{4} - 2.$

$$\begin{aligned} k-\lambda-1 &= \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}\right) - 1 \\ &\quad - \frac{q^{m-2}(q+1)^2 + 2q^{\frac{m-2}{2}}(q-1)}{4} + 2 - 1 \\ &= \frac{q^m - q^{m-2}}{4} = \frac{q^{m-2}(q-1)(q+1)}{4}. \end{aligned}$$

$$\begin{aligned} k(k-\lambda-1) &= \frac{q^{m-2}(q-1)(q+1)(q^m + q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}} - 2)}{8} \\ &= \frac{q^{m-2}(q-1)(q+1)(q^{\frac{m}{2}} - 1)(q^{\frac{m}{2}} + q^{\frac{m-2}{2}} + 2)}{8}. \end{aligned}$$

$$\begin{aligned} v-k-1 &= q^m - \frac{1}{2}\left(q^m + q^{m-1} + q^{\frac{m}{2}} - q^{\frac{m-2}{2}}\right) + 1 - 1 \\ &= \frac{q^m - q^{m-1} - q^{\frac{m}{2}} + q^{\frac{m-2}{2}}}{2} = \frac{q^{\frac{m-2}{2}}(q^{\frac{m}{2}}-1)(q-1)}{2}. \end{aligned}$$

Thus

$$\mu = \frac{q^{\frac{m-1}{2}}(q+1)\left(q^{\frac{m}{2}} + q^{\frac{m-2}{2}} + 2\right)}{4}.$$

In addition, for $q \equiv 3 \pmod 4$ we obtain

$k = \mathcal{D}(m,q) = \frac{1}{2}\left(q^m + q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}}\right) - 1$; and

$\lambda = \mathcal{A}(m,q) = \frac{q^{m-2}(q+1)^2 + 2(-1)^{\frac{m}{2}}q^{\frac{m-2}{2}}(q-1)}{4} - 2.$

$$\begin{aligned} k-\lambda-1 &= \frac{1}{2}\left(q^m + q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}}\right) - 1 \\ &\quad - \frac{q^{m-2}(q+1)^2 + 2(-1)^{\frac{m}{2}}q^{\frac{m-2}{2}}(q-1)}{4} + 2 - 1 \\ &= \frac{q^m - q^{m-2}}{4} = \frac{q^{m-2}(q-1)(q+1)}{4}. \end{aligned}$$

$$\begin{aligned} k(k-\lambda-1) &= \frac{q^{m-2}(q-1)(q+1)(q^m + q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}} - 2)}{8} \\ &= \frac{q^{m-2}(q-1)(q+1)[q^m + (-1)^{\frac{m}{2}}q^{\frac{m}{2}} - 2(-1)^m + q^{m-1} - (-1)^{\frac{m}{2}}q^{\frac{m-2}{2}}]}{8} \\ &= \frac{q^{m-2}(q-1)(q+1)(q^{\frac{m}{2}} - (-1)^{\frac{m}{2}})(q^{\frac{m}{2}} + q^{\frac{m-2}{2}} + 2(-1)^{\frac{m}{2}})}{8}. \end{aligned}$$

$$\begin{aligned} v-k-1 &= q^m - \frac{1}{2}\left(q^m + q^{m-1} + (-q)^{\frac{m}{2}} + (-q)^{\frac{m-2}{2}}\right) + 1 - 1 \\ &= \frac{2q^m - q^m - q^{m-1} - (-q)^{\frac{m}{2}} + (-1)^{\frac{m}{2}}q^{\frac{m-2}{2}}}{2} \\ &= \frac{q^{\frac{m-2}{2}}(q^{\frac{m}{2}} - (-1)^{\frac{m}{2}})(q-1)}{2}. \end{aligned}$$

Thus

$$\mu = \frac{k(k-\lambda-1)}{v-k-1} = \frac{q^{\frac{m-2}{2}}(q+1)\left(q^{\frac{m}{2}} + q^{\frac{m-2}{2}} + 2(-1)^{\frac{m}{2}}\right)}{4}.$$

Hence in both cases, we have $\mu \in \mathbb{N}$ for even dimension m. Therefore the graph $\mathfrak{G}_{m,q}$ could be strongly regular for even dimension m, and indeed, this is the conjecture from [32] to be proved. □

At the core of the proof of the conjecture is the following result.

Theorem 4.19 *If $\mathcal{B}(m,q)$ denotes the number of common neighbors of $\mathbf{0}$ and an element $\mathbf{v}$ with $\langle \mathbf{v}, \mathbf{v} \rangle = 0$ in $\mathbb{F}_q^m \setminus \{\mathbf{0}, \mathbf{v}\}$, then for $m \geq 2$ we have*

$$\mathcal{B}(m,q) = \begin{cases} \mathcal{A}(m,q) & \textit{for } m \textit{ even,} \\ \mathcal{A}(m,q) - (-1)^{\frac{(q-1)(m-1)}{4}} q^{\frac{m-3}{2}} \left(\dfrac{q^2-1}{4} \right) & \textit{for } m \textit{ odd.} \end{cases}$$

For even dimension m, the graph of integral distances $\mathfrak{G}_{m,q}$ is a strongly regular graph.

Proof. Without loss of generality, let $\mathbf{x} = (x_1, x_2, \cdots, x_m)$ and $\mathbf{v} = (1, \omega, 0, \cdots, 0)$, with $\omega^2 = -1$ and $\langle \mathbf{v}, \mathbf{v} \rangle = 0$. Here, $q \equiv 1 \pmod 4$. $\mathbf{x}$ is adjacent to $\mathbf{0}$ and $\mathbf{v}$ if

$$\begin{aligned} x_1^2 + x_2^2 + \sum_{i=3}^{m} x_i^2 &= \alpha^2; & (4.49) \\ (x_1 - 1)^2 + (x_2 - \omega)^2 + \sum_{i=3}^{m} x_i^2 &= \beta^2. & (4.50) \end{aligned}$$

Substracting Equation (4.50) from Equation (4.49) implies $x_1 + \omega x_2 = \dfrac{\alpha^2 - \beta^2}{2}$. We have different cases for α^2 and β^2:

(a) $\alpha^2 = \beta^2 = 0$:

We have

$$\begin{aligned} x_1^2 + x_2^2 + \sum_{i=3}^{m} x_i^2 &= 0; & (4.51) \\ x_1 + \omega x_2 &= 0. & (4.52) \end{aligned}$$

From Equation (4.52), we obtain $\omega x_2 = -x_1$ and thus $x_2 = \omega x_1$.

Equation (4.51) implies that $x_1^2 + \omega^2 x_1^2 + \sum_{i=3}^{m} x_i^2 = 0$ and hence $\sum_{i=3}^{m} x_i^2 = 0$.

If we take $x_i = \gamma_i$ with $i = 3, \cdots, m$ and $x_1 = a$, we have the solutions of the form $(a, \omega a, \gamma_3, \cdots, \gamma_m)$ with $\sum_{i=3}^{m} \gamma_i = 0$; $(a, \gamma_i) \neq (0,0); (1,0)$; and thus $q\mathcal{Z}(m-2,q) - 2$ solutions, where $\mathcal{Z}(m-2,q)$ is one of the three functions defined in Section 2.3.

(b) $\alpha^2 \neq 0$, $\beta^2 = 0$:

We have

$$x_1^2 + x_2^2 + \sum_{i=3}^{m} x_i^2 = \alpha^2; \tag{4.53}$$

$$(x_1 - 1)^2 + (x_2 - \omega)^2 + \sum_{i=3}^{m} x_i^2 = 0. \tag{4.54}$$

Again, substracting Equation (4.54) from Equation (4.53) implies that $2x_1 + 2\omega x_2 = \alpha^2$ and therefore

$$x_2 = -\omega \left(\frac{\alpha^2}{2} - x_1 \right).$$

From Equation (4.53), we get

$$\begin{aligned} x_1^2 + \omega^2 \left(\frac{\alpha^2}{2} - x_1 \right)^2 + \sum_{i=3}^{m} x_i^2 = \alpha^2 &\Rightarrow x_1^2 - \left(\frac{\alpha^4}{4} - 2\frac{\alpha^2}{2} x_1 + x_1^2 \right) + \sum_{i=3}^{m} x_i^2 = \alpha^2 \\ &\Rightarrow -\frac{\alpha^4}{4} + \alpha^2 x_1 + \sum_{i=3}^{m} x_i^2 = \alpha^2. \end{aligned}$$

Put $x_i = \gamma_i$, $i = 3, \cdots, m$. Then

$x_1 = \left(1 - \frac{1}{\alpha^2} \sum_{i=3}^{m} \gamma_i^2 + \frac{\alpha^2}{4} \right)$ and $x_2 = -\omega \left(\frac{\alpha^2}{4} + \frac{1}{\alpha^2} \sum_{i=3}^{m} \gamma_i^2 - 1 \right)$ $(\alpha^2 \neq 0)$.

This gives rise to solutions of the form $(x_1, x_2, \gamma_3, \cdots, \gamma_m)$ and thus $q^{m-2} \left(\frac{q-1}{2} \right)$ solutions.

(c) $\alpha^2 = 0$, $\beta^2 \neq 0$:

We have

$$\begin{aligned} x_1^2 + x_2^2 + \sum_{i=3}^{m} x_i^2 &= 0; & (4.55) \\ (x_1 - 1)^2 + (x_2 - \omega)^2 + \sum_{i=3}^{m} x_i^2 &= \beta^2. & (4.56) \end{aligned}$$

Substracting Equation (4.56) from Equation (4.55), we get $2x_1 + 2x_2\omega = -\beta^2$ and thus $x_2 = \omega\left(\frac{\beta^2}{2} + x_1\right)$.

Equation (4.55) implies

$$\begin{aligned} x_1^2 + \omega^2\left(\frac{\beta^2}{2} + x_1\right)^2 + \sum_{i=3}^{m} x_i^2 = 0 \Rightarrow x_1^2 - \left(\frac{\beta^4}{4} + 2\frac{\beta^2}{2}x_1 + x_1^2\right) + \sum_{i=3}^{m} x_i^2 = 0 \\ \Rightarrow -\frac{\beta^4}{4} - \beta^2 x_1 + \sum_{i=3}^{m} x_i^2 = 0. \end{aligned}$$

Put $x_i = \gamma_i$. Then, $x_1 = \frac{1}{\beta^2}\sum_{i=3}^{m} \gamma_i^2 - \frac{\beta^2}{4}$;

and

$$\begin{aligned} x_2 &= \omega\left(\frac{\beta^2}{2} + \frac{1}{\beta^2}\sum_{i=3}^{m} \gamma_1^2 - \frac{\beta^2}{4}\right) \\ &= \omega\left(\frac{1}{\beta^2}\sum_{i=3}^{m} \gamma_i^2 + \frac{\beta^2}{4}\right) \ (\beta^2 \neq 0). \end{aligned}$$

In this case, we obtain solutions in the similar form as in (b) and thus $q^{m-2}\left(\frac{q-1}{2}\right)$ of them.

(d) $\alpha \neq 0$, $\beta \neq 0$: We consider the two following sub-cases:

(i) $\alpha^2 = \beta^2 \neq 0$.

The system becomes

$$\begin{aligned} x_1^2 + x_2^2 + \sum_{i=3}^{m} x_i^2 &= \alpha^2; & (4.57) \\ x_1 + \omega x_2 &= 0. & (4.58) \end{aligned}$$

From Equation (4.58), we get $\omega x_2 = -x_1$ and thus $x_2 = \omega x_1$.

Equation (4.57) implies $x_1^2 + \omega^2 x_1^2 + \sum_{i=3}^{m} x_i^2 = \alpha^2$ and hence $\sum_{i=3}^{m} x_i^2 = \alpha^2$.

Put $x_i = \gamma_i$ and $a = x_1$, $i = 3, \cdots, m$.

We have the solutions of the form $(a, \omega a, \gamma_3, \cdots, \gamma_m)$ with $\sum_{i=3}^{m} \gamma_i^2 = \alpha^2$

$(\alpha^2 \neq 0)$ and thus $q\mathcal{S}(m-2, q)$ solutions.

(ii) $0 \neq \alpha^2 \neq \beta^2 \neq 0$.

The system becomes

$$\begin{aligned} x_1^2 + x_2^2 + \sum_{i=3}^{m} x_i^2 &= \alpha^2; && (4.59) \\ x_1 + \omega x_2 &= \frac{\alpha^2 - \beta^2}{2}. && (4.60) \end{aligned}$$

Equation (4.60) implies that $x_2 = -\omega \left(\frac{\alpha^2 - \beta^2}{2} - x_1 \right)$.

In addition, Equation (4.59) implies that

$$x_1^2 + \omega^2 \left(\frac{\alpha^2 - \beta^2}{2} - x_1 \right)^2 + \sum_{i=3}^{m} x_i^2 = \alpha^2;$$

and hence

$$x_1^2 - \left(\frac{\alpha^2 - \beta^2}{2} \right)^2 + 2 \left(\frac{\alpha^2 - \beta^2}{2} \right) x_1 - x_1^2 + \sum_{i=3}^{m} x_i^2 = \alpha^2.$$

Put $x_i = \gamma_i$, $i = 3, \cdots, m$. We get $x_1 = \frac{\alpha^2}{\alpha^2 - \beta^2} - \frac{1}{\alpha^2 - \beta^2} \sum_{i=3}^{m} \gamma_i^2 + \frac{\alpha^2 - \beta^2}{4}$.

In addition, we get

$$\begin{aligned} x_2 &= -\omega \left(\frac{\alpha^2 - \beta^2}{2} - x_1 \right) \\ &= -\omega \left(\frac{\alpha^2 - \beta^2}{4} - \frac{\alpha^2}{\alpha^2 - \beta^2} + \frac{1}{\alpha^2 - \beta^2} \sum_{i=3}^{m} \gamma_i^2 \right) \end{aligned}$$

$(0 \neq \alpha^2 \neq \beta^2 \neq 0)$; and thus $q^{m-2}\left(\frac{q-1}{2}\right)\left(\frac{q-3}{2}\right)$ solutions.

Summing all results, we obtain

$$\begin{aligned}\mathcal{B}(m,q) = q\mathcal{Z}(m,q) + 2q^{m-2}\left(\frac{q-1}{2}\right) + q\mathcal{S}(m-2,q) + q^{m-2}\left(\frac{q-1}{2}\right)\left(\frac{q-3}{2}\right)\\ - 2.\end{aligned}$$

Since we are dealing with $q \equiv 1 \pmod 4$ for $\omega^2 = -1$, $\omega \in \mathbb{F}_q$, we get in the following sub-cases of m:

(1) m even ($m-2$ even):

$\mathcal{Z}(m-2,q) = q^{m-3} + q^{\frac{m-2}{2}} - q^{\frac{m-4}{2}}$; and

$\mathcal{S}(m-2,q) = \frac{1}{2}\left(q^{m-2} - q^{m-3} - q^{\frac{m-2}{2}} + q^{\frac{m-4}{2}}\right).$

$$\begin{aligned}\mathcal{B}(m,q) &= q\left(q^{m-3} + q^{\frac{m-2}{2}} - q^{\frac{m-4}{2}}\right) + q^{m-2}\left(\frac{q-1}{2}\right)\\ &\quad + q\cdot\frac{1}{2}\left(q^{m-2} - q^{m-3} - q^{\frac{m-2}{2}} + q^{\frac{m-4}{2}}\right) + q^{m-2}\left(\frac{q-1}{2}\right)\left(\frac{q-3}{2}\right) - 2\\ &= \frac{q^{m-2}(q^2 - 1 + 4 + 2q - 2) + 2q^{\frac{m}{2}} - 2q^{\frac{m-2}{2}}}{4} - 2\\ &= \frac{q^{m-2}(q+1)^2 + 2q^{\frac{m-2}{2}}(q-1)}{4} - 2 = \mathcal{A}(m,q) \text{ since } q \equiv 1 \pmod 4.\end{aligned}$$

(2) m odd ($m-2$ odd):

We have $\mathcal{Z}(m-2,q) = q^{m-3}$; and

$\mathcal{S}(m-2,q) = \frac{1}{2}\left(q^{m-2} - q^{m-3} + q^{\frac{m-1}{2}} - q^{\frac{m-3}{2}}\right).$

Then

$$
\begin{aligned}
\mathcal{B}(m,q) &= q \cdot q^{m-3} + 2q^{m-2}\left(\frac{q-1}{2}\right) + q \cdot \frac{1}{2}\left(q^{m-2} - q^{m-3} + q^{\frac{m-1}{2}} - q^{\frac{m-3}{2}}\right) \\
&\quad + q^{m-2}\left(\frac{q-1}{2}\right)\left(\frac{q-3}{2}\right) - 2 \\
&= \frac{q^{m-2}(4+4q-4+q^2-4q+3+2q-2) + 2q^{\frac{m+1}{2}} - 2q^{\frac{m-1}{2}}}{4} - 2 \\
&= \frac{q^{m-2}(q^2+2q+1) + q^{\frac{m-3}{2}}(2q^2-2q)}{4} - 2 \\
&= \frac{q^{m-2}(q+1)^2 + q^{\frac{m-3}{2}}(3q^2-q^2-2q-1+1)}{4} - 2 \\
&= \frac{q^{m-2}(q+1)^2 + q^{\frac{m-3}{2}}(3q^2-2q-1)}{4} - 2 - q^{\frac{m-3}{2}}\left(\frac{q^2-1}{4}\right).
\end{aligned}
$$

Therefore $\mathcal{B}(m,q) = \mathcal{A}(m,q) - (-1)^{\frac{(q-1)(m-1)}{4}} q^{\frac{m-3}{2}}\left(\dfrac{q^2-1}{4}\right)$ since $q \equiv 1 \pmod 4$. □

We remark by [32, Lemma 3.19] that $\mathcal{B}(m,q)$ is well defined.

The main result is therefore in the following terms.

Theorem 4.20 *Let* $\Gamma = \mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})$ *be the integral distance graph with* $m \equiv 0 \pmod 2$, $q \equiv 1 \pmod 4$. *Then* Γ *is strongly regular.*

Chapter 5

Automorphism groups of the constituent graphs of integral distances graphs

In this chapter, we determine the automorphism groups of the basic constituent graphs of integral distance graphs. Since it was shown that they are all Cayley graphs on $\mathbb{F}_q^m$ under addition, it is enough for the determination of those groups to calculate the stabilizer subgroups of a chosen vertex. In our case, the $\mathbf{0}$ vector is convenient.

The case of dimension $m > 2$ has been studied in [32], so we restrict our attention to the case of dimension $m = 2$.

As with all combinatorial structures, the question of the automorphisms of integral point sets arises. In this case, they are two natural ways to define an automorphism:

Definition 5.1 An *integral automorphism* of the affine plane $\mathbb{F}_q^2$ is a permutation σ of $\mathbb{F}_q^2$ which preserves the integral distances; i.e., for all $\mathbf{x}, \mathbf{y} \in \mathbb{F}_q^2$,

$$N(\mathbf{x} - \mathbf{y}) \in \square_q \Longleftrightarrow N(\mathbf{x}^\sigma - \mathbf{y}^\sigma) \in \square_q.$$

If additionally the permutation σ is an element of the affine semi-linear group $\mathrm{A\Gamma L}_2(\mathbb{F}_q)$, then σ is called an *affine integral automorphism.*

We adopt the notation used in [21] to denote the group of all integral automorphisms by $\mathrm{Aut}(\mathbb{F}_q^2)$. The group of all affine integral automorphisms will be denoted by $\mathrm{AffAut}(\mathbb{F}_q^2)$.

$\mathrm{Aut}(\mathbb{F}_q^2)$ is exactly the automorphism group of the graph of integral distances $\mathfrak{G}_{2,q}$. It is clear that $\mathrm{AffAut}(\mathbb{F}_q^2)$ is a subgroup of $\mathrm{Aut}(\mathbb{F}_q^2)$ [21].

Recall that, if q is even, then any two points are at integral distance. Hence $\mathrm{Aut}(\mathbb{F}_q^2) = S_{\mathbb{F}_q^2}$ and $\mathrm{AffAut}(\mathbb{F}_q^2) = \mathrm{A\Gamma L}_2(\mathbb{F}_q)$. So, again as in the previous chapters, we shall only consider the case where q is odd.

Now we have the following characterisation of the affine integral automorphisms of $\mathbb{F}_q^2$.

Theorem 5.1 [21,29] *Let $q \notin \{5, 9\}$. Then $\mathrm{AffAut}(\mathbb{F}_q^2)$ written as mappings $\mathbb{F}_q^2 \longrightarrow \mathbb{F}_q^2$, is generated by*

(1) *the translations $\lambda_{\mathbf{u}} : \mathbf{x} \longmapsto \mathbf{x} + \mathbf{u}$ for all $\mathbf{u} \in \mathbb{F}_q^2$;*

(2) *the reflexion $R : (x_1, x_2) \longmapsto (x_2, x_1)$;*

(3) *the spiral collineations $M : (x_1, x_2) \longmapsto (x_1, x_2)\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ for $a, b \in \mathbb{F}_q$ with $a^2 + b^2 \in \square_q^*$; and,*

(4) *The Frobenius automorphisms $\sigma : (x_1, x_2) \longmapsto (x_1^p, x_2^p)$, with p the characteristic of $\mathbb{F}_q$.*

In [29], it has been shown that no other permutation of $\mathbb{F}_q^2$ than those mentioned above is an affine integral automorphism of $\mathbb{F}_q^2$.

From them, we easily deduce the order of $\mathrm{AffAut}(\mathbb{F}_q^2)$ in the following.

Corollary 5.2

$$|\mathrm{AffAut}(\mathbb{F}_q^2)| = \begin{cases} q^2(q-1)^2 r & \text{if } q \equiv 1 \pmod 4; q \notin \{5, 9\}; \\ q^2(q+1)(q-1)r & \text{if } q \equiv 3 \pmod 4. \end{cases}$$

Proof. This follows immediately from Theorems 2.20 and 5.1. □

Now we consider the case where $q \equiv 3 \pmod 4$ in the following result to determine the order of $\mathrm{Aut}(\mathbb{F}_q^2)$ for it.

Theorem 5.3 *Let $q \equiv 3 \pmod 4$. $\mathrm{Aut}(\mathbb{F}_q^2)$ is isomorphic to the automorphism group of the Paley graph $P(q^2)$.*

Proof. To see that $\mathrm{Aut}(\mathbb{F}_q^2) \cong \mathrm{Aut}\ P(q^2)$, identify first the set $\mathbb{F}_q^2$ with the extension field $\mathbb{F}_q[i]$, where $i^2 = -1$ (notice that $-1 \notin \square_q$ in $\mathbb{F}_q$ as $q \equiv 3 \pmod 4$); and by Corollary 2.15 we have $N(x-y) = (x-y)^{q+1}$.

As the mapping $x \mapsto x^{q+1}$ maps exactly the square elements of $\mathbb{F}_q[i]$ onto the square elements of $\mathbb{F}_q$, the required isomorphism follows. □

Recall that, given an arbitrary prime power $q' = p^s$ such that $q' \equiv 1 \pmod 4$, the Paley graph $P(q')$ has vertex set $\mathbb{F}_{q'}$, and for distinct $x, y \in \mathbb{F}_{q'}$, $x \sim y$ if and only if $x - y \in \square_{q'}$ by Definition 3.1. The group Aut $P(q')$ was completely determined by Carlitz in [8] where it was proved that

$$\mathrm{Aut}\ P(q') = \{x \mapsto ax^{p^k} + b : a \in \square_{q'}, a \neq 0, b \in \mathbb{F}_{q'}, k \in \{0, 1, \cdots, s-1\}\}. \quad (5.1)$$

With the above results, we shall state the following result.

Proposition 5.4 [21, 26, 29] *Let Γ be the integral distance graph over $\mathbb{F}_q^2$, $q = p^r$, p prime, with $q \equiv 3 \pmod 4$. Then $|\mathrm{Aut}\ \Gamma| = q^2(q^2-1)r$.*

Proof. This follows immediately from Theorem 5.3 and Equation (5.1). □

According to the following theorem, to which we give our own proof for completeness, we have to look at the isomorphism between $\mathrm{AffAut}(\mathbb{F}_q^2)$ and $\mathrm{Aut}(\mathbb{F}_q^2)$ in many cases of q.

Theorem 5.5 [21] *If either $q \equiv 3 \pmod 4$ or $q \neq 5$, q prime, then* $\mathrm{Aut}(\mathbb{F}_q^2) = \mathrm{AffAut}(\mathbb{F}_q^2)$.

Proof. (1) Let $q \equiv 3 \pmod 4$. Since $q^2 \equiv 1 \pmod 4$ and the corresponding integral distance graph is isomorphic to the Paley graph $P(q^2)$ by Theorem 5.3, the result follows immediately from Equation (5.1), Corollary 5.2, and Proposition 5.4.

(2) For the case $q \equiv 1 \pmod 4$, the result also follows from Corollary 5.2 since $q = p$; i.e., $r = 1$. For the rest, refer to [21, Theorem 9]. □

In the remaining case, $q \equiv 1 \pmod 4$, we consider the following permutations of $\mathbb{F}_q^2$. These automorphisms have already been defined in [26].

$\lambda_{(a,b)} : (x_1, x_2) \longmapsto (x_1 + a, x_1 + b),\ a, b \in \mathbb{F}_q,$

$R : (x_1, x_2) \longmapsto (x_2, x_1),$

$M_a^+ : (x_1, x_2) \longmapsto (ax_1, ax_2),\ a \in \mathbb{F}_q^*,$

$M_a^- : (x_1, x_2) \longmapsto (ax_1, a^{-1}x_2),\ a \in \mathbb{F}_q^*,$

$A_1 : (x_1, x_2) \longmapsto (x_1^p, x_2)$, and $A_2 : (x_1, x_2) \longmapsto (x_1, x_2^p)$.

Let F be the group generated by the permutations of $\mathbb{F}_q^2$ defined above. We shall show that F is a subgroup of Aut Γ_i, where $\Gamma_i = \mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2, 3$, with S_1 and S_2 the base subsets of $\mathbb{F}_q^2$ defined in Chapter 3; and S_3 the complement of $S \cup \{\mathbf{0}\}$ in $\mathbb{F}_q^2$, $S = S_1 \cup S_2$.

Moreover, it will be shown that F in its action on $V(\Gamma_i)$, $i = 1, 2, 3$, is primitive. That is, Aut Γ_i, $i = 1, 2, 3$, is therefore primitive.

We first show that F is a subgroup of Aut Γ_i, $i = 1, 2, 3$.

Lemma 5.6 *Let S_i, $i = 1, 2, 3$, be the sets defined as in* Equations (3.1), (3.2), (3.3) *respectively Let $\Gamma_i = \mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2, 3$, be their corresponding Cayley graphs as defined in* Chapter 3*. Then* Aut Γ_i *contains F as a subgroup for each* $i = 1, 2, 3$.

Proof. First, it is obvious that $\lambda_{(a,b)}$ and R are permutations of $V(\Gamma_i)$, $i = 1, 2, 3$.

By Pigeonhole's Principle, it is enough to show that $M_a^{\pm}$ and A_i, $i = 1, 2$, are one-to-one.

Now:

(i) $M_a^+(x_1, x_2) = M_a^+(y_1, y_2) :\Longleftrightarrow (ax_1, ax_2) = (ay_1, ay_2) \Longleftrightarrow (x_1, x_2) = (y_1, y_2)$.

(ii) $M_a^-(x_1, x_2) = M_a^-(y_1, y_2) :\Longleftrightarrow (ax_1, a^{-1}x_2) = (ay_1, a^{-1}y_2)$. This implies that $ax_1 = ay_1$ and $a^{-1}x_2 = a^{-1}y_2$. Thus $(x_1, x_2) = (y_1, y_2)$.

(iii) For $A_1(x_1, x_2) = A_1(y_1, y_2)$, we have $(x_1^p, x_2) = A_1(y_1^p, y_2)$ if and only if $(x_1, x_2) = (y_1, y_2)$. Similarly, $A_2(x_1, x_2) = A_2(y_1, y_2)$ if and only if $(x_1, x_2) = (y_1, y_2)$.

Thus every element of F is a permutation of $\mathbb{F}_q^2$.

For adjacency, $\lambda_{(a,b)}$ are left translations. Hence by Theorem 2.5, they are automorphisms of Γ.

Since $R, M_a^{\pm}, A_i$, $i = 1, 2$, stabilize $\mathbf{0}$, it is enough to show that the image of $\mathbf{x} := (x_1, x_2)$ by the above permutation is also an element of S_i, $i = 1, 2, 3$.

Clearly, $(x, y) \in S_i$ if and only if $(y, x) \in S_i$, for each $i = 1, 2, 3$.

For any $(x, y) \in S_i$, $i = 1, 2$; i.e., $xy \in \Box_q$, we have that

$$\begin{aligned} N^{\phi}(ax, ay) &= a^2xy; \\ N^{\phi}(ax, a^{-1}y) &= xy; \\ N^{\phi}(x^p, y) &= x^py = x^{p-1} \cdot xy \in \Box_q \text{ since } p\text{is odd}; \\ N^{\phi}(x, y^p) &= xy^p = xy \cdot y^{p-1} \in \Box_q \text{ since } p \text{ is odd}. \end{aligned}$$

Similar arguments hold as the latter are also valid for $(x, y) \in S_3$; i.e., $xy \notin \Box_q$. Hence R, $M_a^{\pm}$, and A_i, $i = 1, 2$, are automorphisms of Γ_i, $i = 1, 2, 3$. Therefore F is a subgroup of Aut Γ_i. □

Let Λ be the subgroup of F generated by all translations $\lambda_{(a,b)}$ with $a, b \in \mathbb{F}_q$. For the sake of completeness, we show that the following properties of F hold.

Lemma 5.7 [26] *With notation as above we have the following:*

(i) Λ *is normal in* F.

(ii) $|F| = (q(q-1)r)^2$.

(iii) *The stabilizer* $F_{\mathbf{0}}$ *has orbits* $S_0 = \{\mathbf{0}\}$, S_1, S_2, *and* S_3; *where* $S_1 = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*)$, $S_2 = \{(x_1, x_2) \in \mathbb{F}_q^2 : x_1x_2 \in \Box_q^*\}$, *and* $S_3 = \mathbb{F}_q^2 \setminus (S_0 \cup S_1 \cup S_2)$. *In particular,* F *has rank 4.*

(iv) F *is primitive.*

Proof. (i) We show that $\Lambda \triangleleft F$.

It is sufficient to show that the subgroups $\langle R \rangle$, $\langle M_a^{\pm} \rangle$, and $\langle A_i \rangle$, $i = 1, 2$, normalize $\Lambda = \langle \lambda_{(a,b)} \rangle$; $a, b \in \mathbb{F}_q$.

It is easily shown that $R = R^{-1}$, $(M_a^+)^{-1} = M_{a^{-1}}^+$, and $(M_a^-)^{-1} = M_{a^{-1}}^-$.

In addition, it can be shown that $(x, y)^{A_1^{-1}} = (x^{p^{r-1}}, y)$ and $(x, y)^{A_2^{-1}} = (x, y^{p^{r-1}})$ since $x = x^q = x^p \cdot x^{p^{r-1}}$.

Now we compute the conjugates of $\lambda_{(a,b)}$ by R, $M_a^{\pm}$, and A_i, $i = 1, 2$. We have

(1) $(x, y)^{R^{-1}\lambda_{(a,b)}R} = (x + b, y + a)$; i.e., $R^{-1}\lambda_{(a,b)}R = \lambda_{(b,a)}$.

(2) $(x, y)^{(M_c^+)^{-1}\lambda_{(a,b)}M_c^+} = (x + ca, y + cb)$; i.e., $(M_c^+)^{-1}\lambda_{(a,b)}M_c^+ = \lambda_{(ca,cb)}$.

(3) $(x, y)^{(M_c^-)^{-1}\lambda_{(a,b)}M_c^-} = (x + ca, y + c^{-1}b)$; i.e, $(M_c^-)^{-1}\lambda_{(a,b)}M_c^- = \lambda_{(ca,c^{-1}b)}$.

(4) $(x, y)^{A_1^{-1}\lambda_{(a,b)}A_1} = (x + a^p, y + b)$; i.e., $A_1^{-1}\lambda_{(a,b)}A_1 = \lambda_{(a^p,b)}$.

Similar to (4), it is easily shown that $A_2^{-1}\lambda_{(a,b)}A_2 = \lambda_{(a,b^p)}$.

Hence $\langle R\rangle$, $\langle M_a^{\pm}\rangle$, and $\langle A_i\rangle$, $i = 1, 2$, normalize Λ, and therefore Λ is normal in F.

(ii) To calculate the order of F, we first compute the orders of subgroups Λ, $\langle R\rangle$, $\langle M_a^{\pm}\rangle$, and $\langle A_i\rangle$, $i = 1, 2$. Finally, we show that F is isomorphic to the direct product of them.

Obviously, the group Λ is isomorphic to the additive group $\mathbb{F}_q^2$ and thus $|\Lambda| = q^2$. Clearly, $\langle R\rangle$ is isomorphic to the symmetric group $S_{[2]}$. Thus $|\langle R\rangle| = 2$.

Let us consider the group $\langle M_a^{\pm}\rangle = \langle M_a^+, M_b^-\rangle$, $a, b \in \mathbb{F}_q^*$. This is the group generated by the permutations of the form

$M_a^+M_b^- : (x, y) \longmapsto (x, y)^{M_a^+M_b^-} = (bax, b^{-1}ay).$, $a \neq b$;

$M_a^-M_b^+ : (x, y) \longmapsto (x, y)^{M_a^-M_b^+} = (bax, ba^{-1}y).$, $a \neq b$; and

$M_a^+M_a^- : (x, y) \longmapsto (x, y)^{M_a^+M_a^-} = (a^2x, y).$

Clearly, $\langle M_a^+, M_b^-\rangle = \langle M_a^-, M_b^+\rangle$ since $b^{-1}a$ and ba^{-1} run through all elements of $\mathbb{F}_q^*$. The order of each one is $\dfrac{(q-1)^2}{2} - \dfrac{q-1}{2} = \dfrac{(q-1)(q-2)}{2}$. Also, the order of $\langle M_a^+, M_a^-\rangle$ is $\dfrac{q-1}{2}$. Summing up all of them, we obtain $|\langle M_a^{\pm}\rangle| = \dfrac{(q-1)^2}{2}$.

It is clear that the subgroups $\langle A_i\rangle$, $i = 1, 2$, are isomorphic to the groups of automorphisms of $\mathbb{F}_q$ called *Frobenius automorphisms.* Thus $|\langle A_i\rangle| = r$ since $q = p^r$.

It remains to show that F is isomorphic to the direct product of Λ, $\langle R\rangle$, $\langle M_a^{\pm}\rangle$, and $\langle A_i\rangle$, $i = 1, 2$.

Put $D = \langle R, M_a^{\pm}, A_i, i = 1, 2\rangle$ and $C = \langle R, A_i, i = 1, 2\rangle$.

Since Λ is normal in F by (i), it is sufficient to show that $\langle M_a^{\pm}\rangle$ is normal in D; $\langle A_i, i = 1, 2\rangle$ is normal in C; and A_1 and A_2 commute.

Let us determine the conjugates of $M_a^{\pm}$ by R and A_i, $i = 1, 2$; the conjugate of A_i, $i = 1, 2$ by R; and the conjugate of A_i by A_j, $i, j = 1, 2$ and $i \neq j$.

We have for all $(x, y) \in \mathbb{F}_q^2$:

(1) $(x, y)^{R^{-1}M_a^+R} = (ax, ay)$ and $(x, y)^{R^{-1}M_a^-R} = (a^{-1}x, ay)$; which give

$$R^{-1}M_a^+R = M_a^+ \text{ and } R^{-1}M_a^-R = (M_a^-)^{-1}.$$

(2) $(x, y)^{A_1^{-1}M_a^{\pm}A_1} = (a^{p-1}x, y)^{M_a^{\pm}}$ and $(x, y)^{A_2^{-1}M_a^{\pm}A_2} = (x, a^{\pm(p-1)}y)^{M_a^{\pm}}$.

It follows that, $\langle M_a^{\pm}\rangle \lhd D$ since $(a^{p-1}x, y), (x, a^{\pm(p-1)}y) \in \mathbb{F}_q^2$.

Additionally we have

(3) $(x,y)^{R^{-1}A_1R} = (x, y^p)$ and $(x,y)^{A_2^{-1}A_1A_2} = (x^p, y)$. This implies that

$$R^{-1}A_1R = A_2 \text{ and } A_2^{-1}A_1A_2 = A_1.$$

Similarly, we get $R^{-1}A_2R = A_1$ and $A_1^{-1}A_2A_1 = A_2$.

This shows that $\langle A_1, A_2\rangle$ is normal in $C = \langle R, A_1, A_2\rangle$ and A_i is normal in $\langle A_1, A_2\rangle$, $i = 1, 2$.

Thus we have $\Lambda \lhd F$; $\langle M_a^{\pm}\rangle \lhd D$; and $\langle A_1, A_2\rangle = \langle A_1\rangle \times \langle A_2\rangle \lhd C$.

Hence F is isomorphic to $\Lambda \times \langle M_a^{\pm}\rangle \times \langle A_1\rangle \times \langle A_2\rangle \times \langle R\rangle$, and therefore

$$|F| = q^2 \cdot \frac{(q-1)^2}{2} \cdot r^2 \cdot 2 = (q(q-1)r)^2.$$

(iii) Since $M_a^{\pm}$, R, and A_i, $i = 1, 2$, stabilize $\mathbf{0} = (0,0)$, we find that $F_{\mathbf{0}} = \langle M_a^{\pm}, R, A_i, i = 1, 2\rangle = D$.

Now we determine the orbits of $F_{\mathbf{0}}$ in $\mathbb{F}_q^2$. Since $(0,0)$ is an orbit of $F_{\mathbf{0}}$, it is enough to find all the other orbits.

Take the vectors $(1,0)$ and $(1,1)$ in $\mathbb{F}_q^2$. We have:

(1) $(1,0)^R = (0,1)$; $(1,0)^{M_a^{\pm}} = (a, 0)$; $(1,0)^{RM_a^{\pm}} = (0, a^{\pm 1})$; and $(1,0)_i^A = (1,0)$, $i = 1, 2$ and $a \in \mathbb{F}_q^*$.

(2) $(1,1)^{M_a^{\pm}} = (a, a^{\pm 1})$; $(1,1)_i^A = (1,1)$, $i = 1, 2$; $(1,1)^{M_a^{\pm}A_1} = (a^p, a^{\pm 1})$; and $(1,1)^{M_a^{\pm}A_2} = (a, a^{\pm p})$.

Since $p \pm 1$ is even and the mapping $a \longmapsto a^p$ is a Frobenius automorphism, it follows that

$$(1,0)^{F_{\mathbf{0}}} = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*) = S_1 \text{ and } (1,1)^{F_{\mathbf{0}}} = \{(x,y) \in \mathbb{F}_q^2 : xy \in \square_q^*\} = S_2.$$

Clearly, $(1,\alpha)^{F_{\mathbf{0}}} = \{(x,y) \in \mathbb{F}_q^2 : xy \notin \square_q\} = S_3$ for some $\alpha \notin \square_q$. Hence $S_0 = \{(0,0)\}$, S_1, S_2, and S_3 are orbits of $F_{\mathbf{0}}$. Therefore F has rank 4.

(iv) We apply Theorem 2.30 to F. This states that, F is primitive if and only if Graph(Δ) is connected for each non-diagonal orbital Δ of F. In our case, however, Graph(Δ) $=$ Cay($\mathbb{F}_q^2, S_i$), where S_i is the orbit given in (iii) of Lemma 5.7 and $i > 0$. To show that Cay($\mathbb{F}_q^2, S_i$) is connected for $i = 1, 2, 3$, it is sufficient to show that each S_i generates $\mathbb{F}_q^2$.

(1) Evidently, in $S_1 = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*)$; if we take $\mathbf{x} = (x, 0)$ and $\mathbf{y} = (0, y)$, $x, y \in \mathbb{F}_q^*$, then

$a\mathbf{x} + b\mathbf{y} = (ax, by) \in \mathbb{F}_q^2$ for all $a, b \in \mathbb{F}_q$. Thus $\langle S_1 \rangle = \mathbb{F}_q^2$.

(2) In $S_2 = \{(x, y) \in \mathbb{F}_q^2 : xy \in \square_q^*\}$, let $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$ in S_2; i.e., $x_1x_2, y_1y_2 \in \square_q^*$.

Then for $a, b \in \mathbb{F}_q$, $a\mathbf{x} + b\mathbf{y} = (ax_1 + by_1, ax_2 + by_2)$.

Since the two components run over all elements of $\mathbb{F}_q$, it follows that S_2 generates $\mathbb{F}_q^2$. Similarly, $S_3 = \{(x, y) \in \mathbb{F}_q^2 : xy \notin \square_q\}$ is also a generator of $\mathbb{F}_q^2$. Hence each digraph Graph(Δ) is connected. Therefore F is primitive. □

The orbits S_i, $i = 1, 2, 3$, given in (iii) of Lemma 5.7 are obviously the Cayley sets in the constituent graphs $\Gamma_i = \text{Cay}(\mathbb{F}_q^2, S_i)$. The latter graphs have been considered in Chapters 3 and 4 as Cayley and strongly regular graphs. What follows next, is to study the automorphism groups of each Γ_i, $i = 1, 2, 3$, the main thrust of this chapter. First we look at the automorphism group of Γ_1.

5.1 The automorphism group of $\Gamma_1 = \text{Cay}(\mathbb{F}_q^2, S_1)$.

In this section, we fully determine the automorphism group of $\Gamma_1 = \text{Cay}(\mathbb{F}_q^2, S_1)$ with $S_1 = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*) = \{(x_1, x_2) \in \mathbb{F}_q^2 \setminus \{(0, 0)\} : x_1x_2 = 0\}$.

Let $\mathbf{x} := (x_1, x_2)$ and $\mathbf{y} := (y_1, y_2)$ be vertices in Γ_1. Then $\mathbf{x}$ and $\mathbf{y}$ are adjacent in Γ_1 if and only if

$$N^\phi(\mathbf{x} - \mathbf{y}) = (x_1 - y_1)(x_2 - y_2) = 0; \text{ i.e.,}$$

$x_i = y_i$ for exactly one $i = 1, 2$.

We shall say that $\sigma \in \text{Aut } \Gamma_1$ if and only if

$$N^\phi(\mathbf{x} - \mathbf{y}) = 0 \Longleftrightarrow N^\phi(\mathbf{x}^\sigma - \mathbf{y}^\sigma) = 0.$$

Since Γ_1 is vertex-transitive by Theorem 2.5, it is sufficient to determine the stabilizer $(\text{Aut } \Gamma_1)_{\mathbf{0}}$ of $(0, 0)$ in Aut Γ_1 (by Orbit-Stabilizer Theorem).

In the subgroup $(\text{Aut } \Gamma_1)_{\mathbf{0}}$, σ will permute only the non-zero vectors of $\mathbb{F}_q^2$. Here, it can be shown that any permutation in $\mathbb{F}_q^*$ for exactly one component and any permutation of components in any element of $\mathbb{F}_q^2$ is an element of the subgroup $(\text{Aut } \Gamma_1)_{\mathbf{0}}$ in the following result.

Lemma 5.8 *Let H be a permutation group of $V(\Gamma_1)$ generated by*

$R : (x_1, x_2) \longmapsto (x_2, x_1)$*;*

$\pi_{\sigma_1} : (x_1, x_2) \longmapsto (x_1^{\sigma_1}, x_2)$*; and*

$\pi_{\sigma_2} : (x_1, x_2) \longmapsto (x_1, x_2^{\sigma_2})$*; where $\sigma_1, \sigma_2 \in S_{\mathbb{F}_q}$ and $0^{\sigma_i} = 0$, $i = 1, 2$.*

Then H is a subgroup of the stabilizer $(\text{Aut } \Gamma_1)_{\mathbf{0}}$ *of* $(0, 0)$ *in* $\text{Aut } \Gamma_1$.

Proof. Clearly, R, π_{σ_i}, $i = 1, 2$, stabilize $(0, 0)$.

In order to show that H is a subgroup of $(\text{Aut } \Gamma_1)_{\mathbf{0}}$, it is sufficient to show that R, π_{σ_i}, $i = 1, 2$, preserve the adjacency structure in Γ_1.

For any vertices $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$ in Γ_1, $\{\mathbf{x}, \mathbf{y}\} \in E(\Gamma_1)$ if and only if $(x_1 - y_1)(x_2 - y_2) = 0$.

It follows that $N^{\phi}(\mathbf{x}^R - \mathbf{y}^R) = (x_2 - y_2)(x_1 - y_1) = 0$. Thus $R \in (\text{Aut } \Gamma_1)_{\mathbf{0}}$.

For $\pi_{\sigma_1} : (x_1, x_2) \longmapsto (x_1^{\sigma_1}, x_2)$, we have

$$N^{\phi}(\mathbf{x}^{\pi_{\sigma_1}} - \mathbf{y}^{\pi_{\sigma_1}}) = (x_1^{\sigma_1} - y_1^{\sigma_1})(x_2 - y_2).$$

Since σ_1 is a permutation of $\mathbb{F}_q$, it follows that $x_1^{\sigma_1} = y_1^{\sigma_1} \iff x_1 = y_1$.

However, if $x_1 = y_1$, then $\mathbf{x}$ is adjacent to $\mathbf{y}$. Thus $\mathbf{x}^{\pi_{\sigma_1}}$ is adjacent to $\mathbf{y}^{\pi_{\sigma_1}}$.

With a similar argument applied to π_{σ_1}, it can also be shown that π_{σ_2} preserves the adjacency structure of Γ_1.

Therefore $H = \langle R, \pi_{\sigma_i}, i = 1, 2\rangle$ is a subgroup of the stabilizer $(\text{Aut } \Gamma_1)_{\mathbf{0}}$ of $(0, 0)$ in $\text{Aut } \Gamma_1$. □

As we have just shown that H is a subgroup of $(\text{Aut } \Gamma_1)_{\mathbf{0}}$, we also show the maximality of H in the symmetric group S_{S_1}. (See further details of maximal subgroups of a symmetric group in [3, 37]).

Lemma 5.9 *H is a maximal subgroup of the symmetric group S_{S_1}, where S_1 is the Cayley set of* Γ_1.

Proof. Consider the action of H on $S_1 = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*)$.

Let $\Delta = (\mathbb{F}_q^*, 0)$. Then we have $\Delta^R = (0, \mathbb{F}_q^*)$, and $\Delta^{\pi_{\sigma_1}} = \Delta^{\pi_{\sigma_2}} = \Delta$. So $(\mathbb{F}_q^*, 0)$ and $(0, \mathbb{F}_q^*)$ are blocks for H.

Let $\Delta_1 = (\mathbb{F}_q^*, 0)$ and $\Delta_2 = (0, \mathbb{F}_q^*)$. Then it is shown by [37, Proposition 2.1] that the subgroup of S_{S_1} isomorphic to $S_{\Delta_i} \wr_{[2]} S_{[2]}$ is maximal in S_{S_1} (we use the notation $S_{[2]}$

for a symmetric group instead of S_2 for a Cayley set). This is also isomorphic to the wreath product $S_{\mathbb{F}_q^*} \wr S_{[2]}$.

Hence, it is sufficient to check whether H is isomorphic with the wreath product of $S_{\mathbb{F}_q^*}$ by $S_{[2]}$.

Here we check the normality of R and π_{σ_i}, $i = 1, 2$, in H.

Let us determine the conjugates of R with π_{σ_i}, $i = 1, 2$; and the conjugates of π_{σ_i} by π_{σ_i} and R, $i, j = 1, 2$ and $i \neq j$.

Clearly, we have $R = R^{-1}$, $\pi_{\sigma_1}^{-1} : (x_1, x_2) \longmapsto (x_1^{\sigma_1^{-1}}, x_2)$, and $\pi_{\sigma_2}^{-1} : (x_1, x_2) \longmapsto (x_1, x_2^{\sigma_2^{-1}})$.

It is easily shown that,

$$(x_1, x_2)^{R^{-1}\pi_{\sigma_1}R} = (x_1, x_2^{\sigma_1}) \text{ and } (x_1, x_2)^{\pi_{\sigma_1}^{-1}\pi_{\sigma_1}\pi_{\sigma_2}} = (x_1^{\sigma_1}, x_2).$$

This implies that $R^{-1}\pi_{\sigma_1}R = \pi_{\sigma_2}$ and $\pi_{\sigma_2}^{-1}\pi_{\sigma_1}\pi_{\sigma_2} = \pi_{\sigma_1}$.

Similarly, we have $R^{-1}\pi_{\sigma_2}R = \pi_{\sigma_1}$ and $\pi_{\sigma_1}^{-1}\pi_{\sigma_2}\pi_{\sigma_1} = \pi_{\sigma_2}$.

It follows that π_{σ_1} and π_{σ_2} commute, and R interchanges π_{σ_1} with π_{σ_2}.

Thus $\langle \pi_{\sigma_1}, \pi_{\sigma_2} \rangle = \langle \pi_{\sigma_1} \rangle \times \langle \pi_{\sigma_2} \rangle$ is normal in H, where $\langle \pi_{\sigma_i} \rangle$ is isomorphic with $S_{\mathbb{F}_q^*}$, $i = 1, 2$, and R is isomorphic with $S_{[2]}$.

Hence $H \cong (S_{\mathbb{F}_q^*} \times S_{\mathbb{F}_q^*}) \rtimes S_{[2]} = S_{\mathbb{F}_q^*} \wr S_{[2]}$.

Therefore H is maximal in S_{S_1}. □

From the above result, it is convenient to identify the subgroup H of $(\text{Aut } \Gamma_1)_{\mathbf{0}}$ with the wreath product $S_{\mathbb{F}_q^*} \wr S_{[2]}$. Now we have to prove the converse of Lemma 5.8 to obtain the following.

Corollary 5.10 $H = (\text{Aut } \Gamma_1)_{\mathbf{0}}$.

Proof. By maximality of H, this follows immediately. □

As the conclusion on this matter, we have the following result.

Theorem 5.11 *Let* $\Gamma_1 = \text{Cay}(\mathbb{F}_q^2, S_1)$ *with* $S_1 = (\mathbb{F}_q^*, 0) \cup (0, \mathbb{F}_q^*)$.

Let H *and* $\Lambda = \langle \lambda_{(a,b)} \rangle$ *be the subgroups of* Aut Γ_1 *defined above. Then*

(i) Aut $\Gamma_1 = \Lambda H$*;*

(ii) $|\text{Aut }\Gamma_1| = 2(q!)^2$.

Proof. (i) Clearly, the regular subgroup $\Lambda = \langle \lambda_{(a,b)} \rangle$ of Aut Γ_1 is the orbit of the vector $(0, 0)$ in Aut Γ_1.

By Corollary 5.10, $H = \langle R, \pi_{\sigma_i}, i = 1, 2 \rangle$ is the stabilizer of $(0, 0)$ in Aut Γ_1. Thus (i) follows by orbit-stabilizer theorem.

(ii) Now we determine the order of Aut Γ_1.

First we have $|\Lambda| = |\langle \lambda_{(a,b)} \rangle| = q^2$; and $|H| = |S_{\mathbb{F}_q^*} \wr S_{[2]}| = 2((q-1)!)^2$.

Thus by orbit-stabilizer theorem, we obtain

$$\begin{aligned} |\text{Aut }\Gamma_1| &= |\mathbf{0}^{\text{Aut }\Gamma_1}||(\text{Aut }\Gamma_1)_{\mathbf{0}}| \\ &= |\Lambda| \cdot |H| \\ &= q^2 \cdot 2((q-1)!)^2 \\ &= 2(q!)^2. \end{aligned}$$

□

5.2 The automorphism groups of $\Gamma_2 = \text{Cay}(\mathbb{F}_q^2, S_2)$, $\Gamma_3 = \text{Cay}(\mathbb{F}_q^2, S_3)$ and $\Gamma = \text{Cay}(\mathbb{F}_q^2, S)$ with $S = S_1 \cup S_2$ and $S_3 = \mathbb{F}_q^2 \setminus (S \cup \{\mathbf{0}\})$

In this section, we determine the automorphism group of $\Gamma_2 = \text{Cay}(\mathbb{F}_q^2, S_2)$ with $S_2 = \{(x_1, x_2) \in \mathbb{F}_q^2 : x_1x_2 \in \square_q \setminus \{0\}\}$.

Recall that if given $\mathbf{s} \in S_2$, $\mathbf{x}$ and $\mathbf{y}$ are adjacent vertices in Γ_2 if and only if $\mathbf{x} - \mathbf{y} = \mathbf{s}$.

Put $\mathbf{x} := (x_1, x_2)$ and $\mathbf{y} := (y_1, y_2)$. Then we have

$\mathbf{s} = (x_1 - y_1, x_2 - y_2)$. That is, $\mathbf{s} \in S_2$ if and only if $(x_1 - y_1)(x_2 - y_2) \in \square_q \setminus \{0\}$.

It means that the norm should be a non-zero square. This implies that the corresponding components should not equal as in the previous case of Γ_1.

By Lemma 5.6, Aut Γ_2 contains the group F generated by the permutations $\lambda_{a,b}$, R, $M_a^{\pm}$, and A_i, $i = 1, 2$, and hence primitive by Lemma 5.7(iv).

According to the results from Theorem 5.1 and Lemma 5.6, we find that the results for this case are the same as in Lemmas 5.6 and 5.7, so that Aut Γ_2 and Aut Γ may coincide.

To see the isomorphism between Aut Γ_2 and Aut Γ, we have to look at the isomorphism of graphs $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$ and $\Gamma_3 = \mathrm{Cay}(\mathbb{F}_q^2, S_3)$, with $S_3 = \mathbb{F}_q^2 \setminus (S \cup \{\mathbf{0}\})$, $S = S_1 \cup S_2$.

Lemma 5.12 *Consider the graphs* $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$ *and* $\Gamma_3 = \mathrm{Cay}(\mathbb{F}_q^2, S_3)$ *with* $S_3 = \mathbb{F}_q^2 \setminus (S_1 \cup S_2 \cup \{\mathbf{0}\})$. *The linear mapping* $\tau_\alpha : V(\Gamma_2) \longrightarrow V(\Gamma_3)$ *defined by*

$$\tau_\alpha : (x_1, x_2) \longmapsto (\alpha x_1, x_2) \text{ with } \alpha \notin \square_q$$

is an automorphism of $\mathbb{F}_q^2$.

Proof. We first show that τ_α, $\alpha \notin \square_q$, is $\mathbb{F}_q$-linear.

Let $\mathbf{x} = (x_1, x_2)$, $\mathbf{y} = (y_1, y_2)$ be elements of $\mathbb{F}_q^2$ and $k \in \mathbb{F}_q$.

Then

$$\begin{aligned}(\mathbf{x}+\mathbf{y})^{\tau_\alpha} &= (\alpha(x_1 + y_1), x_2 + y_2) \\ &= (\alpha x_1, y_1) + (\alpha x_2, y_2) \\ &= \mathbf{x}^{\tau_\alpha} + \mathbf{y}^{\tau_\alpha}\end{aligned}$$

and

$$(k\mathbf{x})^{\tau_\alpha} = (\alpha k x_1, k x_2) = k\mathbf{x}^{\tau_\alpha}.$$

Thus τ_α is $\mathbb{F}_q$-linear.

Suppose that we have $\mathbf{x}^{\tau_\alpha} = \mathbf{y}^{\tau_\alpha}$. Then

$(x_1, x_2)^{\tau_\alpha} = (y_1, y_2)^{\tau_\alpha} :\Longleftrightarrow (\alpha x_1, x_2) = (\alpha y_1, y_2)$.

This is equivalent to $\alpha x_1 = \alpha y_1$ and $x_2 = y_2$.

Thus $x_1 = y_1$ and $x_2 = y_2$.

By Pigeonhole's Principle it follows that τ_α is a bijection and hence an automorphism of $\mathbb{F}_q^2$. □

Corollary 5.13 *Let* Γ_2 *and* Γ_3 *be graphs defined above. Then*

(i) $\Gamma_2 \cong \Gamma_3$*;*

(ii) Aut Γ = Aut Γ_3 = Aut Γ_2.

Proof. (i) Consider the Cayley sets S_2 and S_3 corresponding to the graphs Γ_2 and Γ_3, respectively.

Let $\mathbf{x} := (x_1, x_2)$ be an element of S_2. Then $N^{\phi}(\mathbf{x}) = x_1x_2 \in \square_q \setminus \{0\}$. It follows that, for any $\alpha \notin \square_q$, $\mathbf{x}^{\tau_\alpha} = (\alpha x_1, x_2)$ and $N^{\phi}(\mathbf{x}^{\tau_\alpha}) = \alpha x_1 x_2 \notin \square_q$.

Thus $\mathbf{x}^{\tau_\alpha} \in \mathbb{F}_q^2 \setminus (S_1 \cup S_2 \cup \{\mathbf{0}\}) = S_3$. Hence $S_2^{\tau_\alpha} = S_3$ by Lemma 5.12; and (i) follows immediately by Proposition 2.6, Theorem 4.5, and the proof of the Corollary 4.10(i).

(ii) This follows immediately from (i) since Γ_3 is the complement of Γ by Proposition 2.4. □

From the results above, it is sufficient to determine the automorphism group of $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$.

In the following result, it is shown that $\mathrm{Aut}(\mathbb{F}_q^2)$ is not isomorphic to $\mathrm{AffAut}(\mathbb{F}_q^2)$ for all the values of $q \equiv 1 \pmod 4$, $q = p^r$, with $r \geq 2$, $q \neq 9$. For completeness, we give our own proof.

Theorem 5.14 [21] *Let $q \equiv 1 \pmod 4$, $q = p^r$, and $r \geq 2$. Using hyperbolic coordinates, we define the map*

$$\psi : \mathbb{F}_q^2 \longrightarrow \mathbb{F}_q^2, \ (\alpha, \beta) \longmapsto (\alpha, \beta^p).$$

Then ψ is an integral automorphism of $\mathbb{F}_q^2$, but not an affine automorphism.

Proof. The proof is done using hyperbolic coordinates.

We have

$$\begin{aligned} N(\psi(\alpha, \beta)) &= N(\alpha, \beta^p) \\ &= \alpha\beta^p \\ &= \beta^{p-1}\alpha\beta \\ &= \beta^{p-1}N(\alpha, \beta). \end{aligned}$$

Because for p odd, $\beta^{p-1} \in \square_q$, and thus $N(\psi(\alpha, \beta)) \in \square_q$ if and only if $N(\alpha, \beta) \in \square_q$. We check if ψ is a bijection.

If (α, β) ,$(\alpha', \beta') \in \mathbb{F}_q^2$; then $\psi(\alpha, \beta) = \psi(\alpha', \beta')$; i.e., $(\alpha, \beta^p) = (\alpha', \beta'^p)$.

This implies that $\alpha = \alpha'$ and $\beta^p = \beta'^p$, which implies that $\beta = \beta'$; i.e., $(\alpha, \beta) = (\alpha', \beta')$. So ψ is injective and thus a bijection by Pigeonhole's principle. Hence $\psi \in \ \mathrm{Aut}(\mathbb{F}_q^2)$.

Let $P = \gamma(1, 1)$ with $\gamma \in \mathbb{F}_q$ an arbitrary point on the line $L = \mathbb{F}_q(1, 1)$. Then $\psi(P) = (\gamma, \gamma^p)$, which is on L if and only if $\gamma \in \mathbb{F}_p$. So $\psi(L)$ is not a line and therefore $\psi \notin \mathrm{AffAut}(\mathbb{F}_q)$. □

We remark that ψ is a $\mathbb{F}_p$-linear map of order r. The following theorem from [21] holds.

Theorem 5.15 [21] *Let $q \equiv 1 \pmod 4$, $r \geq 2$, and $q \neq 9$. Then*
$\mathrm{Aut}(\mathbb{F}_q^2) = \langle \mathrm{AffAut}(\mathbb{F}_q^2), \psi \rangle$ *and* $|\mathrm{Aut}(\mathbb{F}_q^2)| = [q(q-1)r]^2$.

The above result, combined with Theorem 5.5, will lead to the following one.

Theorem 5.16 [26] *Let $q = p^r$, where p is a prime and $q \equiv 1 \pmod 4$, $q \notin \{5, 9\}$. Then* $|\mathrm{Aut}(\mathbb{F}_q^2)| = (q(q-1)r)^2$.

In the proof of Theorem 5.16, the notations $\mathbf{0} = (0, 0)$ and $\mathbf{1} = (1, 1)$ have been used for the vectors in $\mathbb{F}_q^2$. Recall that, $\mathrm{Aut}(\mathbb{F}_q^2) = \mathrm{Aut}(\mathrm{Cay}(\mathbb{F}_q^2, \mathbb{S}))$, where $\mathbb{S}$ is the connecting set of the integral distance graph defined in Chapter 3.

For $q \equiv 1 \pmod 4$, we have a linear mapping $\phi : (x_1, x_2) \longmapsto (x_1 + \omega x_2, x_1 - \omega x_2)$, with $\omega \in \mathbb{F}_q$ and $\omega^2 = -1$. This maps the graph $\mathrm{Cay}(\mathbb{F}_q^2, \mathbb{S})$ to $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$, where $S = \{\mathbf{x} \in \mathbb{F}_q^2 : \mathbf{x} = (x_1, x_2) \neq \mathbf{0}$ and $x_1 x_2 \in \square_q\}$ (See Chapter 3).

We set $G := \mathrm{Aut}\ \Gamma$. Since $\mathrm{Cay}(\mathbb{F}_q^2, \mathbb{S})$ is isomorphic to Γ, Theorem 5.16 is equivalent to Theorem 5.20 (p. 111).

From the proof of Lemma 5.6, it can be deduced that $G = \mathrm{Aut}\ \Gamma$ contains the group F generated by $\lambda_{(a,b)}$, R, $M_a^{\pm}$, and A_i, $i = 1, 2$.

Recall that $S = \mathbb{S}^\phi$ so that $G = \mathrm{Aut}(\mathrm{Cay}(\mathbb{F}_q^2, \mathbb{S}^\phi)) = \phi^{-1}\mathrm{Aut}(\mathbb{F}_q^2)\phi$. Since $F \leqslant G$, we see that $A := \phi F \phi^{-1} \leqslant \mathrm{Aut}(\mathbb{F}_q^2)$ and $|A| = (q(q-1)r)^2$ by Lemma 5.7. Now we show that A is isomorphic to the group described in Theorem 5.15 in order to determine the order of $\mathrm{Aut}(\mathbb{F}_q^2)$ for $q \equiv 1 \pmod 4$, $q \notin \{5, 9\}$.

Proposition 5.17 *Let $H := \mathrm{AffAut}(\mathbb{F}_q^2)$, $q \equiv 1 \pmod 4$, $q \notin \{5, 9\}$, and ψ an integral automorphism defined in* Theorem 5.14.

Then, $\langle H^\phi, \psi \rangle = F$, where ϕ is the $\mathbb{F}_q$-linear mapping $\phi : (x_1, x_2) \longmapsto (x_1 + \omega x_2, x_1 - \omega x_2)$ with $\omega \in \mathbb{F}_q^*$ and $\omega^2 = -1$ (H^ϕ is the conjugate of H by ϕ).

Proof. For the proof, it is sufficient to find the conjugates of the elements of $\mathrm{AffAut}(\mathbb{F}_q^2)$ from Theorem 5.1 by the $\mathbb{F}_q$-linear mapping ϕ.

Let $\lambda_{\mathbf{u}}$, R, M, and σ be the affine integral automorphisms defined in Theorem 5.1; and $\psi : (x_1, x_2) \longmapsto (x_1, x_2^p)$ with p the characteristic of $\mathbb{F}_q$. Since

$(x_1, x_2)^\phi = (x_1 + \omega x_2, x_1 - \omega x_2) = (x_1, x_2) \begin{pmatrix} 1 & 1 \\ \omega & -\omega \end{pmatrix}$, then

$(x_1, x_2)^{\phi^{-1}} = \left(\frac{1}{2}(x_1 + x_2), -\frac{\omega}{2}(x_1 - x_2)\right) = \frac{1}{2}(x_1, x_2) \begin{pmatrix} 1 & -\omega \\ 1 & \omega \end{pmatrix}$,

$\omega \in \mathbb{F}_q$ and $\omega^2 = -1$.

Hence we have

(1) $(x_1, x_2)^{\phi^{-1}\lambda_{(a,b)}\phi} = (x_1 + a + b\omega, x_2 + a - b\omega)$;

(2) $(x_1, x_2)^{\phi^{-1}R\phi} = (\omega x_1, -\omega x_2) = (\omega x_1, \omega^{-1} x_2)$;

$$\begin{aligned}(3)\ (x_1, x_2)^{\phi^{-1}M\phi} &= \frac{1}{2}(x_1, x_2) \begin{pmatrix} 1 & -\omega \\ 1 & \omega \end{pmatrix} \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \omega & -\omega \end{pmatrix} \\ &= \begin{pmatrix} a + b\omega & 0 \\ 0 & a - b\omega \end{pmatrix};\ a, b, \omega \in \mathbb{F}_q,\ a^2 + b^2 \in \square_q^* \text{ and } \omega^2 = -1;\end{aligned}$$

(4) $(x_1, x_2)^{\phi^{-1}\sigma\phi} = \left(\frac{1-(-1)^{\frac{p+1}{2}}}{2^p} x_1^p + \frac{1+(-1)^{\frac{p+1}{2}}}{2^p} x_2^p, \frac{1+(-1)^{\frac{p+1}{2}}}{2^p} x_1^p + \frac{1-(-1)^{\frac{p+1}{2}}}{2^p} x_2^p\right)$;

i.e.,

$$(x_1, x_2)^{\phi^{-1}\sigma\phi} = \begin{cases} (2^{1-p} x_1^p, 2^{1-p} x_2^p) & \text{if } p \equiv 1 \pmod 4; \\ (2^{1-p} x_2^p, 2^{1-p} x_1^p) & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

For (3), put $a^2 + b^2 := c^2$, $c \in \mathbb{F}_q^*$, and $d := \dfrac{a + b\omega}{c}$. Clearly, $d^{-1} = \dfrac{a - b\omega}{c}$. Then

$(x_1, x_2)^{\phi^{-1}M\phi} = ((a + b\omega)x_1, (a - b\omega)x_2) = (cdx_1, cd^{-1}x_2)$.

It follows immediately that $\phi^{-1}\lambda_{\mathbf{u}}\phi = \lambda_{\mathbf{u}^\phi} \in \Lambda$, $\phi^{-1}R\phi = RM_\omega^-$, $\phi^{-1}M\phi = M_d^- M_c^+$, and

$$\phi^{-1}\sigma\phi = \begin{cases} A_1 A_2 M_{2^{1-p}}^+ & \text{if } p \equiv 1 \pmod 4; \\ A_1 A_2 R M_{2^{1-p}}^+ & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Since ψ corresponds to A_2 in F, the result follows immediately. □

The crucial steps towards the O'Nan Scott Theorem is to show that, if $q \notin \{5, 9\}$, then the primitive group G is an affine group (i.e., of affine type according to Theorem 2.29), which has rank 4. The first part of the statement is given in the following lemma.

Lemma 5.18 [26] *With notations as above, if $q \neq 5$, then G is an affine group. Moreover Λ is normal in G.*

Proof. Since $F \leqslant G$ and F is primitive, so is G. Let H be the socle of G. By Theorem 2.29, $H \cong T \times \cdots \times T = T^m$ for some simple group T and $m \geq 1$, and G is one of the five types; namely, Affine type(A), Regular non-abelian(RN), Almost simple(AS), Diagonal(D), and Product type(P).

Assume that G is not of type A, H is either non-regular or non-abelian. It follows that T is a non-abelian simple group.

We first consider the product type P. Then G is the subgroup of the wreath product $U \wr S_{[s]}$ with $s > 1$, where U is a primitive group of type AS or D. By [11, Exercise 4.8.1], it can be shown that the rank of G is at least 3. So $G_{\mathbf{0}}$ has either the same orbits as $F_{\mathbf{0}}$, or the sets S_1 and S_2 are fused into one $G_{\mathbf{0}}$ orbit. Thus G has rank 3 or 4 since F has rank 4 and $F \leqslant G$. (See Lemma 5.6). The respective subdegrees are:

$$\frac{(q-1)^2}{2}, \frac{(q-1)(q+3)}{2}; \quad 2(q-1), \frac{(q-1)^2}{2}, \frac{(q-1)^2}{2} \tag{5.2}$$

In this case, it has been shown by [26, Lemma 8] that only the case $q = 5$ holds if G is of rank 3, with U of type AS and T 2-transitive. Hence, assume that $q \neq 5$.

In our case, since F acts on the group $\mathbb{F}_q^2$, $q = p^r$, p prime, and $p > 2$, it follows that G is primitive of odd degree.

By [11, Exercise 4.6.2], it can be shown that if G is a finite primitive permutation group of odd degree, then H is either simple or regular. This excludes immediately the types P and D.

Now we consider only the types RN and AS. Since T is non-abelian simple, this also excludes the type RN, since for otherwise, $|H| = |\mathbb{F}_q^2| = p^{2r}$.

Suppose that G is of type AS. Then $H = T$ is a non-abelian simple group acting transitively on $\mathbb{F}_q^2$ since it is a normal subgroup of a primitive group. It follows from Theorem 2.31 that H and hence G is 2-transitive, a contradiction. Hence we have shown that G is an affine group.

It remains to prove that Λ is normal in G. In fact, it is sufficient to show that $H = \Lambda$.

Indeed, by Lemma 5.7(i), Λ is normal in F. Since Λ is elementary abelian, Λ is also the socle of F by Theorem 2.27. Thus Λ is the unique minimal normal subgroup of F; i.e., for every non-trivial normal subgroup $N \lhd F$, $\Lambda \leqslant N$. In particular, if the normal subgroup $N = H \cap F$ is non-trivial, then $\Lambda \leqslant N$. Since $|H| = |\Lambda|$, this then implies that $H = \Lambda$. Therefore, it is sufficient to show that $H \cap F$ is non-trivial.

Assume, towards a contradiction, that $H \cap F$ is trivial. Note that, then $H \cap \Lambda$ is also trivial, hence $H\Lambda > H$. Consider the group HF. Then $H\Lambda/H$ is a subgroup of

HF/H. Since $H \cap F$ is trivial, the mapping $Hf \longmapsto f$, $f \in F$ defines an isomorphism from HF/H to F by The Second Isomorphism Theorem. This isomorphism maps $H\Lambda/H$ to Λ; and since $\Lambda \lhd F$, it follows in turn that, $H\Lambda/H \lhd HF/H$, and so $H\Lambda \lhd HF$. The group HF is primitive and H is a minimal normal subgroup in it. Since H is elementary abelian, H is also the socle of HF by Theorem 2.27, and thus H is the unique minimal normal subgroup of HF.

Consider the center $Z = Z(H\Lambda)$. Then Z is non-trivial since $H\Lambda$ is a p-group by [38, 1.6.14]. In addition, Z is characteristic in $H\Lambda$. Using this and that $H\Lambda \lhd HF$, it follows that $Z \lhd HF$ by [38, 1.5.6(iii)], and hence $H \leqslant Z = Z(H\Lambda)$. This means that $H\Lambda \leqslant C_{S_{\mathbb{F}_q^2}}(H)$, the centralizer of H in the full symmetric group $S_{\mathbb{F}_q^2}$. Since H acts regularly on $\mathbb{F}_q^2$, $C_{S_{\mathbb{F}_q^2}}(H) \cong H$ by [11, Exercise 2.5.6], and so $|H\Lambda| \leq |H|$. This, however, contradicts that $H\Lambda > H$. This completes the proof of the lemma. □

The other part of the statement is now given in the following lemma.

Lemma 5.19 [26] *With notations as above, if $q \notin \{5, 9\}$, then G has rank* 4.

Proof. By Lemma 5.18, G is an affine group. If $q = p$, then $G = F$ by Theorem 5.5, and so G has rank 4 (see Lemma 5.7(iii)). For $13 \leq q \leq 49$ the only non-prime orders are 25 and 49, which have been checked using Magma [6]. Combining all these with Equation (5.2) it is sufficient to prove the following statement:

Claim 1 *Let H be an affine permutation group of degree p^{2r}, where $p > 2$, $r \geq 2$ and $p^r \equiv 1 \pmod 4$, and suppose that H has rank 3 with non-trivial subdegrees:*

$$\frac{(p^r - 1)^2}{2} \text{ and } \frac{(p^r - 1)(p^r + 3)}{2}. \tag{5.3}$$

Then $p^r \leq 49$.

We derive the claim using Theorem 2.32, in fact, we are going to consider step-by-step all classes (A)-(C):

Suppose that H is in class (A). If H is in class (A1), then $H_{\mathbf{0}}$ is isomorphic to a subgroup of a one-dimensional semi-linear group $\Gamma\mathrm{L}_1(\mathbb{F}_{p^{2r}})$, whose order is $2(p^{2r}-1)r$. By [26], if the subdegrees in Equation (5.3) divide $|H_{\mathbf{0}}|$, it follows somewhere that $p^r + 3$ divide $8r$, so that $p^r \leq 8r - 3$. This is only possible if $p^r = 9$ since $p > 2$ and $r \geq 2$. However, $p^r + 3$ cannot divide $8r$ in this case.

Let H be in class (Ai) for $i > 1$. By comparing the subdegrees in Equation (5.3) to the corresponding subdegrees in Table 2 from Appendix B, it is easily shown that they are only in rows 1 and 2 of Table 2 if and only if $q \in \{5, 9\}$, but nowhere in rows 3 and 4 of Table 2 for any value of q (See [26]).

In the remaining classes (B) and (C), if H is supposed to be in one of them, we consider the number p^{2r} such that $p^r \equiv 1 \pmod 4$, $p > 2$, $r \geq 2$ and $p^r > 49$.

If H is in class (B), the only number in Equation (2.2) is 3^8 with corresponding subdegrees 1440 and 5120, see [34, Table 13].

If H is in class (C), the only numbers in Equation (2.3) are 5^6 and 3^{12}. The former corresponds to subdegrees 7560 and 8064, whereas the latter corresponds to subdegrees 65520 and 465920, see [34, Table 14].

Using each of the obtained numbers from both classes in expressions from Equation (5.3), we obtain a contradiction and the claim is proved. □

We now consider the main result of this section.

Theorem 5.20 [26] *With notations as above, if* $q \notin \{5, 9\}$, *then* $|G| = (q(q-1)r)^2$.

Proof. By Lemma 5.19, the set S_1 is an orbit of $G_{\mathbf{0}}$. Consider the action of $G_{\mathbf{0}}$ on S_1. It will be convenient to view $\mathbb{F}_q^2$ as a vector space over $\mathbb{F}_p$ of dimension $2r$. Denote this vector space by V, and set $V_1 = (\mathbb{F}_q, 0)$ and $V_2 = (0, \mathbb{F}_q)$. Clearly, $V = V_1 \oplus V_2$. Recall that Λ consists of the translations $\lambda_{(a,b)}$ by the vectors $(a, b) \in \mathbb{F}_q^2$; and thus, viewed as a permutation group of V, Λ consists of the translations by the vectors of V.

By Lemma 5.18, $G_{\mathbf{0}}$ normalizes Λ, hence it follows that each element $g \in G_{\mathbf{0}}$ acts as an $\mathbb{F}_p$-linear transformation of V. Notice that, $S_1 = V_1 \cup V_2 \setminus \{\mathbf{0}\}$. Now, if for $v, w \in V_1 \setminus \{\mathbf{0}\}$, $v^g \in V_1$ and $w^g \in V_2$, then $(v + w)^g = v^g + w^g \notin S_1$ a contradiction. Hence it follows that $G_{\mathbf{0}}$ preserves the partition of S_1 in to the sets $V_1 \setminus \{\mathbf{0}\}$ and $V_2 \setminus \{\mathbf{0}\}$.

Let $\overline{G_{\mathbf{0}}}$ be the subgroup of $G_{\mathbf{0}}$ that leaves the set $(\mathbb{F}_q^*, 0)$ (and hence also the set $(0, \mathbb{F}_q^*)$) fixed. It is clear that $|G_{\mathbf{0}} : \overline{G_{\mathbf{0}}}| = 2$. Furthermore, let $\overline{G} = \langle \Lambda, \overline{G_{\mathbf{0}}} \rangle$. As Λ is normal in G and Λ is transitive, $|G : \overline{G}| = 2$ and $\overline{G}_{\mathbf{0}} = \overline{G_{\mathbf{0}}}$. The orbit of $\mathbf{1}$ under $\overline{G_{\mathbf{0}}}$ is equal to the set S_2 (this can be seen by using the transformations M_a^+ and M_a^-, $a \in \mathbb{F}_q^*$). By the orbit-stabilizer property, it follows that

$$|G| = 2|\overline{G}| = 2q^2|\overline{G}_{\mathbf{0}}| = 2q^2|S_2||\overline{G}_{\mathbf{0},\mathbf{1}}| = (q(q-1))^2|\overline{G}_{\mathbf{0},\mathbf{1}}|. \qquad (5.4)$$

Let Λ_1 be the subgroup of Λ generated by all translations $\lambda_{(a,0)}$, $a \in \mathbb{F}_q$, and let $H = \langle \Lambda_1, \overline{G_{\mathbf{0}}} \rangle$. For $\lambda_{(a,0)} \in \Lambda_1$ and $g \in \overline{G_{\mathbf{0}}}$ with straightforward calculations, $g^{-1}\lambda_{(a,0)}g =$

$\lambda_{(a',0)}$, where $(a',0) = (a,0)^g$. Thus $H = \overline{G}_{\mathbf{0}}\Lambda_1$. Since $\overline{G}_{\mathbf{0}} \leqslant H$, the orbit of $\mathbf{0}$ under H is a block for $\overline{G}$ by Theorem 2.26. This orbit is found as

$$\mathbf{0}^H = \mathbf{0}^{\overline{G}_{\mathbf{0}}\Lambda_1} = \mathbf{0}^{\Lambda_1} = (\mathbb{F}_q, 0),$$

and hence $(\mathbb{F}_q, 0)$ is a block for $\overline{G}$. Repeating the same argument with the group Λ_2 generated by all translations $\lambda_{(0,a)}$, $a \in \mathbb{F}_q$, another block $(0, \mathbb{F}_q)$ is obtained for $\overline{G}$. Therefore, for every $g \in \overline{G}$ there exist permutations g_1 and g_2 of $\mathbb{F}_q$ such that

$$(x_1, x_2)^g = (x_1^{g_1}, x_2^{g_2}) \text{ for every } (x_1, x_2) \in \mathbb{F}_q^2. \tag{5.5}$$

Assume in addition, that $g \in \overline{G}_{\mathbf{0},\mathbf{1}}$. It is shown that in this case g_1 and g_2 are automorphisms of the Paley graph $P(q)$. Here only g_1 is considered (the permutation g_2 can be handled similarly). Choose $x, y \in \mathbb{F}_q$ such that $x \neq y$ and $x - y \in \Box_q$. Now, $\{(x,1),(y,0)\}$ is an edge of the graph $\mathrm{Cay}(\mathbb{F}_q^2, S)$, $S = S_1 \cup S_2 = \mathbb{S}^{\phi}$. Hence $\{(x,1)^g, (y,0)^g\}$ is also an edge of $\mathrm{Cay}(\mathbb{F}_q^2, S)$; i.e., by Equation (5.5),

$$(x^{g_1} - y^{g_1})(1^{g_2} - 0^{g_2}) \in \Box_q.$$

As $g \in \overline{G}_{\mathbf{0},\mathbf{1}}$, $1^{g_2} = 1$, $0^{g_2} = 0$, and therefore, $x^{g_1} - y^{g_1} \in \Box_q$. This shows that $g_1 \in \mathrm{Aut}\ P(q)$. Now since both g_1 and g_2 fix the elements 0 and 1 in $\mathbb{F}_q$, it follows by Equation (5.1) that $g_1 : x \mapsto x^{p^i}$ for some $i \in \{1, \cdots, r\}$ and $g_2 : x \mapsto x^{p^j}$ for some $j \in \{1, \cdots, r\}$, which gives that $g = A_1^i A_2^j \in \overline{G}_{\mathbf{0},\mathbf{1}}$. Thus $|\overline{G}_{\mathbf{0},\mathbf{1}}| = r^2$, and so by Equation (5.4), $|G| = (q(q-1)r)^2$. □

From the above results, we determine the orders of Aut Γ_2 and Aut Γ_3 in the following.

Corollary 5.21 *Let* $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$ *and* $\Gamma_3 = \mathrm{Cay}(\mathbb{F}_q^2, S_3)$, $q \notin \{5, 9\}$, *with* $S_2 = \{(x_1, x_2) \in \mathbb{F}_q^2 : x_1 x_2 \Box_q^*\}$ *and* $S_3 = \mathbb{F}_q^2 \setminus (S \cup \{\mathbf{0}\})$, $S = S_1 \cup S_2$. *Then*

$$|\mathrm{Aut}\ \Gamma_2| = |\mathrm{Aut}\ \Gamma_3| = (q(q-1)r)^2.$$

Proof. This follows immediately from Theorem 5.20 and Corollary 5.12(ii) □

Chapter 6

Conclusion

In this thesis, we presented the graph $\mathfrak{G}_{m,q}$ as an integral distance graph over $\mathbb{F}_q^m$, $m \geq 2$, with $\mathbb{F}_q$ a finite field and q an odd prime power. In Chapter 3, we considered a subset $S^{(m)}$ of elements of $\mathbb{F}_q^m$, whose squared Euclidean distance with a zero vector is a perfect square in $\mathbb{F}_q$. We have shown that $S^{(m)}$ is a Cayley set so that we defined the Cayley graph $\mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})$. By the isomorphism of $\mathrm{Cay}(\mathbb{F}_q^m, S^{(m)})$ to $\mathfrak{G}_{m,q}$, we deduced that $\mathfrak{G}_{m,q}$ is a Cayley graph.

In particular for the two-dimensional case, much of the work was turned essentially to the sub-case of $q \equiv 1 \pmod 4$. There, it has been shown that there exists an element $\omega \in \mathbb{F}_q$ such that $\omega^2 = -1$. Consequently, this led to the existence of the vanishing directions $\mathbb{F}_q(\omega + i)$ and $\mathbb{F}_q(\omega - i)$ and a linear mapping ϕ defined in Chapter 3, which is a switch to *hyperbolic coordinates*. There, we defined the two base subsets S_1 and S_2 of $\mathbb{F}_q^2$. The one, namely S_1, consists of non-zero elements from the two vanishing directions; and the other, namely S_2, consists of elements of $\mathbb{F}_q^2$ with non-zero squared norm, both in hyperbolic coordinates. These sets were shown to be Cayley sets so that the corresponding constituent graphs $\Gamma_i = \mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2$, of the integral distance graph $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$, with $S = S_1 \cup S_2$, are Cayley graphs. They also formed a Boolean algebra of Cayley sets so that the latter graph Γ and its complement $\Gamma_3 = \mathrm{Cay}(\mathbb{F}_q^2, S_3)$, with $S_3 = \mathbb{F}_q^2 \setminus (S \cup \{\mathbf{0}\})$, are Cayley graphs. Since $\mathfrak{G}_{m,q}$ is a Cayley graph as we mentioned above, we deduced that this holds immediately for $\mathfrak{G}_{2,q}$ with $q \equiv 3 \pmod 4$. Finally, with results from Lemma 3.9, the latter property also holds for $\mathfrak{G}_{2,q}$ with $q \equiv 1 \pmod 4$, and hence $\mathfrak{G}_{2,q}$ is a Cayley graph for any odd prime power q.

For strong regularity, first we considered the two-dimensional case. For $q \equiv 1$

(mod 4), the two constituent graphs $\Gamma_i = \mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2$, were shown to be strongly regular. The calculation of parameters for Γ_1 was much easier than that for Γ_2. In the latter graph, this was done in several lemmas in order to compute each parameter separately. There, we deduced the strong regularity of $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$ in similar ways as for Γ_2, and thus the strong regularity of another constituent graph Γ_3 since it is the complement of Γ by Theorem 2.3. Therefore, all the above results combined with Theorem 2.3 reduced to a Boolean algebra of Cayley sets for strong regularity of the Cayley graphs $\mathrm{Cay}(\mathbb{F}_q^2, S_i)$, $i = 1, 2$.

For the remaining case $q \equiv 3 \pmod 4$, we have seen by Corollary 4.10 that there is no constituent graph of the integral distance graph, since the latter is isomorphic to its complement. So we had only to study strong regularity in similar ways as for Γ. Therefore, from all the above cases, we deduced that $\mathfrak{G}_{2,q}$ is strongly regular for all $q = p^r$, p prime and $p > 2$.

In higher dimension with similar calculations as for $\mathfrak{G}_{2,q}$, $q \equiv 3 \pmod 4$, together with the three functions $\mathcal{S}(m, q)$, $\mathcal{Z}(m, q)$, and $\mathcal{N}(m, q)$ established in Chapter 2, Lemma 4.18, and Theorem 4.19; we have seen that the integral distance graph $\mathfrak{G}_{m,q}$, $m \geq 2$, is strongly regular if and only if m is even. For the last parameter, we have used the relation between all parameters established in Proposition 2.2.

Concerning the symmetries of the integral distance graph $\mathfrak{G}_{m,q}$, $m \geq 2$, our attention restricted to the two-dimensional case since the higher dimensional case was established in [32]. For the former case, if $q \equiv 3 \pmod 4$, it has been shown in [21, 26] that the automorphisms of $\mathfrak{G}_{2,q}$ are exactly the affine automorphisms. In addition, by the isomorphism of $\mathfrak{G}_{2,q}$ to the Paley graph $P(q^2)$, the order of its automorphism group was established by Proposition 5.4.

Our point of interest was the case of $q \equiv 1 \pmod 4$, where we considered the automorphisms of each of the constituent graphs Γ_i, $i = 1, 2, 3$. We showed that the automorphism group of Γ_1 is represented as the product of the translation group by the wreath product of the symmetric group $S_{\mathbb{F}_q^*}$ by $S_{[2]}$. By Corollaries 4.10 and 5.13, and the fact that Γ_3 is the complement of $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$, we have also shown the isomorphism between the automorphism group of the remaining constituent graph $\Gamma_2 = \mathrm{Cay}(\mathbb{F}_q^2, S_2)$ and the automorphism group of the original graph $\Gamma = \mathrm{Cay}(\mathbb{F}_q^2, S)$ which is in turn isomorphic to the integral distance graph $\mathfrak{G}_{2,q}$, $q \equiv 1 \pmod 4$, established in [21, 26].

As an outlook, further research may be conducted to finite rings $\mathbb{Z}_n$, as well as Banach spaces, to see if the properties of the integral distance graphs established in Chapters 3, 4, and 5 hold.

Bibliography

[1] Allie, I. (2017). Meta-Cayley Graphs on Dihedral Groups. MSc Thesis. University of the Western Cape, Bellville, South Africa.

[2] Balakrishnan, R., Ranganathan, K. (2012). *A Textbook of Graph Theory.* New York: Springer-Verlag.

[3] Ball, R. W. (1966). Maximal Subgroups of Symmetric Groups. *Proc. Amer. Math. Soc.* **121**: 393-407.

[4] Beineke, L. W., Wilson, R. J., Cameron, P. J. (2005). *Topics in Algebraic Graph Theory.* New York: Cambridge University Press.

[5] Bondy, J. A., Murty, U. S. R. (2008). *Graph Theory.* New York: Springer-Verlag.

[6] Bosma, W., Cannon, J., Playoust, C. (1997). The Magma Algebra System I: The User Language. *J. Symbolic. Comput.* 24(**3-4**): 235-265.

[7] Brass, P., Moser, M., Pach, J. (2005). *Research Problems in Discrete Geometry.* New York: Springer-Verlag.

[8] Carlitz, L. (1960). A Theorem on Permutations in a Finite Field. *Proc. Amer. Math. Soc.* **11**: 456-459.

[9] Dickson, L. E. (1958). *Linear Groups.* New York: Dover.

[10] Dimiev, S. (2005). A Setting for a Diophantine Distance Geometry. *Tensor (N.S.)* 66(**3**): 275-283; MR MR2189847.

[11] Dixon, J. D., Mortimer, B. (1996). *Permutation Groups.* New York: Springer-Verlag.

[12] Elsawy, A. N. (2009). Paley Graphs and Their Generalisation. Master's Thesis. Heinrich Heine University, Dússeldorf, Germany.

[13] Fawcett, J. B. (2013). Bases of Primitive Permutation Groups. PhD Thesis. University of Cambridge, Cambridge, England, UK.

[14] Foulser, D. A., Kallaher, M. J. (1978) .Solvable, Flag-transitive Rank 3 Collineation Groups. *Geom. Dedicata*. **7**: 111-130.

[15] Fullerton, R. E. (1949). Integral Distances in Banach Spaces. *Bull. Amer. Math. Soc. (N.S.)*. **55**: 901-905.

[16] Godsil, C., Royle, G. (2001). *Algebraic Graph Theory*. New York: Springer-Verlag.

[17] Guralnick, R. M. (1983). Subgroups of Prime Power Index in a Simple Group. *J. Algebra*. **81**: 304-311.

[18] Guy, R. K. (1994). *Unsolved Problems in Number Theory*. New York: Springer-Verlag.

[19] Harborth, H. (1998). Integral distances in point sets, *Karl Der Grosse und Sein Nachwirken, 1200 Jahre Kultur und Wissenschaft in Europa, in: Mathematisches Wissen*. **2**: 213-224.

[20] Iosevich, A., Rudnev, M. (2003). A Combinatorial Approach to Orthogonal Exponentials. *Intern. Math. Research Notices*. **49**: 1-12.

[21] Kiermaier, M., Kurz, S. (2009). Maximal Integral Point Sets in Affine Planes over Finite Fields. *Discrete Math*. **309**: 4564-4575.

[22] Kleber, M. (2008). Encounter at Far Point. *Math. Interigencer*. 30(**1**): 50-53.

[23] Klee, V., Wagon, S. (1991). *Old and New Unsolved Problems in Plane Geometry and Number Theory*. Washington, DC: Mathematical Association of America.xv.

[24] Kohnert, A., Kurz, S. (2006). Integral Point Sets over $\mathbb{Z}_n^m$. *Electron, Notes Discrete Math*. **27**: 65-66.

[25] Kohnert, A. and Kurz, S. (2006). Integral Point Sets over $\mathbb{Z}_n^m$. *Discrete Appl. Math*. **157**: 2105-2117.

[26] Kovács, I., Ruff, J. (2014). Integral Automorphisms of Affine Planes over Finite Fields. *Finite Fields and Their Applications.* **27**: 104-114.

[27] Kovács, I., Kutnar, K., Ruff, J., Szőnyi, T. (2017). Integral Automorphisms of Affine Spaces over Finite Fields. *Des. Codes Cryptogr.* **84**: 181-188.

[28] Kreisel, T., Kurz, S. (2008). There are Integral Heptagons, no three points on a line, no four on a circle. *Discrete Comput. Geom.* **39**: 786-790.

[29] Kurz, S. (2009). Integral Point Sets over Finite Fields. *Australas J. Combin.* **43**: 3-29.

[30] Kurz, S. (2006). Konstruktion und Eigenschaften Ganzzahliger Punktmengen. PhD Thesis. Universität Bayreuth, Bayreuth, Bavaria, Germany.

[31] Kurz, S., Lane, R. (2007). Upper Bounds for Integral Point Sets. *Australas J. Comb.* **39**: 233-240.

[32] Kurz, S., Meyer, H. (2009). Integral Point Sets in Higher Dimensional Affine Spaces over Finite Fields. *J. Comb. Theory, Ser. A.* **116**: 1120-1139.

[33] Lidl, R., Niederreiter, H. (1996). *Finite Fields*. Cambridge: Cambridge Univ. Press.

[34] Liebeck, M. W. (1987). The Affine Permutation Groups of Rank Three. *Proc. Lond. Math. Soc.*(3). **54**: 477-516.

[35] McKay, B. D. (1981). Practical Graph Isomorphism. *Congressus Numerantium.* **30**: 45-87.

[36] Mwambene, E. (2001). Representing Graphs on Groupoids: Symmetry and Form. PhD Thesis. University of Vienna, Vienna, Austria.

[37] Newton, B., Benesh, B. (2006). A classification of Certain Maximal Subgroups of Symmetric Groups. *Journal of Algebra*. 304(**2**): 1108-1113.

[38] Robinson, D. J. S. (1996). *A Course in the Theory of Groups*. New York: Springer-Verlag.

[39] Schmidt, W. M. (2004). *Equations over Finite Fields an Elementary Approach.* Heber City: Kendrick Press.

[40] Suzuki, M. (1981). *Group Theory I.* New York: Springer-Verlag.

Appendices

A Infinite classes (A) of permutation groups labelled by (A1)-(A11)

Types of G	$n = p^d$	**Subdegrees**
(A1): $G_{\mathbf{0}} < \Gamma\mathrm{L}_1(\mathbb{F}_{p^d})$	p^d	given in [14]
(A2): $G_{\mathbf{0}}$ imprimitive	p^{2m}	$2(p^m - 1)$, $(p^m - 1)^2$
(A3): Tensor product	q^{2m}	$(q+1)(q^m - 1)$, $q(q^m - 1)(q^{m-1} - 1)$
(A4): $G_{\mathbf{0}} \rhd \mathrm{SL}_a(\mathbb{F}_q)$	q^{2a}	$(q+1)(q^a - 1)$, $q(q^a - 1)(q^{a-1} - 1)$
(A5): $G_{\mathbf{0}} \rhd \mathrm{SL}_2(\mathbb{F}_q)$	q^6	$(q+1)(q^3 - 1)$, $q(q^3 - 1)(q^2 - 1)$
(A6): $G_{\mathbf{0}} \rhd \mathrm{SU}_a(\mathbb{F}_q)$	q^{2a}	$(q^a - 1)(q^{a-1} + 1), q^{a-1}(q-1)(q^a - 1),$ a even; $(q^a + 1)(q^{a-1} - 1), q^{a-1}(q-1)(q^a + 1),$ a odd.
(A7): $G_{\mathbf{0}} \rhd \Omega_{2a}^{\epsilon}(\mathbb{F}_q)$	q^{2a}	$(q^a - 1)(q^{a-1} + 1), q^{a-1}(q-1)(q^a - 1), \epsilon = +;$ $(q^a + 1)(q^{a-1} - 1), q^{a-1}(q-1)(q^a + 1), \epsilon = -.$
(A8): $G_{\mathbf{0}} \rhd \mathrm{SL}_5(\mathbb{F}_q)$	q^{10}	$(q^5 - 1)(q^2 + 1)$, $q^2(q^5 - 1)(q^3 - 1)$
(A9): $G_{\mathbf{0}} \rhd \mathrm{B}_3(\mathbb{F}_q)$	q^8	$(q^4 - 1)(q^3 + 1)$, $q^3(q^4 - 1)(q - 1)$
(A10): $G_{\mathbf{0}} \rhd \mathrm{D}_5(\mathbb{F}_q)$	q^{16}	$(q^8 - 1)(q^3 + 1)$, $q^3(q^8 - 1)(q^5 - 1)$
(A11): $G_{\mathbf{0}} \rhd \mathrm{Sz}(\mathbb{F}_q)$	q^4	$(q^2 + 1)(q - 1)$, $q(q^2 + 1)(q - 1)$

Table 1: The group G in class (A) of Theorem 2.32 (see [34, Table 12]).

B Non-trivial subdegrees of affine groups of rank 3 in classes (A2)-(A11)

Row	Subdegrees	Conditions
1.	$(p^s+1)(p^r-1), p^s(p^r-1)(p^{r-s}-1)$	$s=0$ or $s \mid r$ or $s=2r/5$ and $5 \mid r$ or $s=3r/4$ and $4 \mid r$ or $s=3r/8$ and $8 \mid r$
2.	$(p^{r-s}+1)(p^r-1), p^{r-s}(p^r-1)(p^s-1)$	$s \mid r$
3.	$(p^{r-s}-1)(p^r+1), p^{r-s}(p^r+1)(p^s-1)$	$s \mid r$ and $s \neq r$
4.	$(p^r+1)(p^{r/2}-1), p^{r/2}(p^r+1)(p^{r/2}-1)$	r is even

Table 2: Subdegrees of affine groups of rank 3 in classes (Ai), $i = 2, \cdots, 11$ (see [26, Table 1]).