ADDITIVE INTERPRETATION OF THE ERDOS-RENYI ORTHOGONAL POLARITY GRAPH

David Fernando Daza Urbano

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Doctorado en Ciencias Matemáticas
Popayán
September, 2022

ADDITIVE INTERPRETATION OF THE ERDOS-RENYI ORTHOGONAL POLARITY GRAPH

David Fernando Daza Urbano

A thesis submitted in partial satisfaction of the requirements for the degree:
Doctor en Ciencias Matemáticas

Advisor
Dr. Carlos Alberto Trujillo Solarte
Faculty at the Universidad del Cauca

Co-Advisor
Dr. Carlos Andrés Martos Ojeda
Faculty at the Universidad del Cauca

Universidad del Cauca
Facultad de Ciencias Naturales, Exactas y de la Educación
Departamento de Matemáticas
Doctorado en Ciencias Matemáticas
Popayán
September, 2022

ACCEPTANCE NOTE

ACCEPTED

Jury: Dra. Amanda Montejano Cantoral

Jury: Dr. Yamidt Bermúdez Tobón

Jury: Dr. Diego Fernando Ruiz Solarte

Popayán, February 8, 2023

I dedicate this thesis to
my father Luis, my mother Lucia, my
brother Juan, and my beloved animals
for their constant support and
unconditional love.

I love you all dearly.

Acknowledgements

I thank God, for letting me through all the difficulties. You are the one who let me finish my degree. I will keep on trusting you for my future. Thank you, Lord.

A special thanks to MINCIENCIAS (Colombia) for supporting my doctoral studies through the Bicentennial Doctoral Excellence Scholarships, BB 2019 01.

I would like to thank to my PhD advisor Professor Carlos Trujillo and my PhD Co-advisor Professor Carlos Martos, for encouraging my research and for allowing me to grow as a researcher. Their advice on both research as well as on my career have been invaluable.

I also have to thank the members of my PhD jury for their helpful career advice and suggestions in general.

I would like to thank the teachers in the department of mathematics at Universidad del Cauca for sharing their knowledge with me.

A special thanks to my family. Words can not express how grateful I am to my mother Lucia, and father Mg Luis for all of the sacrifices that you've made on my behalf. Your prayer for me was what sustained me thus far.

I would also like to thank my beloved brother, Esp. Juan. Thank you for supporting me in everything, and especially I thank you for encouraging me throughout this experience.

Finally, I would like to express my gratitude and thanks to all people who have always been there for me and who influenced my life in so many ways.

Resumen

Un subconjunto A de un grupo abeliano Γ (escrito aditivamente) es un conjunto B_2 en Γ si todas las sumas $a_1 + a_2$, con a_1 y a_2 en A, son diferentes. En esta tesis consideramos tres problemas de investigación que surgieron cuando estudiamos conjuntos B_2 de tipo Singer. En el primero, nos preguntamos sobre la existencia de conjuntos diferencia en grupos de orden p^m, cuando p es un número primo y $m > 1$ es un número entero. En relación a esto, demostramos la inexistencia de conjuntos diferencia abelianos con parámetros $(p^m, k, 1)$. En el segundo, nos interesamos en la construcción de nuevos casi conjuntos diferencia, con respecto a esto, utilizamos conjuntos B_2 de tipo Singer para construir tres nuevas familias de casi conjuntos diferencia. Además, construimos 2-adiseños a partir de estos casi conjuntos diferencia. En el tercero, nos propusimos usar el grafo suma de un conjunto B_2 de tipo Singer para establecer pruebas aditivas de algunas propiedades estructurales (conocidas y nuevas) del grafo polaridad ortogonal Erdös-Rényi ER_q. En particular, demostramos que el grafo suma de un conjunto B_2 de tipo Ruzsa es isomorfo a un subgrafo inducido de ER_q. Las principales herramientas utilizadas en esta investigación son propiedades aditivas de los conjuntos B_2, el Primer Teorema del Multiplicador, el cual garantiza la existencia de un multiplicador de un conjunto diferencia. También utilizamos un método de construcción de casi conjuntos diferencia de Ding. Además, empleamos un resultado de Luca y otros, el cual determina todas las soluciones de una ecuación diofántica.

Palabras clave: Conjunto B_2 de tipo Singer, conjunto diferencia, casi conjunto diferencia, 2-adiseño, grafo suma, grafo polaridad ortogonal Erdös-Rényi ER_q, conjunto B_2 de tipo Ruzsa, Primer Teorema del Multiplicador, multiplicador, ecuación diofántica.

Abstract

A subset A of an abelian group Γ (written additively) is a B_2 set in Γ if all the sums $a_1 + a_2$, with a_1 and a_2 in A, are different. In this thesis we consider three research problems that arose when we study Singer type B_2 sets. In the first we wonder about the existence of difference sets in groups of order p^m, when p is a prime number and $m > 1$ is an integer. In relation to this, we prove the non-existence of abelian difference sets with parameters $(p^m, k, 1)$. In the second we have an interest in the construction of new almost difference sets, regarding this, we use Singer type B_2 sets to construct three new families of almost difference sets. Additionally, we construct 2-adesigns from these almost difference sets. In the third we use the sum graph of a Singer type B_2 set to establish additive proofs of some structural properties (known and new) of the Erdös-Rényi orthogonal polarity graph ER_q. In particular, we prove that the sum graph of a Ruzsa type B_2 set is isomorphic to an induced subgraph of ER_q. The primary tools used in our investigation are additive properties of B_2 sets, the First Multiplier Theorem for Difference Sets. We also make use of Ding's method of constructing almost difference sets. Finally, we employ a result of Luca et al., which determines all the solutions of a given Diophantine equation.

Keywords: Singer type B_2 set, difference set, almost difference set, 2-adesign, sum graph, Erdös-Rényi orthogonal polarity graph ER_q, Ruzsa type B_2 set, First Multiplier Theorem, multiplier, Diophantine equation.

Research Products

Publications

[1] *Almost difference sets from Singer type Golomb rulers*, IEEE Access, **10** (2022), 1132-1137. With C. Martos and C. Trujillo.

[2] *Non-existence of* $(p^m, k, 1)$ *difference sets*, Electronics Letters, **58** (2022), no. 4, 154-155. With C. Martos and C. Trujillo.

[3] *Sidon sets and subgraphs of the Erdös-Rényi orthogonal polarity graph.* Contributions to Discrete Mathematics. Submitted for evaluation. With M. Huicochea, C. Martos and C. Trujillo.

Remark 1. Other papers in which I participated during my doctoral studies are:

[4] *Near-Optimal g-Golomb Rulers*, IEEE Access, **9** (2021), 65482-65489. With C. Martos and C. Trujillo.

[5] *Freiman-Type Theorem For Restricted Sumsets.* International Journal of Number Theory. Submitted for evaluation. With M. Huicochea, C. Martos and C. Trujillo.

[6] *Minimun overlap problem on finite groups.* Boletín de la Sociedad Matemática Mexicana. Submitted for evaluation. With M. Huicochea, C. Martos and C. Trujillo.

Doctoral internship

I made a research stay at the Universidad Autónoma de Zacatecas “Francisco García Salinas”, México, from september 12, 2021 to march 5, 2022, under the supervision of Dr. Mario Alejandro Huicochea Mason, researcher-professor of the Unidad Académica de Matemáticas of this University.

Talks

- *Sidon sets and C_4-saturated graphs.* Second Colombian Workshop on coding Theory (CWC 19), Universidad del Norte, Barranquilla Colombia, january 15–18, 2019.

- *Base Sidon para $\mathbb{F}_p \times \mathbb{F}_p$.* VI Seminario Regional de Teoría de Números, Popayán Colombia, march 11–14, 2020.

- *Grafo suma de conjuntos B_2 y subgrafos de ER_q.* DivulgaMat, Popayán Colombia, march 15–16, 2021.

- *Conjuntos Diferencia.* Seminario de Matemáticas Discretas, Zacatecas México, february 1, 2022.

- *Problemas de combinatoria y conjuntos de Sidon.* Seminario de Matemáticas Discretas, Zacatecas México, february 18, 2022.

- *Conjuntos de Sidon y grafos C_4-Saturados.* Seminario en Línea de Matemáticas Discretas, Zacatecas México, march 2, 2022.

- *Interpretación aditiva del grafo polaridad ortogonal Erdös-Rényi.* Jornadas de Álgebra y Teoría de Números, Popayán Colombia, june 2–3, 2022.

- *Almost Difference Sets From Singer Type Golomb Rulers.* MAPI2, Medellín Colombia, june 8–10, 2022.

Courses

- *Fragments of algebraic graph theory.* Barcelona Graduate School of Mathematics (BGSMath), online, Barcelona España, january 13 to march 25, 2021.

- *Métodos polinomiales.* Universidad Autónoma de Zacatecas (UAZ), Zacatecas México, online august 16 to septiembre 9, in-person septiembre 14 to November 26, 2021.

Workshop

- *Taller Extraordinario de Matemáticas Discretas.* Universidad Autónoma de México (UNAM), Campus Juriquilla, Querétaro México, december 13–17, 2021.

- *VII Encuentro Colombiano de Combinatoria.* Universidad de Los Andes and Universidad Sergio Arboleda, Bogotá Colombia, june 14–25, 2022.

Table of Contents

List of Figures

Chapter 1

Introduction

A subset A of an abelian group Γ (written additively) is a B_2 set or Sidon set in Γ if all the sums $a_1 + a_2$, with a_1 and a_2 in A, are different (except when they coincide because of commutativity, $a_1 + a_2 = a_2 + a_1$). According to Cilleruelo et al. [7], in 1932 the analyst Simon Sidon asked to a young Paul Erdös about the maximal cardinality of a B_2 set of integers in $\{1, \ldots, n\}$. Sidon was interested in this problem in connection with the study of the L_p norm of Fourier series with frequencies in these sets but Erdös was captivated by the combinatorial and arithmetical flavour of this problem and it was one of his favorite problems. Since that time, B_2 sets have received the attention of many researchers and they have been used in many fields, such as communications, fault-tolerant distributed computing, and coding theory, see [3] and references therein. Sidon sets also been used to study combinatorial problems such as product estimates, solvability of some equations [8, 9], or in the field of extremal graph theory to study the number $ex(n, C_4)$ [10, 11].

Since $a + b = c + d$ implies that $a - d = c - b$, A is a B_2 set if all non-zero differences of elements of A are different. If Γ is finite then by counting the number of differences $a - b$, we can see that $|A| < \sqrt{|\Gamma|} + 1/2$. The most interesting B_2 sets are those with large cardinality, that is, when $|A| = \sqrt{|\Gamma|} \pm \delta$ for a small number δ. A well-known construction of B_2 sets with large cardinality is due to Singer [12]. In this thesis, we focus on three problems that arose when we study Singer type B_2 sets.

The first problem is related to difference sets which are a well-known class of mathematical objects used in the construction of designs and other combinatorial structures. If Γ is of order v then a k-subset D of Γ is called a (v, k, λ) *difference set* DS (in Γ) if

$\delta_D(x) = \lambda$ for every nonzero element of Γ, where $\delta_D(x)$ is the *difference function* defined by

$$\delta_D(x) := |(D + x) \cap D|$$

and $D + x := \{d + x : d \in D\}$.

The order of the difference set D is defined as $n = k - \lambda$. Moreover, if Γ is abelian and $\lambda = 1$, then D is called an abelian planar difference set (APDS). Singer's construction [12] guarantees the existence of APDS's provided that n is a prime power. The Prime Power Conjecture states that there are no APDS's whose order is not a prime power.

The following question arises: which groups admit abelian planar difference sets? This question has been studied by several researchers, who have obtained important results on the existence and non-existence of difference sets in abelian and non-abelian groups. For example, in [13] proved that there is no abelian difference set with parameters (261, 105, 42), and in [14] proved that there is no abelian difference set with parameters (220, 73, 24) and (231, 70, 21). For other non-existence results, see [15, 16, 17].

In [2], which is reproduced in Chapter 2, we prove the following.

Theorem (Chapter 2, Theorem 3)**.** If p is a prime number and $m \geq 2$ is an integer then, there are no abelian planar difference sets with parameters $(p^m, k, 1)$.

The second problem is associated with the construction of new families of almost difference sets which are structures very close to DSs. If Γ is of order v then a k-subset D in Γ is a (v, k, λ, t)-*almost difference set* ADS (in Γ) if $\delta_D(x)$ takes on the value λ altogether t times and $\lambda + 1$ altogether $v - t - 1$ times as x ranges over $\Gamma \setminus \{0\}$. That is,

$$\delta_D(x) = |(D + x) \cap D| = \lambda \text{ or } \lambda + 1$$

for each $x \in \Gamma \setminus \{0\}$.

Number theoretic constraints can be applied to show that some groups cannot contain ADSs with certain parameters [18]. One example is that $(v - 1)\lambda + t = k(k - 1)$ must hold for any ADS. Other criteria can be discovered by examining the quotient groups of the original group. Despite the effectiveness of these techniques, no general existence criterion is known to determine exactly which groups contain ADSs [19]. There exist several construction methods of almost difference sets [20, 21, 22, 23, 24, 25, 18]. These constructions come from: difference sets, cyclotomic classes of finite fields, support of some functions, binary sequences with three-level autocorrelation, or larger product group. For a good survey of almost difference sets, the reader is referred to [26].

In Chapter 4, which is based on the paper [1], we prove the following theorems.

Theorem (Chapter 3, Theorem 4)**.** For all prime power, $q \equiv 1 \bmod 3$ greater than 4, there is a

$$\left(\frac{q^2+q+1}{3}, q, 2, 2(q-1)\right)\text{-ADS.}$$

Theorem (Chapter 3, Theorem 5)**.** Let D be a (v, k, λ) difference set in Γ. If

1. $g \in \Gamma \setminus D$;

2. $(g - D) \cap (D - g) = \emptyset$,

then $D \cup \{g\}$ is a $(v, k+1, \lambda, v-1-2k)$ almost difference set in Γ.

Theorem (Chapter 3, Theorem 6)**.** Let D be a (v, k, λ) difference set in Γ. If

1. $d \in D$;

2. $(d - D) \cap (D - d) = \{0\}$,

then $D \setminus \{d\}$ is a $(v, k-1, \lambda-1, 2(k-1))$ almost difference set in Γ.

And, as an application, using a result that relates almost difference set and 2-adesign [27], we construct new 2-adesigns from these new almost difference sets.

Corollary (Chapter 3, Corollary 3)**.** For all prime power $q \equiv 1 \bmod 3$ greater than 4, there is a symmetric 2-$\left(\frac{q^2+q+1}{3}, q, 2\right)$ adesign.

Corollary (Chapter 3, Corollary 4)**.** For all power prime q, there is a symmetric 2-$(q^2+q+1, q+2, 1)$ adesign.

In graph theory, given a fixed graph H, a graph G that does not contain H as a subgraph is called H-free, and an H-free graph that contains a copy of H after the addition of any edge is called H-saturated. The Turán number of H, denoted by $ex(n, H)$, is the maximum number of edges in an n-vertex H-free graph. Determining Turán numbers for different families of graphs is one of the most studied problems in extremal graph theory. In particular, for $H = C_4$, the cycle on four vertices, Reiman [28] showed a general upper bound

$$ex(n, C_4) \leq \frac{n}{4}(1 + \sqrt{4n-3}). \tag{1.1}$$

Brown [29] and Erdös-Rényi-Sós [30] independently constructed graphs that show that (1.1) is asymptotically best possible. These graphs are called Erdös-Rényi orthogonal polarity graphs or Brown graphs, and they are constructed using an orthogonal polarity of the projective plane $PG(2,q)$. The construction is as follows. Let q be a prime power. The Erdös-Rényi graph, denoted ER_q, is the graph whose vertices are the points of $PG(2,q)$, and two distinct vertices (x_0,x_1,x_2) and (y_0,y_1,y_2) are adjacent if and only if $x_0y_0+x_1y_1+x_2y_2=0$. It is well known that this graph has q^2+q+1 vertices, has $\frac{1}{2}q(q+1)^2$ edges, and is C_4-free. So for any prime power q, we know that

$$\frac{1}{2}q(q+1)^2 \leq ex(q^2+q+1, C_4). \tag{1.2}$$

Füredi [31] proved that (1.2) is best possible, and that, any C_4-free graph with q^2+q+1 vertices and $\frac{1}{2}q(q+1)^2$ edges is an orthogonal polarity graph of some projective plane of order q, provided $q \geq 15$. Although the best known application of ER_q is in extremal graph theory, these graphs have applications in hypergraph Turán theory, Ramsey theory, and structural graph theory [32, 33, 34]. The adjacency relation in ER_q is not the most suitable for our algebraic manipulations, for this reason, we will use an isomorphic graph to ER_q. This graph was constructed by Mubayi and Williford in [35], and it is denoted by ER_q^*. Apparently, it is more convenient to work with ER_q^*. For example, in [36] and [11], the authors used B_2 sets to construct graphs which are isomorphic to induced subgraphs of ER_q^*, and therefore isomorphic to ER_q. The graph constructed in [36, 11] is called sum graph and its construction is as follows: given a B_2 set A of an additive group Γ, the *sum graph* $G_{\Gamma,A}=(V,E)$ is formed by $V=\Gamma$ and $\{x,y\}\in E$ if $x+y\in A$ with $x\neq y$. Tait and Timmons [11] proved as their main result that the sum graph of a Bose-Chowla type B_2 set is an induced subgraph of ER_q. In the same direction, Peng et al. [36] proved that the sum graph of the Erdös-Turán type B_2 set $\mathcal{C}=\{(x,x^2): x\in\mathbb{F}_q\}$ is isomorphic to an induced subgraph of ER_q. Recently, Erskine, Fratric and Sirán [37] proved that the sum graph of a Singer type B_2 set is isomorphic to ER_q.

In Chapter 4, based on [3], we use the sum graph of a Singer type B_2 set to establish additive proofs of some structural properties (known and new) of the Erdös-Rényi orthogonal polarity graph. Our main result is the following.

Theorem (Chapter 4, Theorem 10)**.** Let $\mathcal{R}$ be a Ruzsa type B_2 set in $\Gamma=\mathbb{Z}_{p^2-p}$. Then the sum graph $G_{\Gamma,\mathcal{R}}$ is isomorphic to an induced subgraph of ER_p.

The distribution of the content of this thesis is as follows: In Appendix (Preliminaries) we present the notation used throughout this work, as well as some definitions and known results that we consider necessary for the development of the chapters. In Chapter 3 (Difference Set) we introduce the concept of difference set, we present some necessary conditions for its existence and we show the non-existence of $(p^m,k,1)$-DS. In Chapter

4 (Almost Difference Set) we define the almost difference sets, we present three new constructions of this type of sets and using these constructions we derive new 2-adesign. In Chapter 5 (The Erdös-Rényi Orthogonal Polarity Graph: Additive Interpretation) we present the additive interpretation of the Erdös-Rényi Orthogonal Polarity Graph and we establish additive proofs of some structural properties of this graph. Finally, in Chapter 6 (Conclusion And Future Work) we briefly summarize the results obtained in this thesis and we propose some new research problems.

Chapter 2

Difference Set

Remark 2. This chapter is a version of the material appearing in the paper "Non-existence of $(p^m, k, 1)$ difference sets", Electronics Letters, **58** (2022), no. 4, 154-155. Co-authored with C. Martos and C. Trujillo.

Difference sets play an important role in discrete mathematics, either for their mathematical interest or for their applications to other areas. The history of these sets reaches back to Singer's paper [12]. Later, Hall [38] considered difference sets in cyclic groups and introduced the concept of multipliers. Finally, Bruck [39] investigated these sets in arbitrary groups. Difference sets have been studied extensively and they have many interesting applications in computer science [40], interleaved linear arrays [41], etc. A variety of real-world applications can be found in [42]. A k-subset D in an additive group Γ of order v is called a (v, k, λ) *difference set* DS (in Γ) if $\delta_D(x) = \lambda$ for every nonzero element of Γ, where $\delta_D(x)$ is the difference function defined in Preliminares.

The order of the difference set D is defined as $n = k - \lambda$. Moreover, if Γ is abelian and $\lambda = 1$, then D is called an abelian planar difference set (APDS).

Singer's construction [12] guarantees the existence of APDS's provided that n is a prime power. It is conjectured that there are no APDS's whose order is not a prime power. Evans and Mann [43] proved this for cyclic difference sets with $n \leq 1600$, and Gordon [44] extended this for $n \leq 2{,}000{,}000$. This conjecture is known in the literature as the Prime Power Conjecture.

In this chapter, we prove the non-existence of abelian difference sets with parameters

$(p^m, k, 1)$, where $m \geq 2$ is an integer and p is a prime.

2.1 Necessary conditions

If D is a (v, k, λ)-*difference set* in an additive group Γ, then by definition, the parameters must satisfy the equality

$$k(k-1) = \lambda(v-1)$$

and therefore the cardinal of D must be equal to

$$k = \frac{1+\sqrt{4\lambda(v-1)+1}}{2}.$$

In particular, if D is an APDS in Γ then

$$k = \frac{1+\sqrt{4v-3}}{2},$$

and therefore

$$4v - 3 = x^2 \tag{2.1}$$

for some positive odd x.

Other two conditio ns necessary for the existence of an abelian planar difference set are Theorem 1 and Theorem 2, see [44].

Theorem 1. Let n be a positive integer such that $n \equiv 1, 2 \pmod 4$. If the squarefree part of n is divisible by a prime $p \equiv 3 \pmod 4$, then no APDS of order n exists.

Theorem 2. The order of an APDS cannot be divisible by 6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46, 51, 55, 57, 58, 62 or 65.

Remark 3. The condition in Equation (2.1) is necessary, but not sufficient. Indeed, if $v = q^2 + q + 1$ with $q \in \mathbb{N}$, then

$$4(q^2+q+1) - 3 = (2q+1)^2,$$

therefore, $x = 2q + 1$; hence, $k = q + 1$. However, if $q = 6$, then the order of an APDS would be $n = k - \lambda = 7 - 1 = 6$, which is not possible by Theorem 1. Nevertheless, Singer [12] proved that there is always an APDS with parameters $(q^2 + q + 1, q + 1, 1)$ when q is a prime power. For example, if $q = 4$ then $D = \{0, 1, 6, 8, 18\}$ is an APDS in $\mathbb{Z}_{21}$. The order in this case is $n = 4 = 2^2$ (prime power).

2.2 Non-existence of $(p^m, k, 1)$ difference sets

The following question arises: which groups admit abelian planar difference sets? This question has been studied by several researchers, who have obtained important results on the existence and non-existence of difference sets in abelian and non-abelian groups. For example, in [13] proved that there is no abelian difference set with parameters (261, 105, 42), and in [14] proved that there is no abelian difference set with parameters (220, 73, 24) and (231, 70, 21). For other non-existence results, see [17, 16, 15].

We study this problem in groups of order p^m. For this value of $v = |\Gamma| = p^m$, the cardinal of an APDS in Γ must be equal to

$$k = \frac{1+\sqrt{4p^m - 3}}{2} \tag{2.2}$$

and therefore we have the Diophantine equation

$$x^2 + 3 = 4p^m. \tag{2.3}$$

Luca, Tengely, and Togbe studied the Diophantine equation

$$x^2 + C = 4y^m, \tag{2.4}$$

and they obtained all its integer solutions when $x \geq 1$, $y \geq 1$, $\gcd(x, y) = 1$, $m \geq 3$, $C \equiv 3 \pmod 4$, and $1 \leq C \leq 100$, see [45].

Remark 4. In particular, when $C = 3$, Luca, Tengely, and Togbe proved that the only integer solutions (m, x, y) of Equation (2.4) are $(m, 1, 1)$, and $(3, 37, 7)$.

When p is prime, we obtain the following result.

Lemma 1. The only integer solution of Equation (2.3), with $x \geq 1$, $p \geq 1$ prime, and $m \geq 3$, is when $m = 3, x = 37$, and $p = 7$.

Proof.

Case 1. If $p \nmid x$, then $\gcd(x, p) = 1$. Then the result follows from Remark 4 because p is prime.

Case 2. If $p \mid x$, then $x = pr$ with $r \in \mathbb{N}$, and Equation (2.3) implies that

$$p^2 r^2 + 3 = 4p^m,$$

then $p \mid 3$, and so $p = 3$. Thus

$$3^2 r^2 + 3 = 4(3^m)$$

and so $3r^2 + 1 = 4(3^{m-1})$. This last equation has an integer solution only if $m = 1$ and $r = 1$ ($m > 1$ implies that $1 \equiv 0 \bmod 3$ which is not possible). □

As a consequence of Lemma 1, we have the following result.

Theorem 3. If p is a prime number and $m \geq 2$ is an integer then, there are no abelian planar difference sets with parameters $(p^m, k, 1)$.

Proof. **Case 1.** p prime and $m = 2$.
In this case, the associated Diophantine equation is

$$x^2 + 3 = 4p^2 \quad \text{(see Equation (2.3))}.$$

When p is prime, the above equation does not have an integer p solution, because $3 = (2p - x)(2p + x)$ implies that $p = \pm 1$.

Case 2. p prime and $m > 2$.
By Lemma 1, an abelian planar difference set D can exist in a group Γ of order p^m only if its parameters are $(7^3, 19, 1)$, that is, $|\Gamma| = v = 7^3$, and $|D| = k = 19$ (see Equation (2.2)). In this situation, the order of D is $n = 19 - 1 = 18$, but this is not possible by Theorem 2. □

Chapter 3

Almost Difference Set

Remark 5. This chapter is a version of the material appearing in the paper "Almost difference sets from Singer type Golomb rulers", IEEE Access, **10** (2022), 1132-1137. Co-authored with C. Martos and C. Trujillo.

Many groups do not have DSs for any parameters k and λ, but do have structures that are very close to DSs, which motivates the following definition.

A k-subset D in an additive group Γ of order v is said to be a (v, k, λ, t)-*almost difference set* ADS (in Γ) if $\delta_D(x)$ takes on the value λ altogether t times and $\lambda + 1$ altogether $v - t - 1$ times as x ranges over $\Gamma \setminus \{0\}$. This is,

$$\delta_D(x) = |(D + x) \cap D| = \lambda \text{ or } \lambda + 1,$$

for each $x \in \Gamma \setminus \{0\}$.

Note that almost difference sets are a generalization of difference sets (when $t = 0$ or $t = v - 1$). Moreover, for an almost difference set D with parameters (v, k, λ, t), its complement $\Gamma \setminus D$ is also an almost difference set with parameters $(v, v - k, v - 2k + \lambda, t)$. An almost difference set D is called *abelian* or *cyclic* if the group Γ is abelian or cyclic, respectively. Almost all difference sets are interesting combinatorial objects that have several applications in many engineering areas. In coding theory, they can be employed, to construct cyclic codes [46]. Additionally, in cryptography, they can be used to construct functions with optimal nonlinearity [47, 48]. Finally, for CDMA communications, some cyclic almost difference sets yield sequences with optimal autocorrelation [20, 49, 23].

In this chapter, we use Singer type B_2 sets (which are difference sets with $\lambda = 1$, or almost difference set with $\lambda = 0$ and $t = 0$) to construct new families of almost difference sets. These constructions are new, as far as we are aware of. The first construction yields $(N/3, q, 2, 2(q-1))$-ADSs in cyclic groups of order $N/3$, where $N = q^2 + q + 1$ and $q \equiv 1 \bmod 3$ is a prime power greater than 4. This construction uses homomorphic projection. The second construction is obtained by adding a new element to the B_2 set and yields $(q^2 + q + 1, q + 2, 1, (q-2)(q+1))$-ADSs in cyclic groups of order $q^2 + q + 1$ for all prime power q. The third construction is obtained by removing an element of the B_2 set and yields $(q^2 + q + 1, q, 0, 2q)$-ADSs in cyclic groups of order $q^2 + q + 1$ for all prime power q. The latest constructions follow the idea proposed in [20].

Another contribution of this chapter is related to t-adesign, which was defined in [22]. Let $D = (\mathcal{P}, \mathcal{B}, \mathcal{I})$ be an incidence structure with $v \geq 1$ points and $b \geq 1$ blocks, where every block has size k. If every subset of t points of $\mathcal{P}$ is incident with either λ or $\lambda + 1$ blocks of $\mathcal{B}$, then D is called a t-(v, k, λ) adesign, or simply t-adesign. A t-adesign is symmetric if $v = b$. The set $\{D + g : g \in \Gamma\}$ of translates of D, denoted by $Dev(D)$, is called the development of D. The following lemma was established in [27] and provides a relationship between almost difference set and t-adesign.

Lemma 2. Let D be a (v, k, λ) almost difference set in an abelian group Γ. Then, $(\Gamma, Dev(D))$ is a 2-(v, k, λ) adesign.

Using the above lemma and the almost difference sets constructed in this chapter, we give constructions of 2-adesigns.

Next, we describe three new constructions of almost difference sets from Singer type B_2 sets. These constructions can generate infinitely many almost difference sets in $\mathbb{Z}_n$ for appropriate values of n.

3.1 Construction 1

The following theorem shows how to construct an almost difference set from a Singer type B_2 set using homomorphic projection.

Theorem 4. For all prime power, $q \equiv 1 \bmod 3$ greater than 4, there is a

$$\left(\frac{q^2 + q + 1}{3}, q, 2, 2(q-1)\right)\text{-ADS.}$$

Proof. According to Singer's construction, for every prime power q, there is a B_2 set $\mathcal{S}$

in $\mathbb{Z}_{q^2+q+1}$, with $q+1$ elements, particularly for $q \equiv 1 \bmod 3$.
Let $\varphi : \mathbb{Z}_{q^2+q+1} \to \mathbb{Z}_{\frac{q^2+q+1}{3}}$ be the homomorphism defined by

$$\varphi(a) \equiv a \bmod \left(\frac{q^2+q+1}{3}\right),$$

and $D = \varphi(\mathcal{S})$.

Note that, $|D| = q$; indeed, as $\frac{q^2+q+1}{3} \in \mathbb{Z}_{q^2+q+1} \setminus \{0\} = \mathcal{S} \ominus \mathcal{S}$ (see Lemma 5 (ii)), then there are two different elements a and b in $\mathcal{S}$ such that $a - b \equiv \frac{q^2+q+1}{3} \mod (q^2+q+1)$, hence, $a \equiv b \mod (\frac{q^2+q+1}{3})$, that is, $\varphi(a) = \varphi(b)$. Note that there is no other pair of elements $c, d \in \mathcal{S}$ such that $c \equiv d \mod (\frac{q^2+q+1}{3})$, because this contradicts the fact that $\mathcal{S}$ is a B_2 set. Therefore, $|D| = q$.

Let $\mathcal{S} = \{s_1, s_2, \ldots, s_{q+1}\}$ with $s_1 \equiv s_2 \bmod \frac{q^2+q+1}{3}$, and let $D = \{d_1, d_2, \ldots, d_q\}$, where $d_1 = \varphi(s_1) = \varphi(s_2)$ and $d_{i-1} = \varphi(s_i)$, for $3 \leq i \leq q+1$.

Note that for each $x \in \mathbb{Z}_{\frac{q^2+q+1}{3}} \setminus \{0\}$, there are two distinct elements $x_1 = x + \frac{q^2+q+1}{3}$ and $x_2 = x + 2\left(\frac{q^2+q+1}{3}\right)$ in $\mathbb{Z}_{q^2+q+1}$ for which

$$\varphi(x) = \varphi(x_1) = \varphi(x_2). \tag{3.1}$$

On the other hand, by (see Lemma 5 (ii)) there are unique elements s_i, s_j, s_k, s_l, s_t and s_r in $\mathcal{S}$ such that

$$x = s_i - s_j, x_1 = s_k - s_l, \text{ and } x_2 = s_t - s_r,$$

so, by (3.1)

$$\varphi(x) = \varphi(s_i) - \varphi(s_j) = \varphi(s_k) - \varphi(s_l) = \varphi(s_t) - \varphi(s_r),$$

this is,

$$\varphi(x) = d_i - d_j = d_k - d_l = d_t - d_r.$$

As $\varphi(s_1) = \varphi(s_2) = d_1$ then for $3 \leq j \leq q+1$, the $4(q-1)$ pairwise distinct elements

$$s_1 - s_j, s_2 - s_j, s_j - s_1, s_j - s_2$$

satisfy that

$$\varphi(s_1) - \varphi(s_j) = \varphi(s_2) - \varphi(s_j) = d_1 - d_j, \text{ and } \varphi(s_j) - \varphi(s_1) = \varphi(s_j) - \varphi(s_2) = d_j - d_1,$$

therefore, there are $2(q-1)$ distinct elements of $\mathbb{Z}_{\frac{q^2+q+1}{3}}$ that have two different representations as differences of elements in D. The other $\frac{q^2-5q+4}{3}$ elements of $\mathbb{Z}_{\frac{q^2+q+1}{3}}$ can be written in three different ways as differences of elements in D. Thus, D is a $(\frac{q^2+q+1}{3}, q, 2, 2(q-1))$-ADS. □

Example 1. The set $\mathcal{S} = \{0, 1, 6, 21, 28, 44, 46, 54\}$ is a Singer type B_2 set in $\mathbb{Z}_{57}$. Reducing the elements of $\mathcal{S}$ modulo $57/3 = 19$ gives the set

$$\{0, 1, 2, 6, 8, 9, 16\},$$

which is a $(19, 7, 2, 12)$ almost difference set in $\mathbb{Z}_{19}$ by Theorem 4.

Example 2. The set $\mathcal{S} = \{0, 1, 3, 24, 41, 52, 57, 66, 70, 96, 102, 149, 164, 176\}$ is a Singer type B_2 set in $\mathbb{Z}_{183}$. Reducing the elements of $\mathcal{S}$ modulo 183/3=61 gives the set

$$\{0, 1, 3, 5, 9, 24, 27, 35, 41, 42, 52, 54, 57\},$$

which is a $(61, 13, 2, 24)$ almost difference set in $\mathbb{Z}_{61}$ by Theorem 4.

3.2 Construction 2

The following proposition shows how to construct an almost difference from a difference set by adding an element.

Proposition 1. Let D be a $(v, \frac{v-1}{4}, \frac{v-5}{16})$ difference set in Γ, and let $d \in \Gamma \backslash D$. If $2d$ cannot be written as the sum of two distinct elements of D, then $D \cup \{d\}$ is a $(v, \frac{v+3}{4}, \frac{v-5}{16}, \frac{v-1}{2})$ almost difference set in Γ, see [20].

Using the same idea of Proposition 1, we obtain the following result.

Theorem 5. Let D be a (v, k, λ) difference set in Γ. If

1. $g \in \Gamma \setminus D$;

2. $(g - D) \cap (D - g) = \emptyset$,

then $D \cup \{g\}$ is a $(v, k + 1, \lambda, v - 1 - 2k)$ almost difference set in Γ.

Proof. Let $D = \{d_1, d_2, \ldots, d_k\}$. If $(g - D) \cap (D - g) = \emptyset$, then $2g$ cannot be written as a sum of two distinct elements of D; therefore

$$\begin{gathered} g - d_1, g - d_2, \ldots, g - d_k \\ d_1 - g, d_2 - g, \ldots, d_k - g \end{gathered}$$

are $2k$ pairwise distinct elements. Because D is a (v, k, λ) difference set, $D \cup \{g\}$ is a $(v, k + 1, \lambda, v - 1 - 2k)$ almost difference set. □

Corollary 1. There is a $(q^2+q+1, q+2, 1, (q-2)(q+1))$-ADS in $\mathbb{Z}_{q^2+q+1}$, for all prime power q.

Proof. According to Singer's construction, for every prime power q, there is a Singer type B_2 set $\mathcal{S}$ in $\mathbb{Z}_{q^2+q+1}$. In particular, $\mathcal{S}$ is a $(q^2+q+1, q+1, 1)$-DS. Then, the result follows applying Theorem 5 with a suitable element in $\mathbb{Z}_{q^2+q+1} \setminus \mathcal{S}$. □

Example 3. The set $\mathcal{S} = \{0, 1, 4, 6\}$ is a Singer type B_2 set in $\mathbb{Z}_{13}$. Since

1. $8 \in \mathbb{Z}_{13} \setminus \mathcal{S}$;
2. $8 - \mathcal{S} = \{2, 4, 7, 8\}$;
3. $\mathcal{S} - 8 = \{5, 6, 9, 11\}$;
4. $(8 - \mathcal{S}) \cap (\mathcal{S} - 8) = \emptyset$.

Then, $\mathcal{S} \cup \{8\} = \{0, 1, 4, 6, 8\}$, is a $(13, 5, 1, 4)$ almost difference set in $\mathbb{Z}_{13}$ by Theorem 5.

Example 4. The set $\mathcal{S} = \{0, 1, 11, 19, 26, 28\}$ is a Singer type B_2 set in $\mathbb{Z}_{31}$. Since

1. $17 \in \mathbb{Z}_{31} \setminus \mathcal{S}$;
2. $17 - \mathcal{S} = \{6, 16, 17, 20, 22, 29\}$;
3. $\mathcal{S} - 17 = \{2, 9, 11, 14, 15, 25\}$;
4. $(17 - \mathcal{S}) \cap (\mathcal{S} - 17) = \emptyset$.

Then, $\mathcal{S} \cup \{17\} = \{0, 1, 11, 17, 19, 26, 28\}$, is a $(31, 7, 1, 18)$ almost difference set in $\mathbb{Z}_{31}$ by Theorem 5.

Remark 6. Two elements cannot be added to a Singer type B_2 set $\mathcal{S}$ in Theorem 5 to obtain a $(q^2+q+1, q+3, 1, t)$ almost difference set. Indeed, let x_1 and x_2 be two distinct elements in $\mathbb{Z}_{q^2+q+1} \setminus \mathcal{S}$ and $D = \mathcal{S} \cup \{x_1, x_2\}$. As $x_1 \neq x_2$, then $x_1 - x_2 \in \mathcal{S} \ominus \mathcal{S}$ (see Lemma 5 (ii)), so

$$y := x_1 - s_1 = x_2 - s_2$$

for some $s_1, s_2 \in \mathcal{S}$ ($s_1 \neq s_2$). As $y \neq 0$, then $y \in \mathcal{S} \ominus \mathcal{S}$. Therefore, y can be written in three different ways as differences of elements in D.

Example 5. The set $\{0, 1, 11, 19, 26, 28\}$ is a Singer type B_2 set in $\mathbb{Z}_{31}$. By adding 9, and 24, we obtain the set $D = \{0, 1, 9, 11, 19, 24, 26, 28\}$. Note that 9 and 24 cannot be written as the sum of two distinct elements of D, but the element 29 in $\mathbb{Z}_{31}$ can be written as $24 - 26 \equiv 9 - 11 \equiv 26 - 18$. Other elements in $\mathbb{Z}_{31}$ can also be written in three different ways as differences of elements in D; for example 8.

3.3 Construction 3

The following proposition shows how to construct an almost difference set from a difference set by removing an element.

Proposition 2. Let D be a $(v, \frac{v+3}{4}, \frac{n+3}{16})$ difference set in Γ, and let $d \in D$. If $2d$ cannot be written as the sum of two distinct elements of D, then $D \setminus \{d\}$ is a $(v, \frac{v-1}{4}, \frac{v-13}{16}, \frac{v-1}{2})$ almost difference set in Γ, see [20].

Using the same idea of Proposition 2, we obtain the following result.

Theorem 6. Let D be a (v, k, λ) difference set in Γ. If

1. $d \in D$;
2. $(d - D) \cap (D - d) = \{0\}$,

then $D \setminus \{d\}$ is a $(v, k - 1, \lambda - 1, 2(k - 1))$ almost difference set in Γ.

Proof. Let $D = \{d, d_2, \ldots, d_k\}$. If $(d - D) \cap (D - d) = \{0\}$, then $2d$ cannot be written as a sum of two distinct elements of D; therefore

$$d - d_2, d - d_3, \ldots, d - d_k$$
$$d_2 - d, d_3 - d, \ldots, d_k - d$$

are $2(k - 1)$ pairwise distinct elements. Because D is a (v, k, λ) difference set, $D \setminus \{d\}$ is a $(v, k - 1, \lambda - 1, 2(k - 1))$ almost difference. □

Corollary 2. There is a $(q^2 + q + 1, q, 0, 2q)$-ADS in $\mathbb{Z}_{q^2+q+1}$, for all prime power q.

Proof. According to Singer's construction, for every prime power q, there is a Singer type B_2 set $\mathcal{S}$ in $\mathbb{Z}_{q^2+q+1}$. In particular, $\mathcal{S}$ is a $(q^2 + q + 1, q + 1, 1)$-DS. Then, the result follows applying Theorem 6 with a suitable element in $\mathbb{Z}_{q^2+q+1} \setminus \mathcal{S}$. □

Example 6. The set $\mathcal{S} = \{0, 1, 11, 19, 26, 28\}$ is a Singer type B_2 set in $\mathbb{Z}_{31}$. Since

1. $26 \in \mathcal{S}$;
2. $26 - \mathcal{S} = \{0, 7, 15, 25, 26, 29\}$;
3. $\mathcal{S} - 26 = \{0, 2, 5, 6, 16, 24\}$;
4. $(26 - \mathcal{S}) \cap (\mathcal{S} - 26) = \{0\}$.

Then, $\mathcal{S} \setminus \{26\} = \{0, 1, 11, 17, 19, 28\}$, is a $(31, 6, 0, 10)$ almost difference set in $\mathbb{Z}_{31}$ by Theorem 6.

Example 7. The set $\mathcal{S} = \{0, 1, 3, 24, 41, 52, 57, 66, 70, 96, 102, 149, 164, 176\}$ is a Singer type B_2 set in $\mathbb{Z}_{183}$. Since

1. $70 \in \mathcal{S}$;
2. $70 - \mathcal{S} = \{0, 4, 13, 18, 29, 46, 67, 69, 70, 77, 89, 104, 151, 157\}$;
3. $\mathcal{S} - 70 = \{0, 26, 32, 79, 94, 106, 113, 114, 116, 137, 154, 165, 170, 179\}$;
4. $(70 - \mathcal{S}) \cap (\mathcal{S} - 70) = \{0\}$.

Then, $\mathcal{S} \setminus \{70\} = \{0, 1, 3, 24, 41, 52, 57, 66, 96, 102, 149, 164, 176\}$, is a $(183, 12, 0, 26)$ almost difference set in $\mathbb{Z}_{183}$ by Theorem 6.

Remark 7. The process in Theorem 6 can be continued recursively to obtain an almost difference set with parameters $(q^2 + q + 1, q + 1 - i, 0, 2(iq - \binom{i}{2}))$, where $1 \leq i < q$ is the number of elements that are removed.

Example 8. The set $\{0, 1, 6, 8, 18\}$ is a Singer type B_2 set in $\mathbb{Z}_{21}$. By removing 6, we obtain $\{0, 1, 8, 18\}$, which is a $(21, 4, 0, 8)$-ADS. By removing 1 of this set, we obtain $\{0, 8, 18\}$, which is a $(21, 3, 0, 14)$-ADS. By removing 18 of the above set, we obtain $\{0, 8\}$, which is a $(21, 2, 0, 18)$-ADS.

3.4 Constructions of symmetric 2-adesigns

From Theorem 4, Theorem 5, and Lemma 2, we obtain corollaries 3 and 4, respectively.

Corollary 3. For all prime power $q \equiv 1 \bmod 3$ greater than 4, there is a symmetric 2-$\left(\frac{q^2+q+1}{3}, q, 2\right)$ adesign.

Example 9. The set $D = \{0, 1, 2, 6, 8, 9, 16\}$ is a $(19, 7, 2, 12)$ almost difference set in $\mathbb{Z}_{19}$ (see Example 1). By Lemma 2, we obtain a symmetric 2-$(19, 7, 2)$ adesign with the following blocks of size 7:

$\{0, 1, 2, 6, 8, 9, 16\}$
$\{1, 2, 3, 7, 9, 10, 17\}$
$\{2, 3, 4, 8, 10, 11, 18\}$
$\{3, 4, 5, 9, 11, 12, 0\}$
$\{4, 5, 6, 10, 12, 13, 1\}$
$\{5, 6, 7, 11, 13, 14, 2\}$
$\{6, 7, 8, 12, 14, 15, 3\}$
$\{7, 8, 9, 13, 15, 16, 4\}$
$\{8, 9, 10, 14, 16, 17, 5\}$
$\{9, 10, 11, 15, 17, 18, 6\}$
$\{10, 11, 12, 16, 18, 0, 7\}$
$\{11, 12, 13, 17, 0, 1, 8\}$
$\{12, 13, 14, 18, 1, 2, 9\}$
$\{13, 14, 15, 0, 2, 3, 10\}$
$\{14, 15, 16, 1, 3, 4, 11\}$
$\{15, 16, 17, 2, 4, 5, 12\}$
$\{16, 17, 18, 3, 5, 6, 13\}$
$\{17, 18, 0, 4, 6, 7, 14\}$
$\{18, 0, 1, 5, 7, 8, 15\}$

Corollary 4. For all power prime q, there is a symmetric 2-$(q^2 + q + 1, q+2, 1)$ adesign.

Example 10. The set $D = \{0, 1, 4, 6, 8\}$ is a $(13, 5, 1, 4)$ almost difference set in $\mathbb{Z}_{13}$ (see Example 3). By Lemma 2, we obtain a symmetric 2-$(13, 5, 1)$ adesign with the following blocks of size 5:

$\{0, 1, 4, 6, 8\}$
$\{1, 2, 5, 7, 9\}$
$\{2, 3, 6, 8, 10\}$
$\{3, 4, 7, 9, 11\}$
$\{4, 5, 8, 10, 12\}$
$\{5, 6, 9, 11, 0\}$
$\{6, 7, 10, 12, 1\}$
$\{7, 8, 11, 0, 2\}$
$\{8, 9, 12, 1, 3\}$
$\{9, 10, 0, 2, 4\}$
$\{10, 11, 1, 3, 5\}$
$\{11, 12, 2, 4, 6\}$
$\{12, 0, 3, 5, 7\}$

Chapter 4

The Erdös-Rényi Orthogonal Polarity Graph: Additive Interpretation

Remark 8. The following is part of the material appearing in the paper "Sidon sets and subgraphs of the Erdös-Rényi orthogonal polarity graph". Contributions to Discrete Mathematics. Submitted for evaluation. Co-authored with M. Huicochea, C. Martos and C. Trujillo.

In this chapter, let q be a prime power, $\mathcal{S}$ be a Singer type B_2 set in $\Gamma = \mathbb{Z}_{q^2+q+1}$ and $G_{\Gamma,\mathcal{S}}$ be the sum graph with respect to $\mathcal{S}$. Grahame, Fratrič and Širáň proved in [37] that $G_{\Gamma,\mathcal{S}}$ is isomorphic to ER_q, we reproduce the proof here for completeness.

First, they presented Lemma 3 (without proof), since $\mathcal{S}+m$ (for any integer m) and $r\mathcal{S}$ (for any positive integer r with $\gcd(q^2+q+1, r) = 1$) are also Singer type B_2 sets in Γ[1].

Lemma 3. Let $\mathcal{S}$ and $\mathcal{S}'$ be equivalent Singer type B_2 sets for the cyclic group Γ. Then the sum graphs $G_{\Gamma,\mathcal{S}}$ and $G_{\Gamma,\mathcal{S}'}$ are isomorphic.

Proof. Let m and r be integers with $\gcd(q^2+q+1, r) = 1$, and $\mathcal{S}' = \mathcal{S}+m := \{s+m : s \in \mathcal{S}\}$. We define $\varphi : \Gamma \longrightarrow \Gamma$ by $\varphi(i) = i + m/2$ (note that $\gcd(q^2+q+1, 2) = 1$).

[1]Two B_2 sets which are related in this way are called equivalent.

Then,

$$\begin{aligned} i + j = s \in \mathcal{S} \longrightarrow \varphi(i) + \varphi(j) &= i + m/2 + j + m/2 \\ &= i + j + m \\ &= s + m \in \mathcal{S}'. \end{aligned}$$

Thus, if i is adjacent to j in $G_{\Gamma,\mathcal{S}}$, then $\varphi(i)$ is adjacent to $\varphi(j)$ in $G_{\Gamma,\mathcal{S}'}$. Finally, $\varphi^{-1} : \Gamma \longrightarrow \Gamma$ is given by $\varphi^{-1}(i) = i - m/2$.

On the other hand, if $\mathcal{S}' = r\mathcal{S} := \{rs : s \in \mathcal{S}\}$, we define $\phi : \Gamma \longrightarrow \Gamma$ by $\phi(i) = ri$. So,

$$\begin{aligned} i + j = s \in \mathcal{S} \longrightarrow \phi(i) + \phi(j) &= ri + rj \\ &= r(i + j) \\ &= rs \in \mathcal{S}'. \end{aligned}$$

Thus, if i is adjacent to j in $G_{\Gamma,\mathcal{S}}$, then $\phi(i)$ is adjacent to $\phi(j)$ in $G_{\Gamma,\mathcal{S}'}$. Finally, since r is invertible, $\phi^{-1} : \Gamma \longrightarrow \Gamma$ is given by $\phi^{-1}(i) = i/r$. □

Halberstam and Laxton proved in [50] that all Singer type B_2 sets for a given prime power q are equivalent, so by Lemma 3 any sum graph obtained from a Singer type B_2 set is isomorphic to ER_q.

Proposition 3. $G_{\Gamma,\mathcal{S}} \cong ER_q$

Proof.

- Let $q = 4$, and $\mathbb{F}_4 = \{0, 1, \theta, \theta^2\}$ where θ is a primitive element of $\mathbb{F}_4^*$ with minimal polynomial $x^2 + x + 1 \in \mathbb{F}_4[x]$. Then,

  $V(ER_4) = PG(2, 4) = \{(1, 0, 1), (1, \theta^2, 1), (1, 1, 0), (1, \theta^2, \theta^2), (0, 1, 0), (1, \theta, \theta), (0, 1, \theta), (1, \theta, \theta^2), (1, \theta^2, \theta), (1, \theta^2, 0), (1, 0, 0), (0, 1, 1), (0, 0, 1), (1, \theta, 0), (1, 1, 1), (0, 1, \theta^2), (1, \theta, 1), (1, 0, \theta^2), (1, 0, \theta), (1, 1, \theta^2), (1, 1, \theta)\}$.

  By Lemma 3 it is enough to show that the sum graph of the Singer type B_2 set $S = \{0, 1, 4, 14, 16\}$ in $\Gamma = \mathbb{Z}_{21}$ is isomorphic to ER_4. An explicit isomorphism is given by

0	$(1,0,1)$	1	$(1,\theta^2,1)$	2	$(1,1,0)$
3	$(1,\theta^2,\theta^2)$	4	$(0,1,0)$	5	$(1,\theta,\theta)$
6	$(0,1,\theta)$	7	$(1,\theta,\theta^2)$	8	$(1,\theta^2,\theta)$
9	$(1,\theta^2,0)$	10	$(1,0,0)$	11	$(0,1,1)$
12	$(0,0,1)$	13	$(1,\theta,0)$	14	$(1,1,1)$
15	$(0,1,\theta^2)$	16	$(1,\theta,1)$	17	$(1,0,\theta^2)$
18	$(1,0,\theta)$	19	$(1,1,\theta^2)$	20	$(1,1,\theta)$

- Let $q \neq 4$. By [5], $\mathbb{F}_{q^3}$ has a primitive element θ with minimal polynomial

$$x^3 - (\alpha x + \beta) \in \mathbb{F}_q[x].$$

Note that $\beta \in \mathbb{F}_q^*$, since p is irreducible; and $\alpha \in \mathbb{F}_q^*$ since a cube root of an element in $\mathbb{F}_q$ must have multiplicative order at most $3(q-1)$ and so cannot be primitive in $\mathbb{F}_{q^3}$. The existence of this polynomial facilitates the calculations. Let $\mathcal{S}'$[2] be a Singer type B_2 set in Γ constructed from θ, see Appendix A.3.1. By Lemma 3 $G_{\Gamma,\mathcal{S}'} \cong G_{\Gamma,\mathcal{S}}$. Thus, it is enough to prove $G_{\Gamma,\mathcal{S}'} \cong ER_q$.

Let i and j be two distinct vertices in $G_{\Gamma,\mathcal{S}'}$. Remember that these vertices are adjacent if $i + j = k \in \mathcal{S}'$. Since Γ is isomorphic to $\mathbb{F}_{q^3}^*/\mathbb{F}_q^*$ by discrete logarithm to base θ, then

$$i + j = k \iff \theta^i\theta^j = \theta^k \in \{\overline{a+\theta} : a \in \mathbb{F}_q\} \cup \{\overline{1}\} \tag{4.1}$$

Writing down θ^i and θ^j in terms of the basis $\{1, \theta, \theta^2\}$ of $\mathbb{F}_{q^3}^*$ over $\mathbb{F}_q^*$, one has

$$\theta^i = x_0 + x_1\theta + x_2\theta^2 \text{ and } \theta^j = y_0 + y_1\theta + y_2\theta^2$$

for some $x_i, y_i \in \mathbb{F}_q^*$, $i \in \{0, 1, 2\}$. Now, using

$$\theta^3 = \alpha\theta + \beta \text{ and } \theta^4 = \alpha\theta^2 + \beta\theta,$$

we can rewrite (4.1) as:

$$i + j = k \iff \gamma + \delta\theta + (x_0y_2 + x_1y_1 + x_2y_0 + x_2y_2\alpha)\theta^2 \in \{\overline{a+\theta} : a \in \mathbb{F}_q\} \cup \{\overline{1}\}$$

where, $\gamma = x_0y_0 + (x_1y_2 + x_2y_1)\beta$ and $\delta = (x_0y_1 + x_1y_0 + (x_1y_2 + x_2y_1)\alpha + x_2y_2)$. Thus,

[2] $\mathcal{S}' := \{\log_\theta(\overline{\alpha + u}) : u \in \mathbb{F}_q\} \cup \{\log_\theta(\overline{1})\}$, see Appendix A.3.1

$$i + j = k \Longleftrightarrow x_0y_2 + x_1y_1 + x_2y_0 + x_2y_2\alpha = 0.$$

So, $G_{\Gamma,\mathcal{S}'} \cong ER_q^{**}$ (see Appendix A.6.2) and by Theorem 14 (ii) $G_{\Gamma,\mathcal{S}'} \cong ER_q$.

□

4.1 Some properties

Let i be a vertex of $G_{\Gamma,\mathcal{S}}$. Notice that the neighborhood $N(i)$ of i consists of the vertices $j \in \Gamma$ that satisfy $i + j = a$ for some $a \in \mathcal{S}$. This equation has a unique solution for each $a \in \mathcal{S}$, then there are $|\mathcal{S}| = q+1$ solutions, which are different from i if and only if $2i \neq a$. Since q^2+q+1 is odd, for each $a \in \mathcal{S}$ the equation $2i \equiv a \bmod (q^2+q+1)$ has unique solution. Then, $G_{\Gamma,\mathcal{S}}$ has q^2 vertices of degree $q+1$, and $q+1$ absolute vertices. Thus, the vertex set of $G_{\Gamma,\mathcal{S}}$ is a disjoint union of the sets

$V = \{x \in V(G_{\Gamma,\mathcal{S}}) : deg(x) = q+1\}$ and $P = \{x \in V(G_{\Gamma,\mathcal{S}}) : deg(x) = q\}$.

This is, $V(G_{\Gamma,\mathcal{S}}) = V \cup P$ where $|V| = q^2, |P| = q+1$, and $V \cap P = \emptyset$.

Let V_1 be the subset of V comprising all vertices adjacent to at least one absolute vertex and let $V_2 = V \setminus V_1$. We show the following structural information of the $G_{\Gamma,\mathcal{S}}$ graph.

Remark 9. Turán number $ex(q^2+q+1, C_4)$ in Theorem 7 (iv) is defined in Appendix A.4.

Theorem 7. The graph $G_{\Gamma,\mathcal{S}}$ has the following properties:

(i) The set P of absolute vertices is independent;

(ii) Each pair of vertices of V (adjacent or not) are connected by a unique path of length 2, while no edge incident to an absolute vertex is contained in any triangle; in particular, $G_{\Gamma,\mathcal{S}}$ has diameter 2;

(iii) If q is even, then $|V_1| = q^2$ and V_2 is empty; moreover, V_1 contains a vertex v adjacent to all absolute vertices and every vertex in $V_1 \setminus \{v\}$ is adjacent to exactly one absolute vertex and the subgraph of $G_{\Gamma,\mathcal{S}}$ induced by the set $V_1 \setminus \{v\}$ is regular of degree q;

(iv) For all prime powers $q > 13$, $ex(q^2+q+1, C_4) = |E(G_{\Gamma,\mathcal{S}})| = \frac{1}{2}q(q+1)^2$.

Proof. (i) Let i and j be two distinct vertices in P. Then, there are a and b in $\mathcal{S}$ ($a \neq b$) such that $2i = a$ and $2j = b$. If i is adjacent to j, then $i + j = c$ for some $c \in \mathcal{S} \setminus \{a, b\}$. Therefore,

$$\begin{aligned} a + b &= 2i + 2j \\ &= 2(i + j) \\ &= 2c. \end{aligned}$$

Since $\mathcal{S}$ is a B_2 set in Γ, $a = b = c$ which is not possible.

(ii) Let i and j be two vertices in $G_{\Gamma,\mathcal{S}}$. Since $i - j \in \Gamma \setminus \{0\}$, and $d_{\mathcal{S}}(i - j) = 1$ (see Lemma 5 (ii)), there are a and $b \in \mathcal{S}$ such that $i - j = a - b$ and so, the vertex $z = b - j = a - j$ is adjacent to i and j. This implies that $G_{\Gamma,\mathcal{S}}$ has diameter 2. Note that the uniqueness of the path is followed because $G_{\Gamma,\mathcal{S}}$ is C_4-free (see Proposition 10). Let i and j be two distinct vertices in $G_{\Gamma,\mathcal{S}}$ such that $i + j = a$ and $2i = b$ for some $a, b \in \mathcal{S}$ with $a \neq b$. On the other hand, no edge incident to an absolute vertex is contained in any triangle because if there is some $k \in \Gamma \setminus \{i, j\}$ that is adjacent to both i and j, then $i+k = c$ and $j+k = d$ for some $c, d \in \mathcal{S} \setminus \{a, b\}$ ($c \neq d$). Thus,

$$\begin{aligned} a + c &= (i + j) + (i + k) \\ &= (2i) + (j + k) \\ &= b + d. \end{aligned}$$

Since $\mathcal{S}$ is a B_2 set in Γ, $\{a, c\} = \{b, d\}$ which is not possible.

(iii) By First Multiplier Theorem (Theorem 12) with $p = 2$, there is a Singer type set B_2, $\mathcal{S}'$ in Γ such that $\mathcal{S}' = g + \mathcal{S}$ for some $g \in \Gamma$, and $2\mathcal{S}' = \mathcal{S}'$. Note that $G_{\Gamma,\mathcal{S}} \cong G_{\Gamma,\mathcal{S}'}$ by Lemma 3. Let V_1' be the subset of $V(G_{\Gamma,\mathcal{S}'})$ comprising all vertices adjacent to at least one absolute vertex and let $V_2' = V(G_{\Gamma,\mathcal{S}'}) \setminus V_1'$. By Lemma 5 (ii), $\Gamma \setminus \{0\} = \mathcal{S}' \ominus \mathcal{S}' = 2\mathcal{S}' \ominus \mathcal{S}'$ and therefore, for all $h \in \Gamma \setminus \{0\}$ the equation

$$h = 2x - y \tag{4.2}$$

with $x, y \in \mathcal{S}'$ always has a unique solution. The above implies that every vertex in $V_1' \setminus \{0\}$ is adjacent to exactly one absolute vertex; indeed, if there is a vertex $w \neq 0$ adjacent to two distinct absolute vertices u_1 and u_2, then $w + u_1 = a$, $w + u_2 = b$, $2u_1 = c$ and $2u_2 = d$ for some $a, b, c, d \in \mathcal{S}'$. Thus,

$$\begin{aligned} 2a - c &= 2a - 2u_1 \\ &= 2w \\ &= 2b - 2u_2 \\ &= 2b - d \end{aligned}$$

which contradicts that Equation (4.2) has a unique solution. Note that the vertex $v = 0$ is adjacent to all absolute vertices. Moreover, the subgraph of $G_{\Gamma,\mathcal{S}'}$ induced by the set $V_1' \setminus \{0\}$ is regular of degree q. On the other hand, $|V_1'| = q^2$ because Equation (4.2) has $q+1$ solutions when $h = 0$, then there are $q^2 = q^2+q+1-(q+1)$ elements in Γ that are adjacent to at least one absolute vertex. Finally, $|V_1| = |V_1'|$ by the isomorphism of graphs.

(iv) Since $|\Gamma| = q^2 + q + 1$, $|\mathcal{S}| = q + 1$ and $|P| = q + 1$, then Proposition 10 implies that, $G_{\Gamma,\mathcal{S}} = (V, E)$ is C_4-free and also

$$|E| = \frac{1}{2}[(q^2 + q + 1)(q + 1) - (q + 1)] = \frac{1}{2}(q + 1)(q^2 + q) = \frac{1}{2}q(q + 1)^2,$$

therefore,

$$\frac{1}{2}q(q + 1)^2 \leq ex(q^2 + q + 1, C_4).$$

On the other hand, Füredi [31] proved that

$$ex(q^2 + q + 1, C_4) \leq \frac{1}{2}q(q + 1)^2,$$

for all prime powers $q > 13$.

□

Remark 10. Note that in Theorem 7 we can use First Multiplier Theorem with the prime $p = 2$ because q is even and a Singer type B_2 set is a $(q^2+q+1, q+1, 1)$-difference set, see Chapter 2.

4.2 B_2 sets and subgraphs of ER_q

In [11] the authors proved as their main result that the sum graph of a Bose type B_2 set is an induced subgraph of ER_q. In the same direction, Peng et al. [36] proved that the sum graph of the Erdös-Turán type B_2 set $\mathcal{C} = \{(x, x^2) : x \in \mathbb{F}_q\}$ is isomorphic to an induced subgraph of ER_q. In Theorem 10, we prove that the sum graph of a Ruzsa type B_2 set is isomorphic to an induced subgraph of ER_q.

Theorem 8. Let $\mathcal{B}$ be a Bose type B_2 set in $\Gamma = \mathbb{Z}_{q^2-1}$. Then the sum graph $G_{\Gamma,\mathcal{B}}$ is isomorphic to an induced subgraph of the Erdös-Rényi graph ER_q.

Proof. See [[11], Thm.1.2]. □

Theorem 9. Let $\mathcal{C}$ be a Erdös-Turán type B_2 set in $\Gamma = \mathbb{F}_q \times \mathbb{F}_q$. Then the sum graph $G_{\Gamma,\mathcal{C}}$ is isomorphic to an induced subgraph of the Erdös-Rényi graph ER_q.

Proof. See [[36], Thm.1.5]. □

To prove Theorem 8 and Theorem 9, the authors add vertices and some edges to the sum graph of the B_2 set to obtain a graph H, that is C_4-free, has q^2+q+1 vertices, and has $\frac{1}{2}q(q+1)^2$ edges. Then, they give an isomorphism between H and ER_q. It is very likely that Theorem 10 below can be proved by following this method. However, we give a direct proof of this result.

Before presenting our main result of this chapter, we show with an example the method used in Theorem 8.

Example 11. $\mathcal{B} = \{1, 6, 7\}$ is a B_2 set of type Bose-Chowla in $\Gamma = \mathbb{Z}_8$. Figure 4.1 shows the sum graph of the set $\mathcal{B}$.

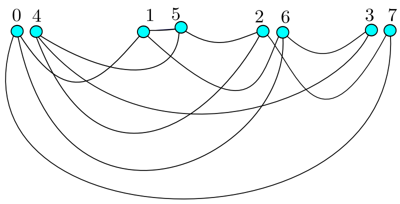


Figure 4.1: $G_{\Gamma,\mathcal{B}}$

Figures 4.2, 4.3, 4.4, 4.5 and 4.6 illustrate the method used in Theorem 8, and Figure 4.7 show ER_3^*. The explicit isomorphism between H and ER_3^* can be deduced from Figures 4.6 and 4.7.

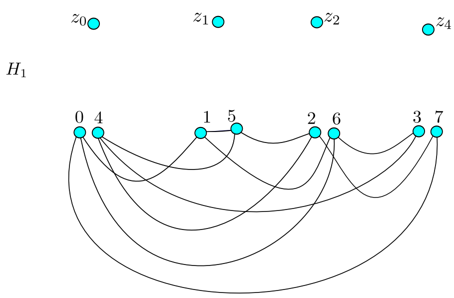


Figure 4.2: A graph H_1 is obtained by adding four new vertices to $G_{\Gamma,\mathcal{B}}$

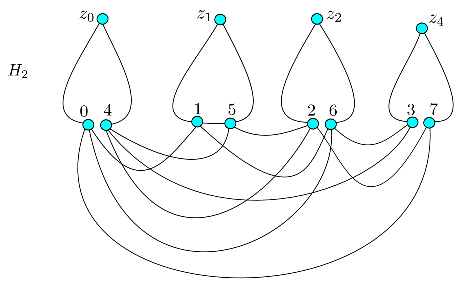


Figure 4.3: A graph H_2 is obtained by adding eight new edges to H_1

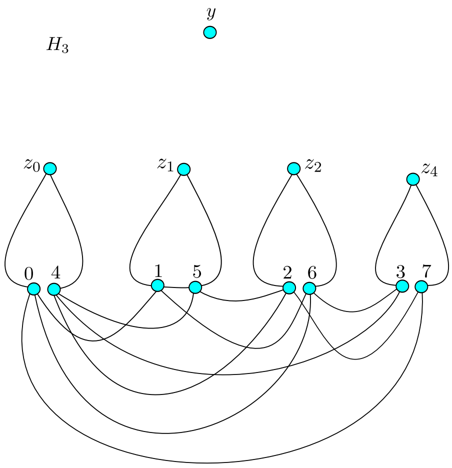


Figure 4.4: A graph H_3 is obtained by adding the vertex y to H_2

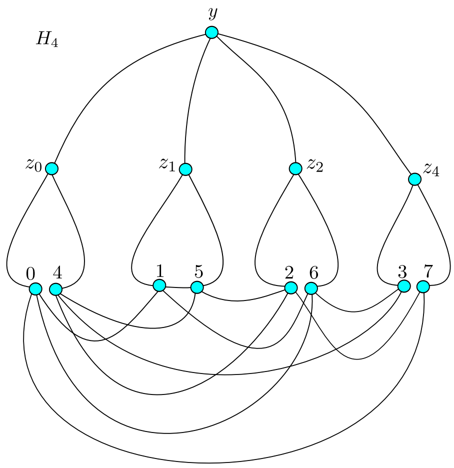


Figure 4.5: A graph H_4 is obtained by adding four new edges to H_3

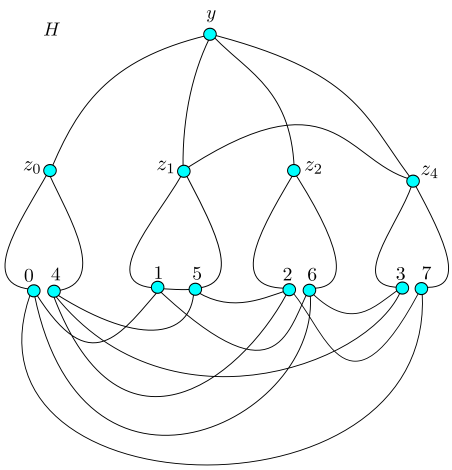


Figure 4.6: A graph H is obtained by adding the edge z_1z_4 to H_4

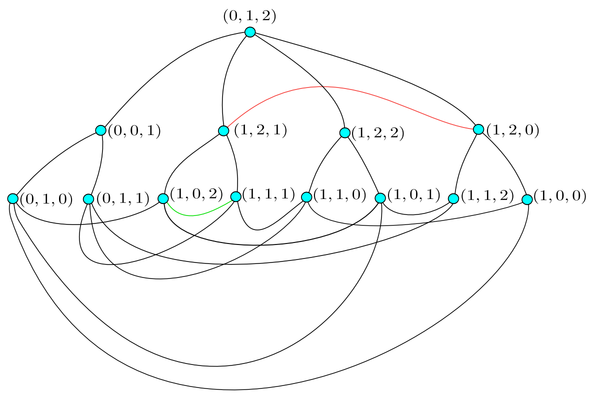


Figure 4.7: ER_3^*

Theorem 10. Let $\mathcal{R}$ be a Ruzsa type B_2 set in $\Gamma = \mathbb{Z}_{p^2-p}$. Then the sum graph $G_{\Gamma,\mathcal{R}}$ is isomorphic to an induced subgraph of the Erdös-Rényi graph ER_p.

Proof. Let $S = \{(1, x_1, x_2) \in V(ER_p^*) : x_1 \neq 0\}$. Note that $|S| = p^2 - p = |V(G_{\Gamma,\mathcal{R}})|$. The statement is that the subgraph H of ER_p^* induced by S is isomorphic to $G_{\Gamma,\mathcal{R}}$. Indeed, let θ be a primitive root modulo p, and consider $\phi : V(H) \longrightarrow V(G_{\Gamma,\mathcal{R}})$ be defined by

$$\phi(1, x_1, x_2) = ((\log_\theta x_1)p - x_2(p-1))(\bmod p^2 - p),$$

where $\log_\theta$ is the isomorphism between $\mathbb{Z}_p^*$ and $\mathbb{Z}_{p-1}$ defined by the discrete logarithm to base θ.

Let $\mathbf{x} = (1, x_1, x_2)$ and $\mathbf{y} = (1, y_1, y_2)$ be two vertices in H. If $\phi(\mathbf{x}) = \phi(\mathbf{y})$, then

$$((\log_\theta x_1)p - x_2(p-1)) \equiv ((\log_\theta y_1)p - y_2(p-1))(\bmod p^2 - p),$$

so $\log_\theta x_1 \equiv \log_\theta y_1 (\bmod p-1)$ and $-x_2(p-1) \equiv -y_2(p-1)(\bmod p)$, therefore $x_1 \equiv y_1(\bmod p-1)$ and $x_2 \equiv y_2(\bmod p)$. Thus, ϕ is injective.

Now, by Equation (A.12), $\mathbf{x}$ and $\mathbf{y}$ are adjacent in ER_p^* if and only if

$$0 = y_2 - x_1 y_1 + x_2.$$

This is, $\mathbf{x}$ is adjacent to $\mathbf{y}$ if and only if $\log_\theta(x_2 + y_2) = \log_\theta x_1 + \log_\theta y_1$.

On the other hand,

$$\begin{aligned} \phi(\mathbf{x}) &= ((\log_\theta x_1)p - x_2(p-1))(\bmod p^2 - p) \quad \text{and} \\ \phi(\mathbf{y}) &= ((\log_\theta y_1)p - y_2(p-1))(\bmod p^2 - p) \end{aligned}$$

are adjacent in $G_{\Gamma,\mathcal{R}}$ if and only if

$$((\log_\theta x_1)p - x_2(p-1) + (\log_\theta y_1)p - y_2(p-1))(\bmod p^2 - p) \quad \in \quad \mathcal{R}.$$

Then, $\phi(\mathbf{x})$ is adjacent to $\phi(\mathbf{y})$ if and only if

$$((\log_\theta x_1 + \log_\theta y_1)p - (x_2 + y_2)(p-1))(\bmod p^2 - p) \in \mathcal{R}.$$

The latter occurs if and only if $\log_\theta(x_2 + y_2) = \log_\theta x_1 + \log_\theta y_1$.

We have proved that $\mathbf{x}$ is adjacent to $\mathbf{y}$ in ER_p^* if and only if $\phi(\mathbf{x})$ is adjacent to $\phi(\mathbf{y})$ in $G_{\Gamma,\mathcal{R}}$. Thus, ϕ is an isomorphism from H to $G_{\Gamma,\mathcal{R}}$ and so $G_{\Gamma,\mathcal{R}}$ is isomorphic to an induced subgraph of ER_p^*. Finally, the result follows from the fact that ER_p^* is isomorphic to ER_p by Theorem 14 (i). □

Example 12. Let $p = 5$. In this case, $S = \{(0,0,1), (1,1,0), (1,1,1), (1,1,2), (1,1,3), (1,1,4), (1,2,0), (1,2,1), (1,2,2), (1,2,3), (1,2,4), (1,3,0), (1,3,1), (1,3,2), (1,3,3), (1,3,4), (1,4,0), (1,4,1), (1,4,2), (1,4,3), (1,4,4)\}$, and $\mathcal{R} = \{3, 14, 16, 17\}$ is a Ruzsa type B_2 set in $\Gamma = \mathbb{Z}_{20}$. Figure 4.8 highlights the subgraph H induced by S within the ER_5 graph, Figure 4.9 shows the H graph, and Figure 4.10 shows the $G_{\Gamma,\mathcal{R}}$ graph. The explicit isomorphism between H and $G_{\Gamma,\mathcal{R}}$ can be deduced from Figures 4.9 and 4.10.

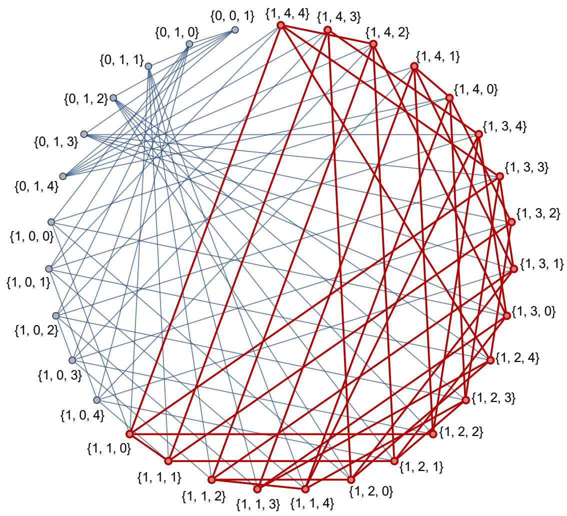


Figure 4.8: H graph within the ER_5 graph

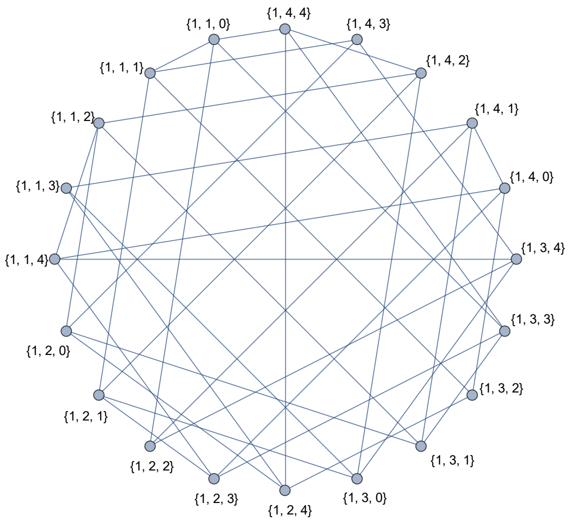


Figure 4.9: H graph

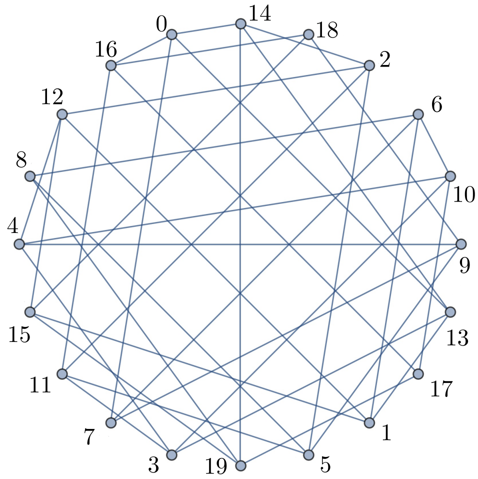


Figure 4.10: $G_{\Gamma,\mathcal{R}}$

Chapter 5

Conclusion And Future Work

5.1 Problem 1

In Chapter 2, we investigate the existence of abelian planar difference sets in groups of order p^m. In Theorem 3 we show the non-existence of these sets if p is prime and $m \geq 2$ is an integer. When $m = 1$ and $p = q^2 + q + 1$ with q prime power, Singer's construction guarantees the existence of an abelian planar difference set with parameters $(q^2 + q + 1, q + 1, 1)$. In this regard, we propose the following conjecture.

Conjecture 1. There are no difference sets with parameters $(p, k, 1)$ for all primes $p = t^2 + t + 1$ with t not a prime power.

5.2 Problem 2

In Chapter 3, we prove that

1. For every prime power $q \equiv 1 \bmod 3$, there exists a $(N/3, q, 2, 2(q-1))$ almost difference set in $\mathbb{Z}_{N/3}$, where $N = q^2 + q + 1$.

2. There exists a $(q^2 + q + 1, q + 2, 1, (q-2)(q+1))$ almost difference set in $\mathbb{Z}_{q^2+q+1}$, for all prime power q.

3. There exists a $(q^2 + q + 1, q + 1 - i, 0, 2(iq - \binom{i}{2}))$ almost difference in $\mathbb{Z}_{q^2+q+1}$, for all prime powers q, and for all $1 \leq i < q$.

Additionally, we construct 2-adesigns from these almost difference sets. At this point we consider it interesting to approach the following problems:

1. To study the structure, properties, and applications of the almost difference sets constructed in Chapter 3.

2. Let $\mathbb{Z}_v$ be the residue class ring module v and t be a divisor of v. Moreover, let S be a difference set in $\mathbb{Z}_v$, $\varphi : \mathbb{Z}_v \to \mathbb{Z}_{\frac{v}{t}}$ be the homomorphism defined by

$$\varphi(a) \equiv a \bmod \left(\frac{v}{t}\right),$$

and $D = \varphi(S)$. For which values of t do the set D form an almost difference set?

3. Is there some infinite family of almost difference sets with parameters $(n, k, 2, t)$, and different from Theorem 4? Is there some infinite family of almost difference sets with parameters $(n, k, 1, t)$?

5.3 Problem 3

The sets B_2 can be generalized in different ways (see [4, 51, 52, 53]). In [53] Ruiz and Trujillo consider the following generalization: Let g and h denote positive integers with $h \geq 2$. Let Γ be an additive group. The set $A = \{a_1, \ldots, a_k\} \subseteq \Gamma$ is a $B_h[g]$ set on Γ if every element of Γ can be written in at most g ways as sum of h elements in A, that is, if given $x \in \Gamma$, the solutions of the equation $x = a_1 + \cdots + a_h$, with $a_1, \ldots, a_h \in A$, are at most g (up to rearrangement of summands) and they present constructions of $B_h[g]$ sets on the abelian groups $(\mathbb{F}^h, +)$, $(\mathbb{Z}_d, +)$, and $(\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_d}, +)$, for $d \geq 2$, $h \geq 2$, $g \geq 1$. In this direction, we propose to study the sum graph of a $B_h[g]$ set and its properties.

5.4 Problem 4

In Chapter 4 we prove that the sum graph of a Ruzsa type B_2 set is isomorphic to an induced subgraph of ER_p. Another interesting problem is to obtain an analogous result for a B_2 set of type Hughes (see Appendix A.3.3).

Appendix A

Preliminaries

A.1 Finite Field

A *field* is a set $\mathbb{F}$ on which two binary operations, called addition and multiplication, are defined and which contains two distinguished elements 0 and 1, with $0 \neq 1$, such that $\mathbb{F}$ is an abelian group with respect to addition having 0 as the identity element, and the elements of $\mathbb{F}$ that are differente of 0 form an abelian group with respect to multiplication having 1 as the identity element. The element 0 is called the zero element and 1 is called the identity.

For a prime p, let $\mathbb{F}_p$ be the set $\{0, 1, \ldots, p-1\}$ of integers and let $\varphi : \mathbb{Z}_p \to \mathbb{F}_p$ be the mapping defined by $\varphi([a]) = a$ for $a = 0, 1, \ldots, p-1$. Then, $\mathbb{F}_p$ endowed with the field structure induced by φ, is a finite field (that is, $\mathbb{F}_p$ contain only finitely many elements), called the Galois field of order p. The finite field $\mathbb{F}_p$ has zero element 0, identity 1, and its structure is exactly the structure of $\mathbb{Z}_p$. Computing with elements of $\mathbb{F}_p$ therefore means ordinary arithmetic of integers with reduction modulo p.

Theorem 11 (Galois)**.** A Finite Field has q elements, where q is the power of a prime. The Field of order q is unique up to isomorphisms.

We denote the finite field of order q as $\mathbb{F}_q$, although it is also denoted $GF(q)$ by many. A finite field has prime characteristic p, this is, the additive order of every nonzero element b is p; i.e, $pb = 0$, and p is the least positive integer for which this holds. We will need the following properties and definitions relating to finite fields. The details of the following facts can be found in Lidl and Niederreiter [54].

(i) The finite field $\mathbb{F}_q$ can be constructed in the following way. Let $f \in \mathbb{F}_q$ be a polynomial of degree h, irreducible over $\mathbb{F}_q$. The quotient ring $\mathbb{F}_q / < f(x) >$ has p^h elements and with the multiplication and addition defined as in this quotient ring, it is the field $\mathbb{F}_{p^h}$.

(ii) For every finite field $\mathbb{F}_q$, the multiplicative group $\mathbb{F}_q^*$ of nonzero elements of $\mathbb{F}_q$ is cyclic. A generator of the cyclic group $\mathbb{F}_q^*$ is called a *primitive element* of $\mathbb{F}_q$.

(iii) $\mathbb{F}_{p^r}$ is a subfield of $\mathbb{F}_{p^h}$ if and only if r divides h.

(iv) $\mathbb{F}_{p^h}$ is a vector space of rank h over $\mathbb{F}_p$.

(v) Let $\mathbb{F}_q$ be a subfield of $\mathbb{F}_r$ and $\theta \in \mathbb{F}_r$. If θ satisfies a nontrivial polynomial equation with coefficients in $\mathbb{F}_q$, that is, if $a_n\theta^n + \cdots + a_1\theta + a_0 = 0$ with $a_i \in \mathbb{F}_q$ not all being 0, then θ is said to be *algebraic* over $\mathbb{F}_q$. An extension $\mathbb{F}_r$ of $\mathbb{F}_q$ is called *algebraic* over $\mathbb{F}_q$ (or an *algebraic extension* of $\mathbb{F}_q$) if every element of $\mathbb{F}_r$ is algebraic over $\mathbb{F}_q$.

(vi) If $\theta \in \mathbb{F}_r$ is algebraic over $\mathbb{F}_q$, then the uniquely determined monic polynomial $g \in \mathbb{F}_q[x]$ generating the ideal $J = \{f \in \mathbb{F}_q[x] : f(\theta) = 0\}$ of $\mathbb{F}_q[x]$ is called the *minimal polynomial* of θ over $\mathbb{F}_q$. By the degree of θ over $\mathbb{F}_q$ we mean the degree of g.

(vi) Let $\mathbb{F}_q$ be a finite field and $\mathbb{F}_r$ a finite field extension. Then $\mathbb{F}_r$ is a simple algebraic extension of $\mathbb{F}_q$ and every primitive element of $\mathbb{F}_r$ can serve as a defining element of $\mathbb{F}_r$ over $\mathbb{F}_q$.

A.2 Additive Number Theory

In this chapter we present the notation that we will use throughout this thesis. Moreover, we present some previous results that we will use in later chapters.

Let Γ be a group written additively. If A and B are subsets of Γ. Then,

- *Sum set of A and B*

$$A + B := \{a + b : a \in A, b \in B\}.$$

- *Restricted sum set of A and B*

$$A \oplus B := \{a + b : a \in A, b \in B, a \neq b\}.$$

- *Difference set of A and B*

$$A - B := \{a - b : a \in A, b \in B\}.$$

- *Restricted Difference set of A and B*

$$A \ominus B := \{a - b : a \in A, b \in B, a \neq b\}.$$

We use $|A|$ to denote the cardinal of a finite set A and $\binom{m}{n}$ to denote the combinatorial number that counts the number of subsets of size n taken from a set with m elements, for $m \geq n$.

An additive group is any abelian group written additively.

Definition 1. Let Γ be an additive group and D be a subset of Γ. The *difference function* denoted by δ_D, has domain Γ, codomain the nonnegative integers, and is denifed by:

$$\begin{aligned} \delta_D(x) &= |\{(d_i, d_j) \in D \times D : d_i - d_j = x\}|, \\ &= |(D + x) \cap D|. \end{aligned}$$

The difference function counts the number of representations of x in the form $d_i - d_j$ with $d_i, d_j \in D$.

A k-subset D in an additive group Γ of order v is called a (v, k, λ) *difference set* DS (in Γ) if $\delta_D(x) = \lambda$ for every nonzero element of Γ, where $\delta_D(x)$ is the difference function of Definition 1. The order of the difference set D is defined as $n = k - \lambda$. Moreover, if Γ is abelian and $\lambda = 1$ then D is called an abelian planar difference set.

The concept of the multiplier was established by Hall in 1947, while he was studying difference sets in cyclic groups. In 1955, Bruck generalized the concept to an arbitrary group.

Definition 2. Let D be a (v, k, λ) difference set in an additive group Γ. An automorphism α of Γ is a multiplier of D, if $\alpha(D) = D + g$ for some $g \in G$.

A multiplier α fixes the difference set D, if $\alpha(D) = D$.

Theorem 12 guarantees under certain conditions, the existence of a multiplier of a difference set. The first result of this nature is due to Hall (1947). His result and proof were generalized by Chowla and Ryser (1950). Years later, Lander presented a much more transparent proof of this result (1980). This was further simplified by Pott (1988), see [42].

Theorem 12 (First Multiplier Theorem (FMT))**.** Let D be a (v, k, λ, n)-difference set of an abelian group Γ (written multiplicatively), and p be a prime that divides n but does not divide v. If $p > \lambda$, then $\alpha : \Gamma \to \Gamma$ defined by $\alpha(x) = x^p$ is a *multiplier* of D.

A.3 B_2 set

Let Γ be an additive group, a non-empty subset $A \subset \Gamma$ is a B_2 *set (or Sidon set)* in Γ if

$$a + b = c + d \text{ implies that } \{a, b\} = \{c, d\}$$

for all $a, b, c, d \in A$.

Lemma 4 is a direct consequence of the definition of a B_2 set and we will use it to embed B_2 sets in a cyclic group to the modular integers.

Lemma 4. Let $(\Gamma_1, +)$ and $(\Gamma_2, *)$ be abelian groups and $\varphi : \Gamma_1 \longrightarrow \Gamma_2$ be an injective homomorphism. If A is a B_2 set in Γ_1, then $\varphi(A)$ is a B_2 set in Γ_2.

Since $a + b = c + d$ implies that $a - d = c - b$, a subset $A \subset \Gamma$ is a B_2 set if all non-zero differences of elements of A are different. A set having distinct differences between any two elements is called Ruler Golomb, this is, B_2 sets and Golomb rulers have equivalent definitions, see for example [4]. If Γ is finite, by counting the number of differences $a - b$, we can see that $|A| < \sqrt{|\Gamma|} + 1/2$. The most interesting B_2 sets are those with large cardinality, that is, $|A| = \sqrt{|\Gamma|} - \delta$ where δ is a small number. The best-known constructions of B_2 sets with large cardinality are due to Singer [12], Erdös-Turán [55] (see also Cilleruelo [8], Example 3), Hughes [56], Bose [57], Ganley [58], and Ruzsa [59]. For more on B_2 sets, we recommend O'Bryant's survey [60].

A.3.1 Singer's Construction.

The proof of Proposition 4, 7, and 9 can be consulted in [61], we present it to make the section self-contained.

Proposition 4. Let θ be a primitive element of $\mathbb{F}_{q^3}$, $\alpha \in \mathbb{F}_{q^3}$ be an element with cubic minimal polynomial over $\mathbb{F}_q$, $\{\overline{\alpha + u} : u \in \mathbb{F}_q\} \cup \{\overline{1}\} \subseteq \mathbb{F}^*_{q^3}/\mathbb{F}^*_q$ be the set consisting of the equivalence classes modulo $\mathbb{F}^*_q$, and $\log_\theta$ be the isomorphism between $\mathbb{F}^*_{q^3}/\mathbb{F}^*_q$ and $\mathbb{Z}_{q^2+q+1}$ defined by the discrete logarithm to base θ . Then

$$\mathcal{S} := \{\log_\theta(\overline{\alpha + u}) : u \in \mathbb{F}_q\} \cup \{\log_\theta(\overline{1})\},$$

is a B_2 set in $\mathbb{Z}_{q^2+q+1}$ with $q+1$ elements.

Proof. Note that $\mathbb{F}_q^*$ is a subgroup of the group $\mathbb{F}_{q^3}^*$, and that the quotient group $\mathbb{F}_{q^3}^*/\mathbb{F}_q^*$ is cyclic of order $(q^3-1)/(q-1) = q^2+q+1$. Next, we will show that the equivalence classes modulo $\mathbb{F}_q^*$

$$\{\overline{\alpha + u} : u \in \mathbb{F}_q\} \cup \{\overline{1}\},$$

form a B_2 set in $\mathbb{F}_{q^3}^*/\mathbb{F}_q^*$.

Suppose that

$$1^{2-r} \prod_{k=1}^{r} (\alpha + a_{i_k}) \equiv 1^{2-r} \prod_{k=1}^{s} (\alpha + a_{j_k}) \pmod{\mathbb{F}_q^*},$$

with

$$1 \le i_1 \le i_r \le q, \qquad 1 \le j_1 \le j_s \le q,$$
$$r, s \le 2.$$

Then, for some $b \in \mathbb{F}_q^*$,

$$\prod_{k=1}^{r} (\alpha + a_{i_k}) \equiv b \prod_{k=1}^{s} (\alpha + a_{j_k}),$$

with

$$1 \le i_1 \le i_r \le q, \qquad 1 \le j_1 \le j_s \le q,$$
$$r, s \le 2.$$

and therefore, α is a root of the polynomial of degree less than or equal to 2

$$P(X) = b \prod_{k=1}^{s} (X + a_{j_k}) - \prod_{k=1}^{r} (X + a_{i_k}) \in \mathbb{F}_q[X],$$

which is only possible if $P(X) = 0$. Thus, $r = s, b = 1$ and

$$\{a_{i_k}\} = \{a_{j_k}\}.$$

Now, by Lemma 4

$$\mathcal{S} := \{\log_\theta(\overline{\alpha + u}) : u \in \mathbb{F}_q\} \cup \{\log_\theta(\overline{1})\}$$

is a B_2 set in $\mathbb{Z}_{q^2+q+1}$.

Finally, $|\mathcal{S}| = q+1$, because $|\{\overline{\alpha + u} : u \in \mathbb{F}_q\} \cup \{\overline{1}\}| = q+1$ and the discrete logarithm is injective. □

Example 13. Let $q = 5$. If θ is a root of the primitive polynomial $x^3 + 3x + 3$ over $\mathbb{F}_5$ and $\alpha = \theta$. Then, the equivalence classes modulo $\mathbb{F}_5^*$

$$\begin{aligned}
\overline{\theta + 0} &= \{\theta, 2\theta, 3\theta, 4\theta\};\\
\overline{\theta + 1} &= \{\theta + 1, 2\theta + 2, 3\theta + 3, 4\theta + 4\};\\
\overline{\theta + 2} &= \{3\theta + 1, \theta + 2, 4\theta + 3, 2\theta + 4\};\\
\overline{\theta + 3} &= \{2\theta + 1, 4\theta + 2, \theta + 3, 3\theta + 4\};\\
\overline{\theta + 4} &= \{4\theta + 1, 3\theta + 2, 2\theta + 3, \theta + 4\};\\
\overline{1} &= \{1, 2, 3, 4\}.
\end{aligned}$$

form a B_2 set in $\mathbb{F}_{125}^*/\mathbb{F}_5^*$.

Since

$$\theta^1 = \theta + 0, \theta^3 = 2\theta + 2, \theta^{10} = 2\theta + 3, \theta^{14} = 4\theta + 3, \theta^{26} = 2\theta + 1, \theta^0 = 1,$$

and $\log_\theta : \mathbb{F}_{125}^*/\mathbb{F}_5^* \longrightarrow \mathbb{Z}_{31}$ is the isomorphism defined by the discrete logarithm to base θ, then by Lemma 4,

$$\begin{aligned}
\mathcal{S} &= \{\log_\theta(\overline{\theta + u}) : u \in \mathbb{F}_5\} \cup \{\log_\theta(\overline{1})\}\\
&= \{1, 3, 10, 14, 26\} \cup \{0\}
\end{aligned}$$

is a B_2 set in $\mathbb{Z}_{31}$.

Remark 11. A reformulation of Singer's construction that we will use in some situations is as follows: Let θ be a primitive element of $\mathbb{F}_{q^3}$, $\alpha \in \mathbb{F}_{q^3}$ be an element with cubic minimal polynomial over $\mathbb{F}_q$, $\log_\theta : \mathbb{F}_{q^3}^* \longrightarrow \mathbb{Z}_{q^3-1}$ be the isomorphism defined by the discrete logarithm to base θ, and $A := \{\log_\theta(\alpha + u) : u \in \mathbb{F}_q\}$. The set

$$\mathcal{S} = A \pmod{q^2 + q + 1} \cup \{0\},$$

is a Singer type B_2 set in $\mathbb{Z}_{q^2+q+1}$, with $q + 1$ elements.

Lemma 5. If $\mathcal{S}$ is a Singer type B_2 set, then

(i) $0 \in \mathcal{S}$,

(ii) $\mathcal{S} \ominus \mathcal{S} = \mathbb{Z}_{q^2+q+1} \setminus \{0\}$,

Proof.

1. It follows from the construction.

2. Since $\mathcal{S} \ominus \mathcal{S} \subseteq \mathbb{Z}_{q^2+q+1}$, $0 \notin \mathcal{S} \ominus \mathcal{S}$ and $|\mathcal{S} \ominus \mathcal{S}| = (q+1)q = q^2 + q$ (because $\mathcal{S}$ is a B_2 set), then
$$\mathcal{S} \ominus \mathcal{S} = \mathbb{Z}_{q^2+q+1} \setminus \{0\}.$$

□

Example 14. Let $q = 7$. If θ is a root of the primitive polynomial $x^3 + 4x^2 + 4x + 4$ over $\mathbb{F}_7$ and $\alpha = \theta$. Then

$$\begin{aligned} B = \{\theta + u : u \in \mathbb{F}_q\} &= \{\theta, \theta+1, \theta+2, \theta+3, \theta+4, \theta+5, \theta+6\}, \\ &= \{\theta^1, \theta^{274}, \theta^{199}, \theta^{225}, \theta^{329}, \theta^{63}, \theta^{78}\}. \end{aligned}$$

Taking the discrete logarithm of B in base θ yields the set

$$\begin{aligned} A = \log_\theta B &= \{\log_\theta(\theta + u) : u \in \mathbb{F}_q\}, \\ &= \{1, 274, 199, 225, 329, 63, 78\}. \end{aligned}$$

Reducing the elements of A modulo 57 gives the set

$$\{1, 46, 28, 54, 44, 6, 21\}.$$

Adding 0 to the above set and ordering its elements yields the Singer type B_2 set in $\mathbb{Z}_{57}$

$$\mathcal{S} = \{0, 1, 6, 21, 28, 44, 46, 54\}.$$

Note that $0 \in \mathcal{S}$ and $\mathcal{S} \ominus \mathcal{S} = \mathbb{Z}_{57} \setminus \{0\}$.

A.3.2 Erdös-Turán's Construction

The proof of Proposition 5, 6, and 8 can be consulted in [62], we present it to make the section self-contained.

Proposition 5. If q is odd, then

$$\mathcal{C} := \{(a, a^2) : a \in \mathbb{F}_q\}$$

is a B_2 set in $(\mathbb{F}_q, +) \times (\mathbb{F}_q, +)$ with q elements.

Proof. It is clear that $|\mathcal{C}| = q$. We will prove that $\mathcal{C}$ is a B_2 set $(\mathbb{F}_q, +) \times (\mathbb{F}_q, +)$.

Suppose that
$$(a, a^2) + (b, b^2) = (c, c^2) + (d, d^2)$$
with $\{a, a^2\}, \{b, b^2\}, \{c, c^2\}, \{d, d^2\} \in \mathcal{C}$. Then
$$a + b = c + d, \tag{A.1}$$
$$a^2 + b^2 = c^2 + d^2. \tag{A.2}$$
By (A.1),
$$a^2 + 2ab + b^2 = (a + b)^2 = (c + d)^2 = c^2 + 2cd + d^2, \tag{A.3}$$
and by (A.2), (A.3), and the fact that $\mathbb{F}_q$ has characteristic $q \neq 2$,
$$ab = cd. \tag{A.4}$$
Now, (A.1) and (A.4) imply that the polynomial
$$P(X) = X^2 - (a + b)X + ab \in \mathbb{F}_q[x]$$
is factored completely as
$$P(X) = (X - a)(X - b) = (X - c)(X - d).$$
Since $\mathbb{F}_q[x]$ is a unique factorization domain, and the roots of a polynomial are unique,
$$\{a, b\} = \{c, d\},$$
and therefore,
$$\{(a, a^2), (b, b^2)\} = \{(c, c^2), (d, d^2)\}.$$
□

Lemma 6. $\mathcal{C} \ominus \mathcal{C} = (\mathbb{F}_q \times \mathbb{F}_q) \backslash \{(0, a) : a \in \mathbb{F}_q\}$.

Proof. Suppose that $\mathcal{C} \ominus \mathcal{C} = (\mathbb{F}_q \times \mathbb{F}_q) \backslash A$ and consider the set $B = \{(0, z) : z \in \mathbb{F}_q\}$. Then $B \subseteq A$ because of $(\mathcal{C} \ominus \mathcal{C}) \cap B = \emptyset$. Now, $|\mathcal{C} \ominus \mathcal{C}| = q^2 - q = q^2 - |A|$ and $|B| = q$ implies that $A = B$. □

Example 15. Let $q = 5$. Then,
$$\mathcal{C} = \{(0, 0), (1, 1), (2, 4), (3, 4), (4, 1)\}$$
is a B_2 set in $(\mathbb{F}_5, +) \times (\mathbb{F}_5, +)$ with 5 elements. Moreover,
$$\mathcal{C} \ominus \mathcal{C} = (\mathbb{F}_5 \times \mathbb{F}_5) \backslash \{(0, a) : a \in \mathbb{F}_5\}.$$

The proof of Proposition 6 and 8 is similar to that of Proposition 5, for this reason we omit their proof.

A.3.3 Hughes's Construction.

Proposition 6. If q is odd and α is an element in $\mathbb{F}_q^*$, then

$$\mathcal{I}_\alpha = \{(a-\alpha, a) : a \in \mathbb{F}_q^*, a \neq \alpha\}$$

is a B_2 set in $\mathbb{F}_q^* \times \mathbb{F}_q^*$ with $q-2$ elements.

Lemma 7. If $A_1 = \{(1, z) : z \in \mathbb{F}_q^*\}$, $A_2 = \{(z, 1) : z \in \mathbb{F}_q^*\}$ and $A_3 = \{(z, z) : z \in \mathbb{F}_q^*\}$, then

$$\mathcal{I}_\alpha \ominus \mathcal{I}_\alpha = \mathbb{F}_q^* \times \mathbb{F}_q^* \backslash (A_1 \cup A_2 \cup A_3).$$

Proof. Suppose that $\mathcal{I}_\alpha \ominus \mathcal{I}_\alpha = \mathbb{F}_q^* \times \mathbb{F}_q^* \backslash A$. Then $(1, z),\ (z, 1) \in A$ for all $z \in \mathbb{F}_q*$, since

$$\mathcal{I}_\alpha \ominus \mathcal{I}_\alpha = \{((a-\alpha)(b-\alpha)^{-1}, ab^{-1}) : a, b, \alpha \in \mathbb{F}_q^*, a \neq b,\ b \neq \alpha \text{ and } \alpha \neq a\}.$$

Now suppose that there exists $z \in \mathbb{F}_q^*$ such that $(z, z) \in \mathcal{I}_\alpha \ominus \mathcal{I}_\alpha$. Then, $z = (a-\alpha)(b-\alpha)^{-1} = ab^{-1}$ for some $a, b \in \mathbb{F}_q^*$. Hence,

$$\begin{aligned} a - \alpha &= ab^{-1}(b-\alpha) \\ &= a - ab^{-1}\alpha \end{aligned}$$

and so $(ab^{-1} - 1)\alpha = 0$, which is not possible. Therefore, $A_1 \cup A_2 \cup A_3 \subseteq A$. Finally,

$$|\mathcal{I}_\alpha \ominus \mathcal{I}_\alpha| = 2\binom{q-2}{2} = q^2 - 5q + 6 = q^2 - 2q + 1 - |A|$$

and $|A_1 \cup A_2 \cup A_3| = 3q - 5$ implies that $A_1 \cup A_2 \cup A_3 = A$. □

Example 16. Let $q = 7$ and $\alpha = 1$. Then

$$I_1 = \{(2, 1), (3, 2), (4, 3), (5, 4), (6, 5), (7, 6)\}$$

is a B_2 set in $\mathbb{F}_7^* \times \mathbb{F}_7^*$ with 5 elements. Moreover,

$$\mathcal{I}_1 \ominus \mathcal{I}_1 = \mathbb{F}_7^* \times \mathbb{F}_7^* \backslash (A_1 \cup A_2 \cup A_3).$$

where

$$\begin{aligned} A_1 &= \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6)\}, \\ A_2 &= \{(1, 1), (2, 1), (3, 1), (4, 1), (5, 1), (6, 1)\}, \\ A_3 &= \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6)\}. \end{aligned}$$

A.3.4 Bose's Construction.

Proposition 7. If $\alpha \in \mathbb{F}_{q^2}$ is an algebraic element of degree 2 over $\mathbb{F}_q$, θ is a primitive element of $\mathbb{F}_{q^2}$, and $\log_\theta$ is the isomorphism between $\mathbb{F}^*_{q^2}$ and $\mathbb{Z}_{q^2-1}$ defined by the discrete logarithm to base θ, then

$$\mathcal{B} := \log_\theta(\alpha + \mathbb{F}_q) = \{\log_\theta(\alpha + a) : a \in \mathbb{F}_q\}$$

is a B_2 set in $(\mathbb{Z}_{q^2-1}, +)$ with q elements.

Proof. We will prove that the set

$$\alpha + \mathbb{F}_q = \{\alpha + a : a \in \mathbb{F}_q\},$$

is a B_2 set in the group $(\mathbb{F}^*_{q^2}, \cdot)$.

Suppose the opposite, this is,

$$(\alpha + a_1)(\alpha + a_2) = (\alpha + a_3)(\alpha + a_4),$$

where $\{a_1, a_2\} \neq \{a_3, a_4\}$.

Then, α is a root of the non-zero polynomial of degree less than 2,

$$P(X) = (X - a_1)(X - a_2) - (X - a_3)(X - a_4) \in \mathbb{F}_q[X],$$

which is not possible because α has degree 2 over $\mathbb{F}_q$.

Now, by Lemma 4

$$\mathcal{B} := \log_\theta(\alpha + \mathbb{F}_q) = \{\log_\theta(\alpha + a) : a \in \mathbb{F}_q\}$$

is a B_2 set in $(\mathbb{Z}_{q^2-1}, +)$.

Finally, $|\mathcal{B}| = q$, because $|A(\alpha)| = |\alpha + \mathbb{F}_q| = q$ and the discrete logarithm is injective. $\square$

Lemma 8. If $\mathcal{B}$ is a Bose type B_2 set in $\mathbb{Z}_{q^2-1}$ and $M_{q+1} := \{x \in \mathbb{Z}_{q^2-1} : x \equiv 0 \pmod{q+1}\}$, then

(i) $\mathcal{B} \cap M_{q+1} = \emptyset$.

(ii) $(\mathcal{B} \ominus \mathcal{B}) \cap M_{q+1} = \emptyset$.

(iii) $\mathcal{B} \pmod{q+1} = \{a \pmod{q+1} : a \in \mathcal{B}\} = [1, q]$.

(iv) $\mathcal{B} \ominus \mathcal{B} = \mathbb{Z}_{q^2-1} \backslash M_{q+1}$.

Proof.

(i) Suppose that $\mathcal{B} \cap M_{q+1} \neq \emptyset$, then there are $a \in \mathcal{B}$ and $t \in \mathbb{Z}$ such that $a = t(q+1)$, so $\theta^a = \theta^{t(q+1)} = c$ for some $c \in \mathbb{F}_q^*$, since $\mathbb{F}_q^* = \langle \theta^{(q+1)} \rangle$. On the other hand, as $a \in \mathcal{B}$, there is $k \in \mathbb{F}_q$ such that $\log_\theta(\alpha + k) = a$, therefore, $\alpha + k = \theta^a = c$ and thus $\alpha \in \mathbb{F}_q$, which is a contradiction.

(ii) Assume that $(\mathcal{B} \ominus \mathcal{B}) \cap M_{q+1} \neq \emptyset$, then there are $a, b \in \mathcal{B}$, $a \neq b$ and $t \in \mathbb{Z}$ such that $a - b = t(q+1)$. Then $\theta^{a-b} = \theta^{t(q+1)}$ and as $\mathbb{F}_q^* = \langle \theta^{q+1} \rangle$ then $\theta^{a-b} = c$ for some $c \in \mathbb{F}_q^*$. On the other hand, there are k_1 and k_2 in $\mathbb{F}_q$ with $k_1 \neq k_2$ such that $a = \log_\theta(\alpha + k_1)$ and $b = \log_\theta(\alpha + k_2)$, because $a, b \in \mathcal{B}$. The above implies that $\theta^a = \alpha + k_1$ and $\theta^b = \alpha + k_2$; therefore $c = \theta^{a-b} = \frac{\alpha + k_1}{\alpha + k_2}$. Since $k_1 \neq k_2$, $c \neq 1$, then $\alpha + k_1 = c(\alpha + k_2)$ and so $(1-c)\alpha = ck_2 - k_1$. Thus, $\alpha = (ck_2 - k_1)(1-c)^{-1} \in \mathbb{F}_q^*$ which is a contradiction.

(iii) It follows from (i) and (ii).

(iv) Note that $|\mathcal{B} \ominus \mathcal{B}| = 2\binom{q}{2} = q(q-1) = q^2 - q$, because $\mathcal{B}$ is a B_2 set and $|\mathcal{B}| = q$. From the above and the fact that $(\mathcal{B} \ominus \mathcal{B}) \cap M_{q+1} = \emptyset$, then $|\mathbb{Z}_{q^2-1}| - |M_{q+1}| = q^2 - 1 - (q-1) = q^2 - q = |\mathcal{B} \ominus \mathcal{B}|$.

□

Example 17. Let $q = 7$. If θ is a root of the primitive polynomial $x^2 + x + 3$ over $\mathbb{F}_7$ and $\alpha = \theta$. Then, the set

$$\begin{aligned} \theta + \mathbb{F}_7 &= \{\theta + a : a \in \mathbb{F}_7\} \\ &= \{\theta + 0, \theta + 1, \theta + 2, \theta + 3, \theta + 4, \theta + 5, \theta + 6\} \\ &= \{\theta^1, \theta^{31}, \theta^{11}, \theta^{26}, \theta^{12}, \theta^{14}, \theta^5\}. \end{aligned}$$

is a B_2 set in the group $(\mathbb{F}_{49}^*, \cdot)$.

Now, since $\log_\theta : \mathbb{F}_{49}^* \longrightarrow \mathbb{Z}_{48}$ is the isomorphism defined by the discrete logarithm to base θ, then by Lemma 4

$$\begin{aligned}\mathcal{B} &:= \log_\theta(\theta + \mathbb{F}_7)\\ &= \{\log_\theta(\theta + a) : a \in \mathbb{F}_7\}\\ &= \{1, 31, 11, 26, 12, 14, 5\}.\end{aligned}$$

is a B_2 set in $(\mathbb{Z}_{48}, +)$.

Example 18. Let $\mathcal{B} = \{1, 5, 11, 12, 14, 26, 31\}$ be the Bose type B_2 set in $\mathbb{Z}_{48}$ constructed in Example 17. It can be verified that

- $|\mathcal{B}| = 7$,
- $M_8 = \{0, 8, 16, 24, 32, 40\}$,
- $\mathcal{B} \cap M_8 = \emptyset$,
- $\mathcal{B} \ominus \mathcal{B} = \{1, 2, 3, 4, 5, 6, 7, 9, 10, 11, 12, 13, 14, 15, 17, 18, 19, 20, 21, 22, 23, 25, 26, 27, 28, 29, 30, 31, 33, 34, 35, 36, 37, 38, 39, 41, 42, 43, 44, 45, 46, 47\}$,
- $(\mathcal{B} \ominus \mathcal{B}) \cap M_8 = \emptyset$,
- $\mathcal{B}(\text{mod} 8) = \{1, 2, 3, 4, 5, 6, 7\}$,
- $\mathcal{B} \ominus \mathcal{B} = \mathbb{Z}_{48} \setminus M_8$.

A.3.5 Ganley's Construction.

Proposition 8. If q is odd, then

$$\mathcal{I} = \{(a, a) : a \in \mathbb{F}_q^*\}$$

is a B_2 set in $\mathbb{F}_q \times \mathbb{F}_q^*$ with $q - 1$ elements.

Lemma 9. If $A_1 = \{(0, z) : z \in \mathbb{F}_q^*\}$ and $A_2 = \{(z, 1) : z \in \mathbb{F}_q^*\}$, then

$$\mathcal{I} \ominus \mathcal{I} = \mathbb{F}_q \times \mathbb{F}_q^* \backslash (A_1 \cup A_2).$$

Proof. Suppose that $\mathcal{I} \ominus \mathcal{I} = \mathbb{F}_q \times \mathbb{F}_q^* \backslash A$. Then,

$$\mathcal{I} \ominus \mathcal{I} = \{(a - b, ab^{-1}) : a, b \in \mathbb{F}_q^*, a \neq b\}$$

implies that $A_1 \subset A$ and $A_2 \subset A$. To conclude the proof, note that $|A| = 2(q-1) = |A_1| + |A_2|$ is a consequence of

$$|\mathcal{I} \ominus \mathcal{I}| = 2\binom{q-1}{2} = q^2 - 3q + 2 = q(q-1) - |A|.$$

Therefore, $A = A_1 \cup A_2$. $\square$

Example 19. Let $q = 5$. Then

$$\mathcal{I} = \{(1,1),(2,2),(3,3),(4,4)\}$$

is a B_2 set in $\mathbb{F}_7 \times \mathbb{F}_7^*$ with 6 elements. Moreover,

$$\mathcal{I} \ominus \mathcal{I} = \mathbb{F}_7 \times \mathbb{F}_7^* \backslash (A_1 \cup A_2),$$

where $A_1 = \{(0,1),(0,2),(0,3),(0,4)\}$ and $A_2 = \{(1,1),(2,1),(3,1),(4,1)\}$.

A.3.6 Ruzsa's Construction.

Proposition 9. If θ is a primitive root modulo a prime p, this is, $\langle\theta\rangle = \mathbb{Z}_p^*$, and $\log_\theta : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_{p-1}$ is the isomorphism defined by the discrete logarithm to base θ, and $\mathbb{Z}_p^*$ is considering as a subset of $\mathbb{Z}_{p^2-p}$, then

$$\mathcal{R} := \{((\log_\theta a)p - a(p-1)) (\mathrm{mod}\, p^2 - p) : a \in \mathbb{Z}_p^*\},$$

is a B_2 set in $\mathbb{Z}_{p^2-p}$ with $p-1$ elements.

Proof. Suppose that in $\mathbb{Z}_{p^2-p}$

$$((\log_\theta a)p - a(p-1)) + ((\log_\theta b)p - b(p-1)) \equiv ((\log_\theta c)p - c(p-1)) + ((\log_\theta d)p - d(p-1)),$$

with $a, b, c, d \in \mathbb{Z}_p^*$. Then,

$$(\log_\theta a + \log_\theta b)p \equiv (\log_\theta c + \log_\theta d)p \pmod{p-1}; \quad \text{(A.5)}$$

$$(-a-b)(p-1) \equiv (-c-d)(p-1) \pmod{p}. \quad \text{(A.6)}$$

Since p and $p-1$ are relatively prime, (A.5) implies that

$$ab \equiv cd \pmod{p}, \quad \text{(A.7)}$$

and (A.6) implies that

$$a + b \equiv c + d \pmod{p}. \quad \text{(A.8)}$$

Now, (A.7) and (A.8) imply that the polynomial

$$P(X) = X^2 - (a+b)X + ab \in \mathbb{Z}_p[x]$$

is factored completely as

$$P(X) = (X-a)(X-b) = (X-c)(X-d).$$

Since $\mathbb{Z}_p[x]$ is a unique factorization domain, and the roots of a polynomial are unique,

$$\{a, b\} = \{c, d\},$$

and therefore,

$$\{((\log_\theta a)p - a(p-1)), ((\log_\theta b)p - b(p-1))\} = \{((\log_\theta c)p - c(p-1)), ((\log_\theta d)p - d(p-1))\}.$$

□

The following lemma is an immediate consequence of the definition of $\mathcal{R}$, see [1] and references therein.

Lemma 10. If $\mathcal{R}$ is a Ruzsa type B_2 set in $\mathbb{Z}_{p^2-p}$ and $M_i := \{x \in \mathbb{Z}_{p^2-p} : x \equiv 0 \bmod i\}$ with $i \in \{p, p-1\}$, then

$$\mathcal{R} \ominus \mathcal{R} := \{a - a' : a, a' \in \mathcal{R}, a \neq a'\} = \mathbb{Z}_{p^2-p} \backslash (M_p \cup M_{p-1}).$$

Proof.

(i). Note that $|M_p| = p-1$, $|M_{p-1}| = p$ and $M_p \cap M_{p-1} = \{0\}$. Then,

$$|M_p \cup M_{p-1}| = |M_p| + |M_{p-1}| - |M_p \cap M_{p-1}| = 2(p-1).$$

On the other hand, $(\mathcal{R} \ominus \mathcal{R}) \cap (M_p \cup M_{p-1}) = \emptyset$ since $(\mathcal{R} \ominus \mathcal{R}) \cap M_i = \emptyset$. Therefore,

$$|\mathcal{R} \ominus \mathcal{R}| = 2\binom{p-1}{2} = p^2 - 3p + 2 = p^2 - p - 2(p-1) = |\mathbb{Z}_{p^2-p} \backslash (M_p \cup M_{p-1})|$$

completes the proof.

□

Example 20. Let $\theta = 7$. Then, the elements of $\mathbb{Z}_7^*$ are represented as:

$$7^0 = 1 \qquad 7^1 = 7 \qquad 7^2 = 4 \qquad 7^3 = 6 \qquad 7^4 = 2 \qquad 7^5 = 3$$

Since $\log_\theta : \mathbb{Z}_7^* \longrightarrow \mathbb{Z}_6$ is the isomorphism defined by the discrete logarithm to base θ, then

$$\begin{array}{ll} ((\log_\theta 1)7 - 1(6))(\text{mod } 42) = 36 & ((\log_\theta 2)7 - 2(6))(\text{mod } 42) = 16 \\ ((\log_\theta 3)7 - 3(6))(\text{mod } 42) = 17 & ((\log_\theta 4)7 - 4(6))(\text{mod } 42) = 32 \\ ((\log_\theta 5)7 - 5(6))(\text{mod } 42) = 19 & ((\log_\theta 6)7 - 6(6))(\text{mod } 42) = 27. \end{array}$$

Thus,

$$\mathcal{R} = \{16, 17, 19, 27, 32, 36\}$$

is a B_2 set in $\mathbb{Z}_{42}$, with 6 elements. Moreover,

$$\mathcal{R} \ominus \mathcal{R} = \mathbb{Z}_{42} \setminus (M_7 \cup M_6),$$

where $M_7 = \{0, 7, 14, 21, 28, 35\}$ and $M_6 = \{0, 6, 12, 18, 24, 30, 36\}$.

A.4 Graph Theory

An *undirected graph* G is an ordered pair of disjoint sets (V, E) such that E is a subset of the set $V \times V$ of unordered pairs of V. The elements of V are called *vertices* and the elements of E *edges*. The graphs studied in this thesis do not have edges with identical ends (loops), nor two different edges joining the same pair of vertices (multiple edges). To refer to a graph we will usually write $G = (V, E)$. The number of vertices of G is called the *order* of G and the number of edges in G is called the *size* of G. If $\{u, v\}$ is an edge, then u and v are *adjacent* or *neighboring* vertices in the graph. Moreover, $\{u, v\}$ is said *incident* with u and v. We will use the notation uv to indicate that u and v are adjacent. The *neighborhood* of a vertex v, denoted by $N(v)$, is the set of all neighbors of v. The *degree* of a vertex v, denoted $deg(v)$, is equal to the cardinality of the neighborhood of v. A graph is called *k-regular* if all its vertices have degree equal to k, where k is some non-negative integer. A graph $H = (V', E')$ is a *subgraph* of the graph $G = (V, E)$, if $V' \subseteq V$ and $E' \subseteq E$. A *walk* of length n is a list of vertices $(v_0, v_1, \ldots, v_n)$ such that $v_i \sim v_{i+1}$ for all integers i, $0 \leq i \leq n - 1$. A *path* is a walk in which all vertices are distinct. An *n-cycle* is a walk in which all vertices are distinct with the exception of $v_0 = v_n$. Frequently, 3-cycles are referred to as triangles, 4-cycles as quadrilaterals, etc. We will also denote an n-cycle by C_n. The *length* of a path $(v_0, v_1, \ldots, v_n)$ or a cycle $(v_0, v_1, \ldots, v_{n-1}, v_0)$ is defined to be $n - 1$.

Two graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are *isomorphic* if there is a bijection (a one-to-one, onto map) φ from V_1 to V_2 such that

$$uv \in E_1 \Longleftrightarrow \varphi(u)\varphi(v) \in E_2.$$

In this case, we call φ an isomorphism from G_1 to G_2 and we write $G_1 \cong G_2$.
The *Turán number* of a graph G, denoted by $ex(n, G)$, is the maximum number of edges in a graph on n vertices not containing G as a subgraph. If a graph G does not contain another graph F as a subgraph, we say that G is *F-free*. A graph G is *F-saturated* if G is F-free and adding any new edge to G creates a copy of F. The graph G in Figure A.1 is C_3-saturated, since it is C_3-free and a copy of C_3 is created by adding the edge kj or il to it. However, the graph H in Figure A.1 is C_3-free but is not C_3-saturated, since we can add to this the edge ij and no copy of C_3 is created.

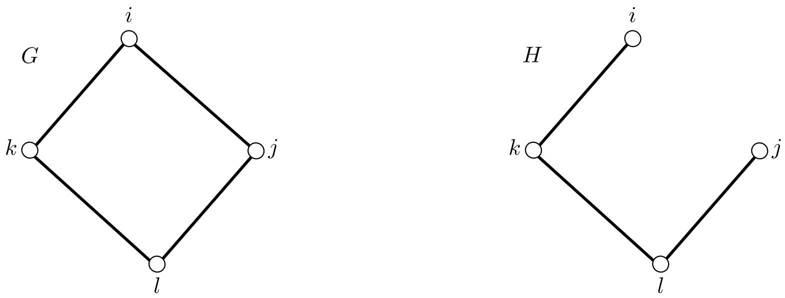


Figure A.1: The graphs G and H.

A.5 Sum graph of a finite B_2 set

Let A be a finite B_2 set of an additive group Γ. An elemenet i in Γ is called absolute vertice if $i + i \in A$. The *sum graph* $G_{\Gamma,A} = (V, E)$ is formed by $V = \Gamma$ and $\{i, j\} \in E$ if and only if $i + j \in A$ with $i \neq j$.

Proposition 10. The sum graph $G_{\Gamma,A} = (V, E)$ is a C_4-free graph and

$$2|E| = |\Gamma||A| - |P|,$$

where $P := \{x \in \Gamma : x + x \in A\}$.

Proof. If (x_0, x_1, x_2, x_3) is a C_4 in $G_{\Gamma,A}$, then

$$x_0 + x_1 = a_1,\ x_1 + x_2 = a_2,\ x_2 + x_3 = a_3 \text{ and } x_3 + x_0 = a_4,$$

where $a_1, a_2, a_3, a_4 \in A$. Hence,

$$(x_0 + x_1) + (x_2 + x_3) = a_1 + a_3 = a_2 + a_4 = (x_1 + x_2) + (x_3 + x_0),$$

and thus $\{a_1, a_3\} = \{a_2, a_4\}$ because A is a B_2 set in Γ. If $a_1 = a_2$ or $a_1 = a_4$ then $x_0 = x_2$ or $x_1 = x_3$, respectively, which is a contradiction.

On the other hand, if x is a vertex in $G_{\Gamma,A}$, then deg(x)=$|A|-1$ if $x \in P$, or deg(x)=$|A|$ in other case. Therefore,

$$2|E| = \sum_{x \in P} \deg(x) + \sum_{x \notin P} \deg(x) = (|A|-1)|P| + |A|(|\Gamma| - |P|) = |A||\Gamma| - |P|.$$

□

A.6 The Erdös-Rényi Orthogonal Polarity Graph: Geometric and Algebraic Interpretation

In this section we present the Erdös-Rényi orthogonal polarity graph and describe its structure from a geometric and algebraic approach.

First of all, we present some geometric concepts since the geometric definition of the Erdös-Rényi orthogonal polarity graph is closely related to them. The first definition is a detailed description of the projective plane $PG(2, q)$ and the second is about polarities of projective planes; we take both definitions from Williford's doctoral thesis [63].

Definition 3. The projective plane $PG(2, q) = (X, L)$ is formed by taking a vector space W of dimension 3 over the finite field $\mathbb{F}_q$, q a prime power, and taking X to be the set of 1-dimensional subspaces of W. As each such subspace contains a unique vector whose leftmost non-zero entry is 1, we will use these vectors to represent these 1-dimensional subspaces. These vectors are called *left-normalized* vectors. Elements of L are maximal sets of one dimensional subspaces which lie together in a two dimensional subspace. As any two dimensional subspace has a one dimensional orthogonal complement, we may also represent elements of L with *left normalized vectors*, though we will use square brackets instead of parentheses to distinguish them. For $\mathbf{x} = (x_0, x_1, x_2) \in X, \mathbf{y} = [y_0, y_1, y_2] \in L$ we then have that $\mathbf{x} \in \mathbf{y}$ if and only if $x_0y_0 + x_1y_1 + x_2y_2 = 0$.

Example 21. $PG(2,2) = (X, L)$

where $X = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7\}$ and $L = \{L_1, L_2, L_3, L_4, L_5, L_6, L_7\}$ with

$$\begin{aligned}
P_1 &= \{(0,0,0),(0,0,1)\} & L_1 &= \{(0,0,0),(0,0,1),(0,1,0),(0,1,1)\}\\
P_2 &= \{(0,0,0),(0,1,0)\} & L_2 &= \{(0,0,0),(1,0,1),(0,0,1),(1,0,0)\}\\
P_3 &= \{(0,0,0),(0,1,1)\} & L_3 &= \{(0,0,0),(0,0,1),(1,1,0),(1,1,1)\}\\
P_4 &= \{(0,0,0),(1,0,1)\} & L_4 &= \{(0,0,0),(0,1,0),(1,0,1),(1,1,1)\}\\
P_5 &= \{(0,0,0),(1,1,0)\} & L_5 &= \{(0,0,0),(0,1,0),(1,1,0),(1,0,0)\}\\
P_6 &= \{(0,0,0),(1,1,1)\} & L_6 &= \{(0,0,0),(0,1,1),(1,0,1),(1,1,0)\}\\
P_7 &= \{(0,0,0),(1,0,0)\} & L_7 &= \{(0,0,0),(0,1,1),(1,1,1),(1,0,0)\}
\end{aligned}$$

thus, the vectors representing the points and lines are

$$\begin{aligned}
P_1 &: (0,0,1) & L_1 &: [1,0,0]\\
P_2 &: (0,1,0) & L_2 &: [0,1,0]\\
P_3 &: (0,1,1) & L_3 &: [1,1,0]\\
P_4 &: (1,0,1) & L_4 &: [1,0,1]\\
P_5 &: (1,1,0) & L_5 &: [0,0,1]\\
P_6 &: (1,1,1) & L_6 &: [1,1,1]\\
P_7 &: (1,0,0) & L_7 &: [0,1,1].
\end{aligned}$$

The graphical representation of $PG(2,2)$ is known as the Fano plane, see Figure A.2. It is the finite projective plane with the smallest possible number of points and lines: 7 points and 7 lines, with 3 points on every line and 3 lines through every point.

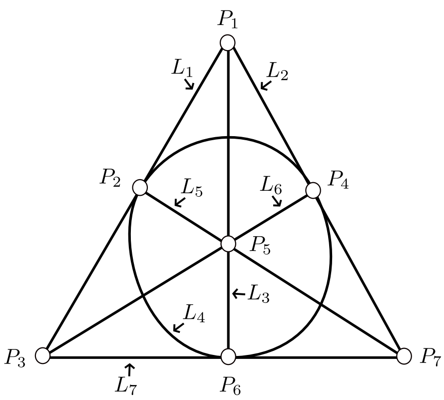


Figure A.2: Fano plane

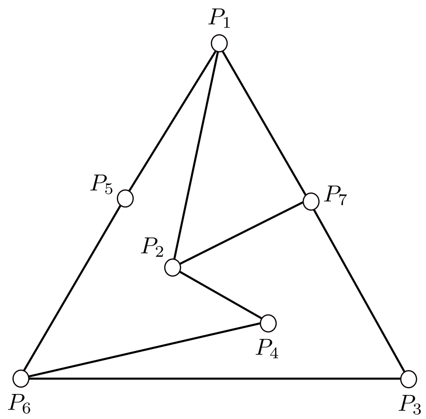
Definition 4. A *polarity* of a projective plane is a bijective map $\phi : X \cup L \longrightarrow X \cup L$ that maps points to lines and lines to points with the property that $p \in l$ if and only if $\phi(l) \in \phi(p)$, and ϕ^2 is the identity map on $X \cup L$. A point $\mathbf{x}$ such that $\mathbf{x} \in \phi(\mathbf{x})$ is called an *absolute point* of the polarity ϕ.

The *polarity graph* of a projective plane $\pi = (X, L)$ with respect to a polarity ϕ is the graph $G = (V, E)$ with vertex set $V = X$ and edge set given by

$$E = \{\{\mathbf{x}, \mathbf{y}\} \in V \times V : \mathbf{x} \in \phi(\mathbf{y})\}.$$

A trivial polarity of $PG(2, q)$ is given by $\rho : PG(2, q) \longrightarrow PG(2, q)$ such that $\rho : (x_0, x_1, x_2) \mapsto [x_0, x_1, x_2]$, $\rho : [x_0, x_1, x_2] \mapsto (x_0, x_1, x_2)$. When $\pi = PG(2, q)$ and the polarity used is ρ, the resulting polarity graph is known as the *Erdös-Rényi orthogonal polarity graph*. This graph was introduced in this form by Erdös-Rényi in 1962 [64] to give constructive examples of graphs with small maximum degree, relatively few edges and diameter 2. Example 2 illustrates the Erdös-Rényi orthogonal polarity graph obtained from $PG(2, 2)$ (see Example 21) and the polarity ρ defined above.

Example 22.



Bondy in [65] cites two earlier references to this type of graph, the first is a paper of Artzy [66] who called it a reduced Levi graph; the second is a paper of Kempe [67] where the notion of polarity graph appears.

This graph can also be defined without direct reference to polarities. This is more common in graph theory literature, so we include this definition as well.

Definition 5. The *Erdös-Rényi orthogonal polarity* graph, denoted ER_q, is the graph whose vertices are the left normalized vectors of $PG(2,q)$, and two distinct vertices (x_0, x_1, x_2) and (y_0, y_1, y_2) are adjacent if and only if $x_0y_0 + x_1y_1 + x_2y_2 = 0$.

Example 23. Let $PG(2,3) = \{P_1, P_2, P_3, P_4, P_5, P_6, P_7, P_8, P_9, P_{10}, P_{11}, P_{12}, P_{13}\}$ where

$$
\begin{array}{lll}
P_1 = (0,0,1) & P_6 = (1,0,1) & P_{11} = (1,2,0) \\
P_2 = (0,1,0) & P_7 = (1,0,2) & P_{12} = (1,2,1) \\
P_3 = (0,1,1) & P_8 = (1,1,0) & P_{13} = (1,2,2) \\
P_4 = (0,1,2) & P_9 = (1,1,1) & \\
P_5 = (1,0,0) & P_{10} = (1,1,2) &
\end{array}
$$

The ER_3 graph is illustrated in Figure A.3.

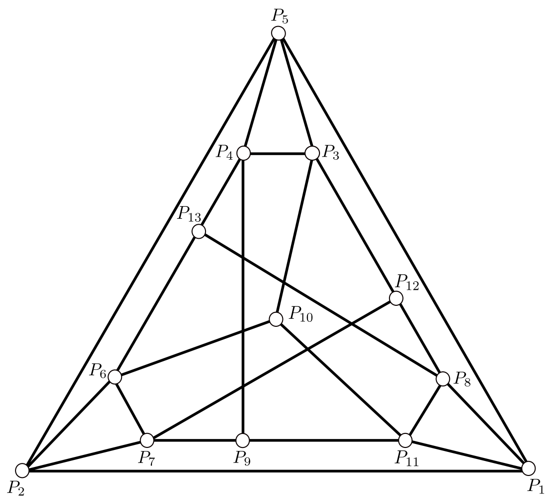


Figure A.3: ER_3

Remark 12. ER_q is a simple graph. A point $\mathbf{x} = (x_0, x_1, x_2) \in PG(2,q)$ that satisfies the equation $x_0^2 + x_1^2 + x_2^2 = 0$ is called an *absolute vertex* of the graph. In Example 23 the point $P_{10} = (1,1,2)$ is an absolute vertex of ER_3.

In 1966, Erdös, Rényi and Sós [30] and independently Brown [29] considered ER_q in connection with the Turán number $ex(q^2+q+1, C_4)$ of the four cycle C_4 which consists in determining the largest number of edges in a graph on q^2+q+1 vértices without cycles of length four. They independently proved that ER_q has q^2+q+1 vertices, has

$\frac{1}{2}q(q+1)^2$ edges, and is C_4-free. Then, for any prime power q,

$$\frac{1}{2}q(q+1)^2 \leq ex(q^2+q+1, C_4).$$

To make this chapter self-contained, we reproduce the proof here. The number of different points of $PG(2,q)$ is q^2+q+1 because for each $\lambda \in \mathbb{F}_q^*$, the point $(\lambda a, \lambda b, \lambda c) \in PG(2,q)$ represents the same point as (a,b,c). Therefore, $v(ER_q) = q^2+q+1$. A straight line in $PG(2,q)$ is the set of all points (x,y,z) which satisfy the equation $ax+by+cz=0$; let us remember that this line is denoted by $[a,b,c]$. The point (a,b,c) and the line $[a,b,c]$ are clearly conjugate elements with respect to the conic $x^2+y^2+z^2=0$. Then, there are $q+1$ points on each line, any two different lines have exactly one point in common and through any two given points there is exactly one straight line. The polarity ρ defined above maps the point $A=(a,b,c)$ into the line $\rho(A)=[a,b,c]$ and conversely. This mapping has evidently the properties: if the point B lies on the line $\rho(A)$ then the point A lies on the line $\rho(B)$; if C is the point of intersection of the lines $\rho(A)$ and $\rho(B)$ then $\rho(C)$ is identical with the line passing through the points A and B; A is on $\rho(A)$ if and only if $a^2+b^2+c^2=0$, i.e. if A lies on the conic $x^2+y^2+z^2=0$. Clearly a vertex A in ER_q has the degree q or $q+1$ according to whether A is on the conic $x^2+y^2+z^2=0$ or not. Thus,

$$\frac{1}{2}(n^{3/2}-n) \leq \frac{1}{2}q(q^2+q+1) \leq e(ER_q)$$

and

$$e(ER_q) \leq \frac{1}{2}(q+1)(q^2+q+1) \leq \frac{1}{2}(n^{3/2}+n),$$

where $n = q^2+q+1$.

Finally the diameter of ER_q is equal to 2. As a matter of fact any two points A and B can be joined by the path ABC where C is the point of intersection of the lines $\rho(A)$ and $\rho(B)$. Moreover, A and B can be joined by a single edge if A lies on $\rho(B)$. But the point C such that the edges AC and BC both belong to ER_q is in any case unique; thus ER_q does not contain any cycle of length 4.

A.6.1 Some properties of ER_q

Let $\mathbf{x} = (x_0, x_1, x_2)$ be a vertex of ER_q. Notice that the neighborhood $N(\mathbf{x})$ of $\mathbf{x}$ consists of the vertices $\mathbf{y} = (y_1, y_2, y_3)$ that satisfy the linear equation

$$x_0y_0 + x_1y_1 + x_2y_2 = 0.$$

This equation has q^2-1 non-zero solutions that represent $(q^2-1)/(q-1) = q+1$ distinct projective points, which are different from $\mathbf{x}$ if and only if $x_0^2+x_1^2+x_2^2 \neq 0$.

Then, ER_q has q^2 vertices of degree $q+1$, and $q+1$ absolute vertices, lying on the quadric $x_0^2+x_1^2+x_2^2=0$. Thus, the vertex set of ER_q is a disjoint union of the sets

$V=\{\mathbf{x}\in V(ER_q):deg(\mathbf{x})=q+1\}$ and $W=\{\mathbf{x}\in V(ER_q):deg(\mathbf{x})=q\}$.

This is, $V(ER_q)=V\cup W$ where $|V|=q^2, |W|=q+1$, and $V\cap W=\emptyset$.

Let V_1 be the subset of V comprising all vertices adjacent to at least one absolute vertex and let $V_2=V\setminus V_1$. Bachratý and Širáň presented in [68] the following structural information of the ER_q graph.

Theorem 13. For every prime power q, the graph ER_q has the following properties:

(i) The set W of absolute vertices is independent;

(ii) Each pair of vertices of V (adjacent or not) are connected by a unique path of length 2, while no edge incident to an absolute vertex is contained in any triangle; in particular, ER_q has diameter 2;

(iii) If q is odd, then every vertex of V_1 is adjacent to exactly two absolute vertices, and $|V_1|=q(q+1)/2$, $|V_2|=q(q-1)/2$;

(iv) If q is odd, then the subgraphs of ER_q induced by V_1 and V_2 are regular of degree $(q-1)/2$ and $(q+1)/2$, respectively;

(v) If q is even, then $|V_1|=q^2$ and V_2 is empty; moreover, V_1 contains a vertex v adjacent to all absolute vertices and every vertex in $V_1\setminus\{v\}$ is adjacent to exactly one absolute vertex and the subgraph of ER_q induced by the set $V_1\setminus\{v\}$ is regular of degree q.

Proof. (i) Let $\mathbf{a}=(a_1,a_2,a_3)$ and $\mathbf{b}=(b_1,b_2,b_3)$ be two distinct vertices of W. Then

$$\begin{aligned}\mathbf{a}\cdot\mathbf{a}&=a_1^2+a_2^2+a_3^2=0,\\ \mathbf{b}\cdot\mathbf{b}&=b_1^2+b_2^2+b_3^2=0.\end{aligned}$$

If $\mathbf{a}$ is adjacent to $\mathbf{b}$ then

$$a_1b_1+a_2b_2+a_3b_3=0.$$

The above implies that $\mathbf{a}$ and $\mathbf{b}$ are solutions of the linear system

$$\begin{aligned}\mathbf{a}\cdot\mathbf{x}&=a_1x_1+a_2x_2+a_3x_3=0,\\ \mathbf{b}\cdot\mathbf{x}&=b_1x_1+b_2x_2+b_3x_3=0.\end{aligned}\tag{A.9}$$

Since the vectors **a** and **b** are linearly independent over $\mathbb{F}_q$, the solution space of the linear system (A.9) has dimension one. Therefore, **a**=**b**, which is not possible. It follows that no pair of absolute vertices can be adjacent, this is, W is an independent set.

(ii) Let $\mathbf{a} = (a_1, a_2, a_3)$ and $\mathbf{b} = (b_1, b_2, b_3)$ be two distinct vertices of ER_q (adjacent or not). If $\mathbf{c} = (c_1, c_2, c_3)$ and $\mathbf{d} = (d_1, d_2, d_3)$ are two distinct vertices of ER_q adjacent to **a** and **b**, then

$$\begin{aligned}
\mathbf{a} \cdot \mathbf{c} &= a_1c_1 + a_2c_2 + a_3c_3 = 0,\\
\mathbf{b} \cdot \mathbf{c} &= b_1c_1 + b_2c_2 + b_3c_3 = 0,\\
\mathbf{a} \cdot \mathbf{d} &= a_1d_1 + a_2d_2 + a_3d_3 = 0,\\
\mathbf{b} \cdot \mathbf{d} &= b_1d_1 + b_2d_2 + b_3d_3 = 0.
\end{aligned}$$

Since the solution space of the linear system (A.9) has dimension one, $\mathbf{c} = \mathbf{d}$, which is a contradiction. Thus, every pair of distinct vertices are connected by exactly one path of length two, this implies that ER_q has diameter 2.

On the other hand, let $\mathbf{a} = (a_1, a_2, a_3)$ and $\mathbf{b} = (b_1, b_2, b_3)$ be two distinct adjacent vertices of ER_q. If **a** is an absolute vertex and the edge $\{\mathbf{a}, \mathbf{b}\}$ is contained in a triangle, then there is a vertex $\mathbf{c} = (c_1, c_2, c_3)$ of ER_q different from **a** and **b** such that $\{\mathbf{a}, \mathbf{c}\}$ and $\{\mathbf{b}, \mathbf{c}\}$ are edges of ER_q. Then,

$$\begin{aligned}
\mathbf{a} \cdot \mathbf{a} &= a_1a_1 + a_2a_2 + a_3a_3 = 0,\\
\mathbf{b} \cdot \mathbf{a} &= b_1a_1 + b_2a_2 + b_3a_3 = 0,
\end{aligned} \tag{A.10}$$

$$\begin{aligned}
\mathbf{a} \cdot \mathbf{c} &= a_1c_1 + a_2c_2 + a_3c_3 = 0,\\
\mathbf{b} \cdot \mathbf{c} &= c_1c_1 + c_2c_2 + b_3c_3 = 0.
\end{aligned} \tag{A.11}$$

By (A.10), (A.11) and the fact that the solution space of the linear system (A.9) has dimension one, $\mathbf{c} = \mathbf{a}$, which is not possible.

(iii) Let q be odd. Invoking Chapters 7 and 8 of [69], the set W forms a conic and hence an oval. By Corollary 8.2 of [69] applied to the oval W, every vertex of V_1 and V_2 corresponds to a line of $PG(2, q)$ containing exactly two points of W (a bisecant) or no point of W (an external line), respectively, and $|V_1| = q(q + 1)/2, |V_2| = q(q - 1)/2$.

(iv) Table 8.1 of [69] shows that a bisecant contains $(q - 1)/2$ points each lying on exactly two lines determined by projective coordinates corresponding to a vertex in W, while an external line contains $(q + 1)/2$ points each of which lies on no line determined by projective coordinates corresponding to a vertex in W.

□

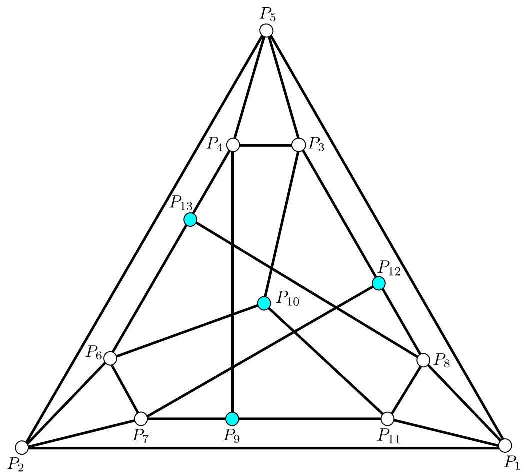


Figure A.4: The four absolute vertices colored in blue form an independent set

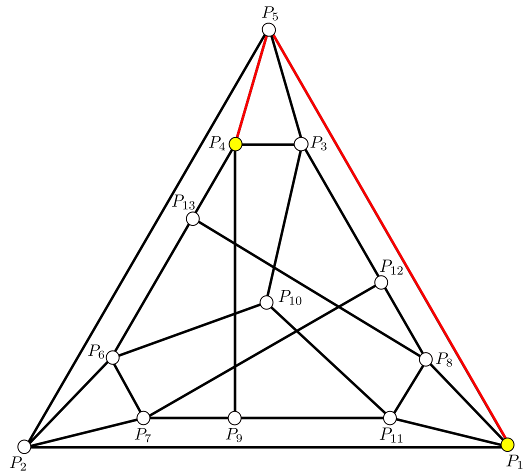


Figure A.5: The edges colored in red show the only path of length 2 between the two non-adjacent vertices P_1 and P_4 colored in yellow

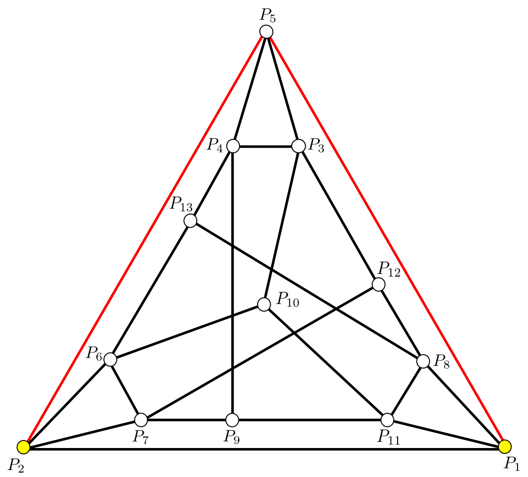


Figure A.6: The edges colored in red show the only path of length 2 between the two adjacent vertices P_1 and P_2 colored in yellow

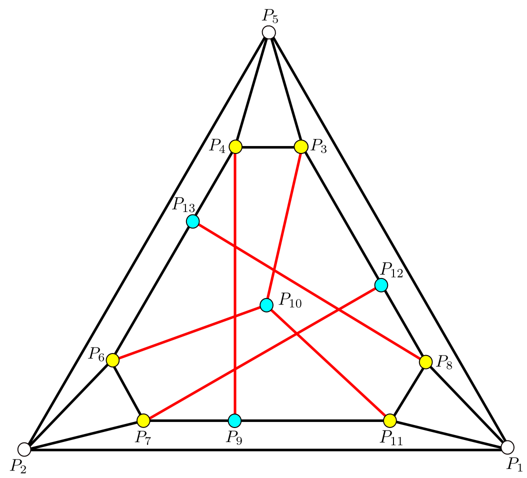


Figure A.7: No red edge incident to an blue absolute vertex is contained in any triangle in ER_3

Example 24. According to Example 3, $W = \{P_9, P_{10}, P_{12}, P_{13}\}$ where $P_9 = (1, 1, 1)$, $P_{10} = (1, 1, 2), P_{12} = (1, 2, 1)$ and $P_{13} = (1, 2, 2)$. Moreover, $V = \{P_1, P_2, \ldots, P_{11}\}$, $V_1 = \{P_3, P_4, \ldots, P_{11}\}$ and $V_2 = \{P_1, P_2, P_5\}$. By Theorem 13 (i), W is an independent set in ER_3, see Figure A.4. Figure A.5, A.6 and A.7 illustrate Theorem 13 (ii) for some vertices of ER_3.

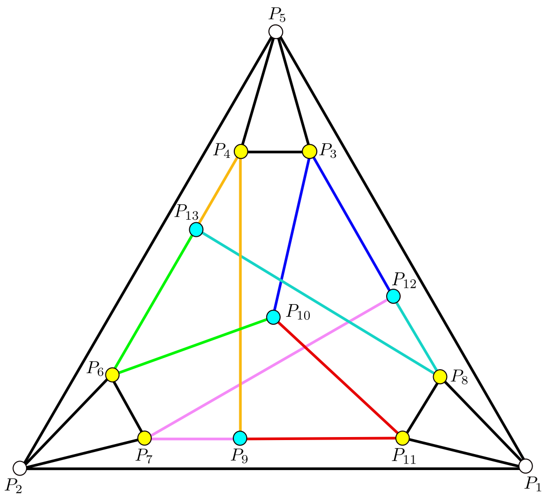


Figure A.8: The vertices de V_1 are colored in yellow and the absolute vertices are colored in blue. Every vertex of V_1 is adjacent to exactly two absolute vertices

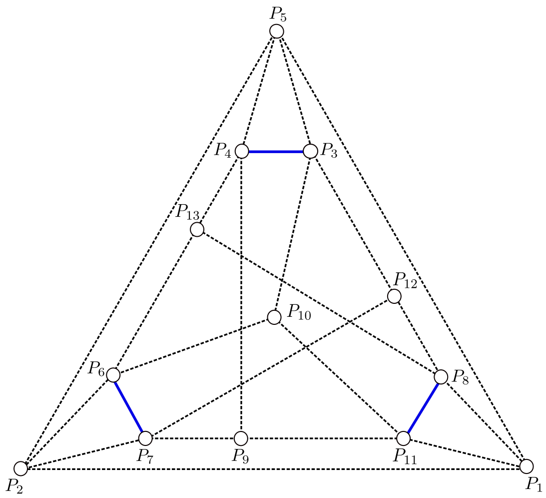


Figure A.9: Subgraph induced by V_1

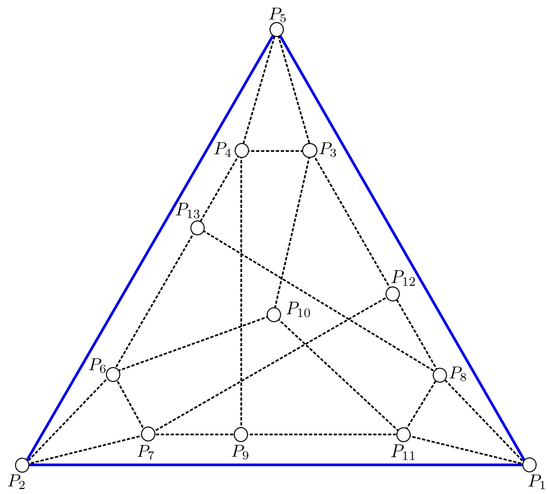


Figure A.10: Subgraph induced by V_2

By (iii) of Theorem 13, $|V_1| = q(q+1)/2 = 3(4)/2 = 6$, $|V_2| = q(q-1)/2 = 3(2)/2$, and every vertex of V_1 (yellow vertices) is adjacent to exactly two absolute vertices (blue vertices), see Figure A.8. For example, P_3 is adjacent to P_{10} and P_{12}. Finally, by (iv) of Theorem 13, the subgraphs of ER_3 induced by V_1 and V_2 are regular of degree $(q-1)/2 = (3-1)/2 = 1$ and $(q+1)/2 = (3+1)/2 = 2$, respectively, see Figures A.9 and A.10.

To illustrate Theorem 13 (v), let $\mathbb{F}_4 = \{0, 1, \theta, \theta^2\}$ with $\theta^2 = \theta + 1$ and $PG(2,4) = \{P_1, P_2, \ldots, P_{21}\}$ where

$$\begin{array}{llll}
P_1 = (1,0,1) & P_7 = (0,1,\theta) & P_{12} = (0,1,1) & P_{17} = (1,\theta,1)\\
P_2 = (1,\theta^2,1) & P_8 = (1,\theta,\theta^2) & P_{13} = (0,0,1) & P_{18} = (1,0,\theta^2)\\
P_3 = (1,1,0) & P_9 = (1,\theta^2,\theta) & P_{14} = (1,\theta,0) & P_{19} = (1,0,\theta)\\
P_4 = (1,\theta^2,\theta^2) & P_{10} = (1,\theta^2,0), & P_{15} = (1,1,1) & P_{20} = (1,1,\theta^2)\\
P_5 = (0,1,0) & P_{11} = (1,0,0) & P_{16} = (0,1,\theta^2) & P_{21} = (1,1,\theta).\\
P_6 = (1,\theta,\theta) & & &
\end{array}$$

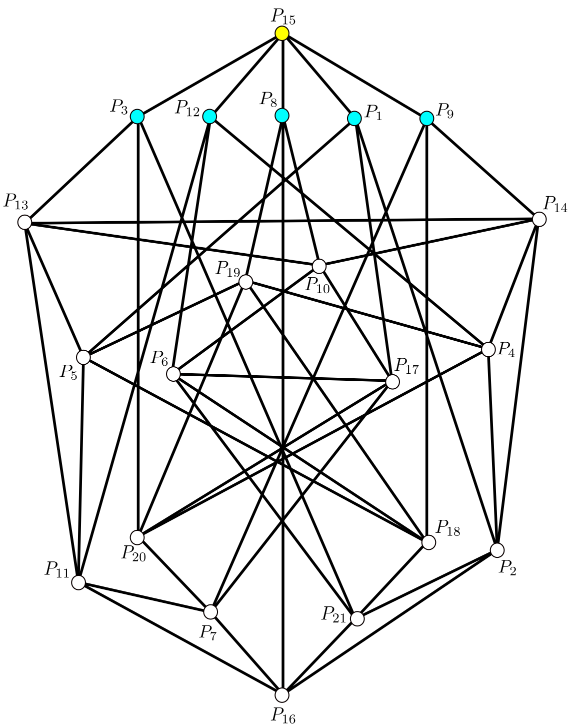


Figure A.11: The vertex P_{15} colored in yellow is adjacent to all absolute vertices colored in blue

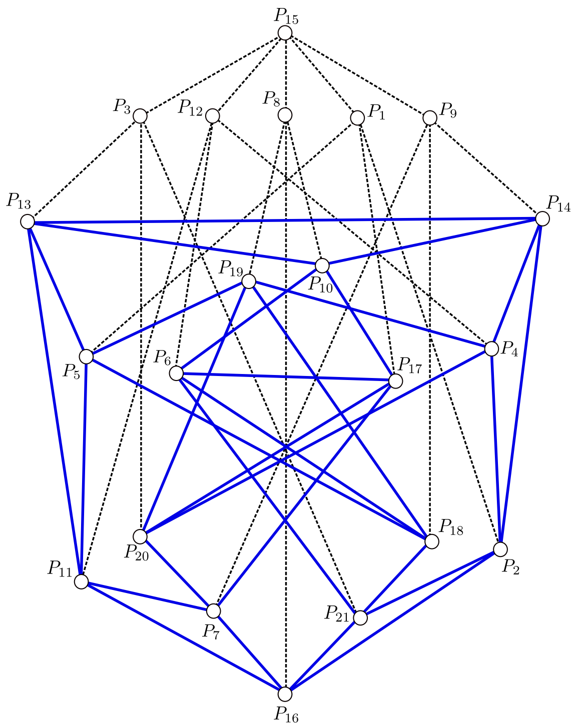


Figure A.12: Subgraph induced by $V_1 \setminus \{P_{15}\}$

In this case, $V_1 = V = \{P_2, P_4, P_5, P_6, P_7, P_{10}, P_{11}, P_{13}, P_{14}, P_{15}, P_{16}, P_{17}, P_{18}, P_{19}, P_{20}, P_{21}\}$, $|V_1| = q^2 = 4^2 = 16$ and V_2 is empty. Note that P_{15} is adjacent to all absolute vertices which are P_1, P_3, P_8, P_9 and P_12; every vertex in $V_1 \setminus \{P_{15}\}$ is adjacent to exactly one absolute vertex, see Figure A.11. The subgraph of ER_4 induced by $V_1 \setminus \{P_{15}\}$ is regular of degree 4, see Figure A.12.

A.6.2 Two subgraphs isomorphic to ER_q

The adjacency relation in ER_q is not the most suitable for algebraic manipulations, for this reason, we present two graphs isomorphic to ER_q. The first was constructed by Mubayi and Williford in [35], and its definition is as follows:

Definition 6. For q an odd prime power, ER_q^* is the graph whose vertex set is $V(ER_q)$ in which two vertices (x_0, x_1, x_2) and (y_0, y_1, y_2) are adjacent if

$$x_0y_2 - x_1y_1 + x_2y_0 = 0.$$

The second was constructed by Erskine, Fratrič and Širáň in [37], and its definition is as follows:

Definition 7. Let $\alpha \in \mathbb{F}_q^*$. For q a prime power, ER_q^{**} is the graph whose vertex set is $V(ER_q)$ in which two vertices (x_0, x_1, x_2) and (y_0, y_1, y_2) are adjacent if

$$x_0y_2 + x_1y_1 + x_2y_0 + \alpha x_2y_2 = 0.$$

Lemma 11. *Let q be a prime power and let b be any element of $\mathbb{F}_q$. Then there exist $c, d \in \mathbb{F}_q$ such that $c^2 + d^2 = b$.*

Theorem 14.

(i) ER_q *is isomorphic to* ER_q^*;
(ii) ER_q *is isomorphic to* ER_q^{**}.

Proof.

1. The matrix associated with the bilinear form of ER_q is the identity matrix

$$I = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

while the associated with the bilinear form of ER_q^* is

$$M = \begin{pmatrix} 0 & 0 & 1 \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}.$$

Mubayi and Williford showed that there is a basis change matrix A which transforms M to I, up to a scalar multiple; more precisely, they found a matrix A such that $A^T M A = \lambda I$, for some non-zero λ.

- If q is a power of 2, they use the following matrix:

$$A_2 = \begin{pmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}.$$

- If q is odd, let $a, b, c, d, i \in \mathbb{F}_q$ be such that $a^2 = -2, b^2 = 2, c^2 + d^2 = -1, i^2 = -1$, when they exist. Mubayi et al. used the following change of variables for $q \equiv 1 \bmod 4$ and $q \equiv 3, 7 \bmod 8$ which they labeled A_1, A_3, A_7, respectively:

$$A_1 = \begin{pmatrix} \frac{1+i}{2} & 0 & \frac{1-i}{2} \\ 0 & i & 0 \\ -\frac{(1-i)}{2} & 0 & -\frac{(1+i)}{2} \end{pmatrix}, \quad A_3 = \begin{pmatrix} \frac{a}{2} & a & \frac{a}{2} \\ -1 & -1 & -1 \\ -\frac{a}{2} & 0 & \frac{a}{2} \end{pmatrix}, \quad A_7 = \begin{pmatrix} \frac{1}{b} & a & \frac{1}{b} \\ -\frac{d}{b} & c & \frac{d}{b} \\ \frac{c}{b} & d & -\frac{c}{d} \end{pmatrix}.$$

2. Again, the matrix associated with the bilinear form of ER_q is the identity matrix I, while the associated with the bilinear form of ER_q^{**} is

$$B = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & \alpha \end{pmatrix}.$$

Erskine, Fratrič and Širáň showed that there is a basis change matrix A such that $A^T B A = \gamma I$, for some non-zero γ. By Lemma 11 there exist $c, d \in \mathbb{F}_q$ with $c^2 + d^2 = -1$, for odd q it can be checked that the following matrix A satisfies $A^T B A = -I$:

$$\begin{pmatrix} d - c\alpha/2 & -(c + d\alpha/2) & -(1 + \alpha/2) \\ c - d & c + d & 1 \\ c & d & 1 \end{pmatrix}.$$

If q is a power of 2, then the non-zero element $\alpha \in \mathbb{F}_q$ has a unique square root $\sqrt{\alpha} \in \mathbb{F}_q$, and then one can take

$$\begin{pmatrix} \sqrt{\alpha} & 0 & 0 \\ 0 & 1 & 0 \\ \sqrt{\alpha^{-1}} & 0 & \sqrt{\alpha^{-1}} \end{pmatrix}.$$

□

Bibliography

[1] D. Daza, C. Martos, and C. Trujillo. Almost difference sets from Singer type Golomb rulers. *IEEE Access*, 10:1132 – 1137, 2022.

[2] D. Daza, C. Martos, and C. Trujillo. Non-existence of $(p^m, k, 1)$ difference sets. *Electronics Letters*, 58(4):154 – 155, 2022.

[3] D. Daza, M. Huicochea, C. Martos, and C. Trujillo. Sidon sets and subgraphs of the Erdös-Rényi orthogonal polarity graph. *Contributions to Discrete Mathematics*, Submitted for evaluation.

[4] C. Martos, D. Daza, and C. Trujillo. Near-Optimal g-Golomb Rulers. *IEEE Access*, 9:65482 – 65489, 2021.

[5] D. Daza, M. Huicochea, C. Martos, and C. Trujillo. Theorem For Restricted Sumsets. *International Journal of Number Theory*, Submitted for evaluation.

[6] C. Martos, M. Huicochea, D. Daza, and C. Trujillo. Minimun overlap problem on finite groups. *Boletín de la Sociedad Matemática Mexicana*, Submitted for evaluation.

[7] J. Cilleruelo, I. Ruzsa, and C. Vinuesa. Generalized Sidon sets. *Advances in Mathematics*, 225(5):2786 – 2807, 2010.

[8] J. Cilleruelo. Combinatorial problems in finite fields and Sidon sets. *Combinatorica*, 5(32):497 – 511, 2012.

[9] L. A. Vinh. Graphs generated by Sidon sets and algebraic equations over finite fields. *Journal of Combinatorial Theory, Series B*, 6(103):651 – 657, 2013.

[10] M. Tait and C. Timmons. Sidon sets and graphs without 4-cycles. *J. Comb.*, 2(5):155 – 165, 2014.

[11] M. Tait and C. Timmons. Orthogonal Polarity Graphs and Sidon Sets. *Journal of Graph Theory*, 2(82):103 – 116, 2016.

[12] J. Singer. A Theorem in Finite Projective Geometry and Some Applications to Number Theory. *Transactions of the American Mathematical Society.*, 3(43):377 – 385, 1938.

[13] J. R. Hufford. $(261, 105, 42)$ Abelian Difference Sets Do Not Exist. Master's thesis, Wright State University, March 2015.

[14] A. S. Osifodunrin and K. W. Smith. $(220, 73, 24)$ and $(231, 70, 21)$ Difference Sets Do Not Exist. *Journal of Applied Sciences Research*, 6(7):897 – 904, 2010.

[15] K. T. Arasu. $(81, 16, 3)$ abelian difference sets do not exists. *Journal of Combinatorial Theory Series A*, 43(2):343 – 350, 1986.

[16] A. S. Osifodunrin. On non-existence of some difference sets. *Mathematical Communications*, 17:469 – 488, 2012.

[17] A. S. Osifodunrin and J. Aizebeokhai. Non-Existence of $(155, 56, 20)$ difference sets. *Journal of the Nigerian Mathematical Society*, 38(1):11 – 19, 2019.

[18] Y. Zhang, G. J. Lei, and S. P. Zhang. A new family of almost difference sets and some necessary conditions. *IEEE Transactions on Information Theory*, 52(5):2052 – 2061, 2006.

[19] D. Clayton. A note on almost difference sets in nonabelian groups. *Designs, Codes and Cryptography*, 72(3):1 – 6, 2017.

[20] K. T. Arasu, C. Ding, T. Helleseth, P. Kumar, and H. Martinsen. Almost difference sets and their sequences with optimal autocorrelation. *IEEE Transactions on Information Theory*, 47(7):2934 – 2943, 2001.

[21] Y. Cai and C. Ding. Binary sequences with optimal autocorrelation. *Theoretical Computer Science*, 410(24):2316 – 2322, 2009.

[22] C. Ding. *Codes from Difference Sets.* World Scientific Publishing Co. Pte Ltd. Hackensack, first edition, 2015.

[23] C. Ding, T. Helleseth, and H. Martinsen. New families of binary sequences with optimal three-level autocorrelation. *IEEE Transactions on Information Theory*, 47(1):428 – 433, 2001.

[24] C. Ding, A. Pott, and Q. Wang. Constructions of almost difference sets from finite fields. *Designs, Codes and Cryptography*, 72(3):581 – 592, 2014.

[25] C. Ding and X. Tang. New classes of balanced quaternary and almost balanced binary sequences with optimal autocorrelation value. *IEEE Transactions on Information Theory*, 56(12):6398 – 6405, 2010.

[26] K. Nowak. A survey on almost difference sets. *arXiv math.CO*, page 1409.0114v1, 2014.

[27] J. Michel and B. Ding. A generalization of combinatorial designs and related codes. *Designs, Codes and Cryptography*, 82(3):511 – 529, 2017.

[28] J. Robinson and A. Bernstein. über ein problem von k. zarankiewicz. *Acta Math Acad Sci Hungar*, 9(1–4):29 – 47, 1958.

[29] W. G. Brown. On graphs that do not contain a Thomsen graph. *Mathematical Bulletin*, 9(3):281 – 285, 1966.

[30] P. Erdös, A. Rényi, and P. Turán. On a problem of graph theory. *Studia Scientiarum Mathematicarum Hungarica*, 1:215 – 235, 1966.

[31] Z. Füredi. On the number of edges of quadrilateral-free graphs. *Journal of Combinatorial Theory, Series B*, 60(1):1 – 6, 1996.

[32] C. Balbuena, P. García, and L. P. Montejano. Superconnectivity of graphs with odd girth g and even girth h. *Discrete Applied Mathematics*, 159(2–3):91 – 99, 2011.

[33] A. Kostochka, P. Pudlák, and V. Rödl. Some constructive bounds on Ramsey numbers. *Journal of Combinatorial Theory, Series B*, 100(64):439 – 445, 2010.

[34] F. Lazebnik and J. Verstraëte. On hypergraphs of girth five. *The Electronic Journal of Combinatorics*, 10(25):1 – 15, 2003.

[35] D. Mubayi and J. Williford. On the independence number of the Erdös-Rényi and projective norm graphs and a related hypergraph. *Journal of Graph Theory*, 2(56):113 – 127, 2007.

[36] X. Peng, M. Tait, and C. Timmons. On the chromatic number of the Erdös-Rényi orthogonal polarity graph. *The Electronic Journal of Combinatorics*, 2(22):1 – 19, 2015.

[37] G. Erskine, P. Fratrič, and J. Širáň. Graphs derived from perfect difference sets. *Australasian Journal of Combinatorics*, 80(1):48 – 56, 2021.

[38] M. Hall. Cyclic projective planes. *Duke Mathematical Journal*, 14(4):1079 – 1090, 1947.

[39] R. H. Bruck. Difference sets in a finite group. *Transactions of the American Mathematical Society*, 78:464 – 481, 1955.

[40] C. J. Colbourn. Applications of combinatorial designs in computer science. *ACM Computing Surveys*, 21(2):223 – 250, 1989.

[41] G. Oliveri, P. Rocca, and A. Massa. Interleaved linear arrays with difference sets. *Electronics Letters*, 46:323 – 324, 2010.

[42] T. Beth, D. Jungnickel, and Lenz. H. *Design Theory.* Cambridge University Press, second edition, 1999.

[43] T. A. Evans and H. B. Mann. On simple difference sets. *Sankhya: The Indian Journal of Statistics*, 11:357 – 364, 1951.

[44] M. Gordon. The Prime Power Conjecture is True for $n < 2000000$. *The Electronic Journal of Combinatorics*, 1:1 – 7, 1994.

[45] F. Luca, S. Tengely, and A. Togbé. On the Diophantine equation $x^2 + c = 4y^n$. *Annales Mathematiques du Quebec*, 33(2):171 – 184, 2009.

[46] C. Ding. Cyclic codes from cyclotomic sequences of order four. *Finite Fields and Their Applications*, 23(1):8 – 34, 2013.

[47] T. Cusick, C. Ding, and A. Renvall. *Stream Ciphers and Number Theory.* North-Holland Publishing Co., Amsterdam, first edition, 1988.

[48] C. Ding. The differential cryptanalysis and design of the natural stream ciphers. *Lecture Notes in Computer Science. Springer-Verlag*, 809:101 – 115, 1994.

[49] C. Ding, T. Helleseth, and K. Y. Lam. Several classes of sequences with three-level autocorrelation. *IEEE Transactions on Information Theory*, 45(7):2606 – 2612, 1999.

[50] H. Halberstam and Laxton. R. On perfect difference sets. *The Quarterly Journal of Mathematics*, 14(1):86 – 90, 1963.

[51] M. H. Mateeni, M. K. Mahmmod, D. Alghazzawi, and J.-B Liu. tructures of power digraphs over the congruence equation $x^p \equiv y \pmod{m}$ and enumerations. *American Institute of Mathematical Sciences*, 6(5):4581 – 4596, 2021.

[52] M. H. Mateeni, M. K. Mahmmod, A. D. Kattan, and S. Ali. A novel approach to find partitions of z_m with equal sum subsets via complete graphs. *American Institute of Mathematical Sciences*, 6(9):99981 – 10024, 2021.

[53] D. Ruiz and C. Trujillo. Construction of $B_h[g]$ sets in product of groups. *Revista Colombiana de Matemáticas*, 50(2):165 – 174, 2016.

[54] R. Lidl and R. Niederreiter. *Introduction to Finite Fields and their applications.* Cambridge University Press, revised edition, 2002.

[55] P. Erdös and P. Turán. On a problem of Sidon in additive number theory, and on some related problems. *Journal of the London Mathematical Society*, (16):212 – 215, 1941.

[56] D. R. Hughes. Planar division neo-rings. *Transactions of the American Mathematical Society*, 2(80):502 – 527, 1955.

[57] R. C. Bose and S. Chowla. Theorems in the additive theory of numbers. *Commentarii Mathematici Helvetici*, (37):141 – 147, 1962.

[58] M. J. Ganley. Direct product difference sets. *Journal of Combinatorial Theory, Series A*, 3(23):321 – 332, 1977.

[59] I. Z. Ruzsa. Solving a linear equation in a set of integers I. *Acta Arithmetica*, 3(65):259 – 268, 1993.

[60] K. O'Bryant. A complete annotated bibliography of work related to Sidon sequences.

The Electronic Journal of Combinatorics, DS 11:1 – 39, 2004.

[61] C. Gómez and C. Trujillo. A new construction of modular B_h-sequences. *Matemática Enseñanza Universitaria*, 19(1):53 – 62, 2011.

[62] N. Y. Caicedo. *Conjuntos de Sidon en dos dimensiones.* PhD thesis, Universidad del Valle, Marzo 2016.

[63] J. Williford. *Constructions In Finite Geometry With Applications To Graphs.* PhD thesis, Delaware University, May 2004.

[64] P. Erdös and A. Rényi. On a problem in the theory of graphs. *Mathematical Institute of the Hungarian Academy of Sciences*, 7:623 – 641, 1962.

[65] J. A. Bondy. Extremal Problems of Paul Erdös on Circuits in Graphs. *Paul Erdös and his mathematics II*, 2:135 – 156, 1999.

[66] R. Artzy. Self-dual configurations and their Levi graphs. *Proceedings of the American Mathematical Society*, 7(2):299 – 303, 1956.

[67] A. B. Kempe. A Memoir on the Theory of Mathematical Form. *Philosophical Transactions of the Royal Society of London*, 177:1 – 70, 1886.

[68] M. Bachratý and J. Širáň. Polarity graphs revisited. *Ars Mathematica Contemporanea*, 8:55 – 67, 2015.

[69] J. Hirschfeld. *Projective geometries over finite fields.* Oxford University Press, second edition, 1998.