UNIVERSITY OF CALIFORNIA, SAN DIEGO

Connections between graph theory, additive combinatorics, and finite incidence geometry

A dissertation submitted in partial satisfaction of the
requirements for the degree
Doctor of Philosophy

in

Mathematics

by

Michael Tait

Committee in charge:

Professor Jacques Verstraëte, Chair
Professor Fan Chung Graham
Professor Ronald Graham
Professor Shachar Lovett
Professor Brendon Rhoades

2016

The dissertation of Michael Tait is approved, and it is acceptable in quality and form for publication on microfilm and electronically:

_____

_____

_____

_____

_____

Chair

University of California, San Diego

2016

DEDICATION

To Lexi.

TABLE OF CONTENTS

LIST OF FIGURES

ACKNOWLEDGEMENTS

I must first thank my advisor Jacques Verstraëte for making this thesis possible. His support for research and travel was invaluable. More importantly, our work together transformed me into the mathematician that I am today. Thank you, Jacques, for the problems you offered to me, for your insight, for your hard work, and for your encouragement.

I would like to thank several other mathematicians who have helped me along the way: Craig and Josh, for being outstanding collaborators and friends; Sebi, for both professional and non-professional advice; my thesis committee, for their time; Fan, Mike, and Laura, for both guidance and recommendation letters; everyone from the GRWC, for the math, for the advice, for the late nights and early mornings, and for the friendships; Troy, Flo, Paul, and Po, for hosting; Rob and Francesca, for long hours in the pool; Aida, the social butterfly; and Rob, Jay, and Dan, for fielding foolish questions with trivial answers for several years.

I am lucky to have had friends that made my time (spent both mathematically and not) in San Diego a lot of fun. Thank you Rob, Jay, Dan, Grimm, Fred, Kim, Gautam, Josh, Francesca, Sinan, Corey, Naneh, Shaunak, Christian, Moody, Sankeerth, Molly, Adam, Mariah, BFish, CJ, Anh, Kelly, 10Kem, Weaver, Em, Feeney, Melissa, Vega, Townsend, CWall, Mel, Pierce, Chris, and George.

Finally, I want to thank my family and Lexi for their love, support, and encouragement.

Chapter 2 is a version of material appearing in "Small dense subgraphs of polarity graphs and the extremal number for the 4-cycle, *Australasian Journal of Combinatorics*, 63(1), (2015), 107–114, co-authored with Craig Timmons. The author was the primary investigator and author of this paper.

Chapter 3 is a version of the material appearing in "On the chromatic number of the Erdős-Rényi orthogonal polarity graph", *Electronic Journal of Combinatorics*, P2.21, (2011), 1–19, co-authored with Xing Peng and Craig Timmons. The author was the primary investigator and author of this paper.

Chapter 4 is a version of the material in "Independent sets in polarity graphs", co-authored with Craig Timmons, which has been submitted for publication. The author was the primary investigator and author of this paper.

Chapter 5 is a version of the material appearing in "On sets of integers with restrictions on their products", *European Journal of Combinatorics*, 51, (2016), 268–274, co-authored with Jacques Verstraëte. The author was the primary investigator and author of this paper.

Chapter 6 is a version of the material in "A Szemerédi-Trotter type theorem, sum-product estimates in finite quasifields, and related results", co-authored with Thang Pham, Craig Timmons, and Le Anh Vinh, which has been submitted for publication. The author was one of the primary investigators and authors of this paper.

VITA

2010	B. S. in Mathematics and Economics, University of Delaware
2011	M. S. in Mathematics, University of Delaware
2016	Ph. D. in Mathematics, University of California, San Diego

PUBLICATIONS

Sebastian M. Cioabă and Michael Tait. More Counterexamples to the Alon-Saks-Seymour Conjecture and the Rank-Coloring Conjecture. *The Electronic Journal of Combinatorics*, P26, 1–9, (2011).

Sebastian M. Cioabă and Michael Tait. Variations on a theme of Graham and Pollak. *Discrete Mathematics*, Volume 313, Issue 5, 665 – 676, (2013).

Michael Tait and Craig Timmons. Sidon sets and graphs without 4-cycles. *Journal of Combinatorics*, Volume 5, Issue 2, 155 –165 (2014).

Bob Chen, Jeong Han Kim, Michael Tait, and Jacques Verstraëte. On Coupon Colorings of Graphs. *Discrete Applied Mathematics* 193, 94 – 101, (2015).

Xing Peng, Michael Tait, and Craig Timmons. On the chromatic number of the Erdős-Rényi orthogonal polarity graph. *The Electronic Journal of Combinatorics*, P2.21, 1–19, (2015).

Michael Tait and Craig Timmons. Small dense subgraphs of polarity graphs and the extremal number for the 4-cycle. *The Australasian Journal of Combinatorics*, Volume 63 (1), 107–114, (2015).

Michael Tait and Jacques Verstraëte. On sets of integers with restrictions on their products. *European Journal of Combinatorics* 51, 268 – 274 (2016).

Michael Tait and Craig Timmons. Orthogonal polarity graphs and Sidon sets. To appear in *Journal of Graph Theory*.

ABSTRACT OF THE DISSERTATION

Connections between graph theory, additive combinatorics, and finite incidence geometry

by

Michael Tait

Doctor of Philosophy in Mathematics

University of California San Diego, 2016

Professor Jacques Verstraëte, Chair

This thesis studies problems in extremal graph theory, combinatorial number theory, and finite incidence geometry, and the interplay between these three areas.

The first topic is the study of the Turán number for C_4. Füredi showed that C_4-free graphs with $\mathrm{ex}(n, C_4)$ edges are intimately related to polarity graphs of projective planes. We prove a general theorem about dense subgraphs in a wide class of polarity graphs, and as a result give the best-known lower bounds for $\mathrm{ex}(n, C_4)$ for many values of n. We also study the chromatic and independence numbers of polarity graphs, with special emphasis on the graph ER_q.

Next we study Sidon sets on graphs by considering what sets of integers may look like when certain pairs of them are restricted from having the same product. Other generalizations of Sidon sets are considered as well.

We then use C_4-free graphs to prove theorems related to solvability of equations. Given an algebraic structure R and a subset $A \subset R$, define the *sum set* and *product set* of A to be $A + A = \{a + b : a, b \in A\}$ and $A \cdot A = \{a \cdot b : a, b \in A\}$ respectively. Showing under what conditions at least one of $|A + A|$ or $|A \cdot A|$ is large has a long history of study that continues to the present day. Using spectral properties of the bipartite incidence graph of a projective plane, we deduce that nontrivial sum-product estimates hold in the setting where R is a finite quasifield.

Several related results are obtained.

Finally, we consider a classical question in finite incidence geometry: what is the subplane structure of a projective plane? A conjecture widely attributed to Neumann is that all non-Desarguesian projective planes contain a Fano subplane. By studying the structural properties of polarity graphs of a projective plane, we show that any plane of even order n which admits a polarity such that the corresponding polarity graph has exactly $n+1$ loops must contain a Fano subplane. The number of planes of order up to n which our theorem applies to is not bounded above by any polynomial in n.

1

Introduction

> *"It is often forcefully stated that combinatorics is a collection of problems, which may be interesting in themselves but are not linked and do not constitute a theory."*
>
> – László Lovász, *Combinatorial Problems and Exercises*

This thesis studies the interplay between graph theory, additive combinatorics, and finite incidence geometry. Questions in *extremal graph theory* ask to optimize some graph parameter subject to a constraint. A fundamental question in this area is to maximize the number of edges in a graph or hypergraph which is not allowed to contain fixed forbidden subgraphs. These questions are called *Turán-type problems* and are a cornerstone in extremal combinatorics. Starting from the question of maximizing the number of edges in a C_4-free graph, we branch into the field of *additive combinatorics*. This field, also called *combinatorial number theory*, asks to deduce combinatorial properties of a set when the only information one knows is the size of the set. The use of various graphs coming from projective planes will be central in our study of both areas. We also go the opposite direction and study a question about the subplane structure of a projective plane from the perspective of graph theory.

We now briefly describe the main results given in the thesis. Each chapter will contain its own introduction containing definitions, historical background, and motivation for the problems it contains.

1.1 Polarity graphs and the Turán number for C_4

Given a fixed graph H, the *Turán number of* H is denoted by $\mathrm{ex}(n, H)$ and is the maximum number of edges in a simple n-vertex graph that does not contain H as a subgraph. In Chapter 2, we give the best-known lower bounds on the Turán number $\mathrm{ex}(n, C_4)$ for many values of n by proving a general theorem that guarantees subgraphs in certain polarity graphs that contain many edges.

Estimating Turán numbers of various graphs (or more generally: for various families of hypergraphs) is one of the most important topics in combinatorics, as most questions in extremal combinatorics can be phrased as a Turán problems with the appropriate families of excluded graphs. As such, these problems have a rich history of study (cf [39, 56, 76]), an incomplete version of which is given in the introduction of Chapter 2.

The connection between the Turán number for C_4 and graphs coming from projective planes is well-known. We prove a general theorem, given in Chapter 2, that gives the best-known lower bounds for $\mathrm{ex}(n, C_4)$ for many values of n by manipulating various polarity graphs. One particular case of this theorem gives the following corollary, improving a result of the author and Timmons [80] and disproving a conjecture of Abreu, Balbuena, and Labbate [1].

Theorem. *If q is a prime power, then*

$$\mathrm{ex}(q^2 - q - 2, C_4) \geq \frac{1}{2}q^3 - q^2 + \frac{3}{2}q - O\left(q^{1/2}\right).$$

From here, we study properties of polarity graphs without Turán numbers in mind. One polarity graph of particular interest is the graph ER_q. If q is a prime power, the vertices of ER_q are the one-dimensional subspaces of a three-dimensional vector space over $\mathbb{F}_q$, and two distinct subspaces are adjacent if they are orthogonal to each other. The graph ER_q has been studied in a variety of settings, some of which are described in Chapter 3. In Chapter 3, we study the chromatic number of ER_q. In particular, we prove the following theorem, which is best possible up to the constant 2.

Theorem. *If $q = p^{2r}$ where p is an odd prime and $r \geq 1$ is an integer, then*

$$\chi\left(ER_q\right) \leq 2q^{1/2} + O\left(q^{1/2}/\log q\right).$$

In Chapter 4, we extend this theorem to a more general setting, studying the chromatic and independence numbers of a large family of polarity graphs that includes ER_q.

1.2 Sidon sets and sum-product estimates

Given a monoid R and a subset $A \subset R$, A is called a *Sidon set* if for $a, b, c, d \in A$,

$$a + b = c + d \tag{1.1}$$

implies that $\{a, b\} = \{c, d\}$. Sidon sets and their generalizations have been studied in hundreds of research articles, and some background is given in Chapter 5. We study a generalization of Sidon sets to graphs. A Sidon set is a set where *all* pairs are required to have distinct sums. By introducing a graph, one can prescribe which pairs must have distinct sums. We study this generalization to graphs where R is the integers under multiplication. That is, we are studying sets of integers where prescribed pairs of products must be distinct. A coloring χ of a graph G is called *product-injective* if $\chi(u) \cdot \chi(v) \neq \chi(x) \cdot \chi(y)$ for distinct edges $uv, xy \in E(G)$. Let $P(G)$ denote the smallest integer N such that there is a product-injective coloring $\chi : V(G) \to [N]$. Let $P(n, d)$ represent the maximum possible value of $P(G)$ over all n-vertex graphs G of maximum degree at most d. We prove the following theorem in Chapter 5:

Theorem. *There exists constant $a, b > 0$ such that $P(n, d) \sim n$ if $d \leq n^{1/2}(\log n)^{-a}$ and $P(n, d) \sim n \log n$ if $d \geq n^{1/2}(\log n)^{b}$.*

Sidon sets are sets where the *sum set* $A + A := \{a + b : a, b \in A\}$ is as large as it possibly could be. What if one asks for a set A with a small sum set? If $A \subset \mathbb{Z}$, then if A is an arithmetic progression it has as small a sum set as possible. However, in this case the *product set* of A, $A \cdot A = \{a \cdot b : a, b \in A\}$ is very large. Erdős and Szemerédi showed that in general, if A is a subset of the integers, than either $A + A$ or $A \cdot A$ is large [33]. Heuristically, a set cannot look like both an

arithmetic progression and a geometric progression at the same time. Numerous analogs of this theorem have been proven in other algebraic settings, which we discuss in Chapter 6. We expand this active research area by proving that such a sum-product estimate holds in the setting of a finite quasifield. The takeaway of our theorem is that one does not require associativity of multiplication to have a nontrivial sum-product estimate.

Theorem. *Let Q be a finite quasifield with q elements and $A \subset Q\backslash\{0\}$. There is a positive constant c such that the following hold.*

If $q^{1/2} \ll |A| < q^{2/3}$, then

$$\max\{|A+A|, |A\cdot A|\} \geq c\frac{|A|^2}{q^{1/2}}.$$

If $q^{2/3} \leq |A| \ll q$, then

$$\max\{|A+A|, |A\cdot A|\} \geq c(q|A|)^{1/2}.$$

We prove several results of similar flavor in Chapter 6 concerning the solvability of various equations over a finite quasifield.

1.3 Subplanes of projective planes

A fundamental question in incidence geometry is about the subplane structure of projective planes. There are relatively few results concerning when a projective plane of order k is a subplane of a projective plane of order n. Neumann [67] found Fano subplanes in certain Hall planes, which led to the conjecture that every finite non-Desarguesian plane contains $PG(2,2)$ as a subplane (this conjecture is widely attributed to Neumann, though it does not appear in her work). We prove the following.

Theorem. *Let Π be a finite projective plane of even order which admits an orthogonal polarity. Then Π contains a Fano subplane.*

The number of projective planes of order less than n which our theorem applies to is not bounded above by any polynomial in n.

1.4 Frequently used notation

- **Interval notation:** For real numbers $y \geq x \geq 1$, we use the notation $[x] = \{1, 2, \ldots, \lfloor x \rfloor\}$ and $[x, y] = \{\lfloor x \rfloor, \ldots, \lfloor y \rfloor\}$.

- **Asymptotic notation:** Let f and g be functions $f, g : \mathbb{Z}^+ \to \mathbb{R}$. We write $f = O(g)$ if there exists a constant M and n_0 such that for $n \geq n_0$,

$$f(n) \leq Mg(n).$$

  We write $f = o(g)$ if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 0.$$

  We write $f \sim g$ if

$$\lim_{n\to\infty} \frac{f(n)}{g(n)} = 1.$$

  We write $f = \Omega(g)$ if $g = O(f)$ and $f \ll g$ if $f = o(g)$. We write $f = \Theta(g)$ if $f = O(g)$ and $g = O(f)$.

- **Probabilistic notation:** If $(A_n)_{n\in\mathbb{N}}$ is a sequence of events in a probability space, then we say A_n occurs asymptotically almost surely as $n \to \infty$ if $\lim_{n\to\infty} P(A_n) = 1$. If X is a random variable we write $\mathbb{E}(X)$ for the expectation of X. Let the Erdős-Rényi random graph, $G_{n,p}$, be a graph chosen uniformly from the probability space $\mathcal{G}_{n,p}$ where edges of K_n are present in $G_{n,p}$ independently with probability p.

- **Graph notation:** Let F and G be graphs and $S, T \subset V(G)$. We use $\chi(G)$ and $\alpha(G)$ to denote the chromatic and independence numbers of G respectively. $G[S]$ will denote the graph induced by the set S. $e(S)$ will denote the number of edges induced by S, ie $e(S) = |E(G[S])|$. $e(S, T)$ will denote the number of edges with one endpoint in S and one endpoint in T. $\Delta(G)$ will denote the maximum degree of G. C_4 is the cycle on 4 vertices and ER_q is the Erdős-Rényi orthogonal polarity graph of order $q^2 + q + 1$. The Turán number for F is denoted by $\mathrm{ex}(n, F)$.

- **Algebraic notation:** For q a prime power $\mathbb{F}_q$ denotes the field with q elements and $\mathbb{F}_q^*$ denotes the multiplicative group of $\mathbb{F}_q$. $\mathbb{F}_q^k$ will denote either

the k-fold direct product of $\mathbb{F}_q$ or a k-dimensional vector space over $\mathbb{F}_q$, and the meaning will be clear from context. $\mathbb{F}_q[X]$ denotes the polynomial ring in one indeterminate over $\mathbb{F}_q$.

2

Quadrilateral-free graphs

"Furthermore it is typically easy to verify at least one of the properties in a class, thereby establishing that all the properties in the class hold."

– Fan Chung and Ron Graham [22]

2.1 Introduction

Let F be a graph. Recall that a graph G is said to be *F-free* if G does not contain F as a subgraph, and that $\mathrm{ex}(n, F)$ denotes the *Turán number* of F, which is the maximum number of edges in an n-vertex F-free graph. Write $\mathrm{Ex}(n, F)$ for the family of n-vertex graphs that are F-free and have $\mathrm{ex}(n, F)$ edges. Graphs in the family $\mathrm{Ex}(n, F)$ are called *extremal graphs*. Determining $\mathrm{ex}(n, F)$ for different graphs F is one of the most well-studied problems in extremal graph theory. A case of particular interest is when $F = C_4$, the cycle on four vertices. A well known result of Kővari, Sós, and Turán [57] implies that $\mathrm{ex}(n, C_4) \leq \frac{1}{2}n^{3/2} + \frac{1}{2}n$. Brown [15], and Erdős, Rényi, and Sós [32] proved that $\mathrm{ex}(q^2 + q + 1, C_4) \geq \frac{1}{2}q(q + 1)^2$ whenever q is a power of a prime. It follows that $\mathrm{ex}(n, C_4) = \frac{1}{2}n^{3/2} + o(n^{3/2})$. For more on Turán numbers of bipartite graphs, we recommend the survey of Füredi and Simonovits [39].

The C_4-free graphs constructed in [15] and [32] are examples of *polarity*

graphs. To define these graphs, we introduce some ideas from finite geometry. Let $\mathcal{P}$ and $\mathcal{L}$ be disjoint, finite sets, and let $\mathcal{I} \subset \mathcal{P} \times \mathcal{L}$. We call the triple $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ a *finite geometry*. The elements of $\mathcal{P}$ are called *points*, and the elements of $\mathcal{L}$ are called *lines*. A *polarity* of the geometry is a bijection from $\mathcal{P} \cup \mathcal{L}$ to $\mathcal{P} \cup \mathcal{L}$ that sends points to lines, sends lines to points, is an involution, and respects the incidence structure. Given a finite geometry $(\mathcal{P}, \mathcal{L}, \mathcal{I})$ and a polarity π, the *polarity graph* G_π is the graph with vertex set $V(G_\pi) = \mathcal{P}$ and edge set

$$E(G_\pi) = \{\{p, q\} : p, q \in \mathcal{P}, (p, \pi(q)) \in \mathcal{I}\}.$$

Note that G_π will have loops if there is a point p such that $(p, \pi(p)) \in \mathcal{I}$. Such a point is called an *absolute point*. We will work with polarity graphs that have loops, and graphs obtained from polarity graphs by removing the loops. A case of particular interest is when the geometry is the Desarguesianian projective plane $PG(2, q)$. For a prime power q, this is the plane obtained by considering the one-dimensional subspaces of $\mathbb{F}_q^3$ as points, the two-dimensional subspaces as lines, and incidence is defined by inclusion. A polarity of $PG(2, q)$ is given by sending points and lines to their orthogonal complements. The polarity graph obtained from $PG(2, q)$ with this polarity is often called the *Erdős-Rényi orthogonal polarity graph* and is denoted ER_q. This is the graph that was constructed in [15, 32] and we recommend [8] for a detailed study of this graph. We will study ER_q in more detail in Chapter 3.

The main theorem of the chapter will apply to ER_q as well as to other polarity graphs that come from projective planes that contain an oval. An *oval* in a projective plane of order q is a set of $q+1$ points, no three of which are collinear. It is known that $PG(2, q)$ always contains ovals. One example is the set of $q + 1$ points

$$\{(1, t, t^2) : t \in \mathbb{F}_q\} \cup \{(0, 1, 0)\}$$

which form an oval in $PG(2, q)$. There are also non-Desaurgesian planes that contain ovals. We now state the main theorem of this chapter.

Theorem 2.1.1. *Let Π be a projective plane of order q that contains an oval and has a polarity π. If $m \in \{1, 2, \ldots, q + 1\}$, then the polarity graph G_π contains a*

subgraph on at most $m + \binom{m}{2}$ *vertices that has at least*

$$2\binom{m}{2} + \frac{m^4}{8q} - O\left(\frac{m^4}{q^{3/2}} + m\right)$$

edges.

Theorem 2.1.1 allows us to obtain the best-known lower bounds for $\mathrm{ex}(n, C_4)$ for certain values of n by taking the graph ER_q and removing a small subgraph that has many edges. All of the best lower bounds in the current literature are obtained using this technique (see [1, 35, 80]). An open conjecture of McCuaig is that any graph in $\mathrm{Ex}(n, C_4)$ is an induced subgraph of some orthogonal polarity graph (cf [37]). For $q \geq 15$ a prime power, Füredi [38] proved that any graph in $\mathrm{Ex}(q^2 + q + 1, C_4)$ is an orthogonal polarity graph of some projective plane of order q. For some recent progress on this problem, see [35]. By considering certain induced subgraphs of ER_q, Abreu, Balbuena, and Labbate [1] proved that

$$\mathrm{ex}(q^2 - q - 2, C_4) \geq \frac{1}{2}q^3 - q^2$$

whenever q is a power of 2. They conjectured that this lower bound is best possible. Using Theorem 2.1.1, we answer their conjecture in the negative.

Corollary 2.1.2. *If* q *is a prime power, then*

$$\mathrm{ex}(q^2 - q - 2, C_4) \geq \frac{1}{2}q^3 - q^2 + \frac{3}{2}q - O\left(q^{1/2}\right).$$

Corollary 2.1.2 also improves the main result of [80]. In Section 2.2 we give some necessary background on projective planes and polarity graphs. We prove Theorem 2.1.1 and Corollary 2.1.2 in Section 2.3. We finish this chapter with some concluding remarks in Section 2.4.

2.2 Preliminaries

Let $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be a finite projective plane of order q. A *k-arc* is a set of k points in Π such that no three of the points are collinear. It is known that $k \leq q+1$ when q is odd, and $k \leq q+2$ when q is even. A line $l \in \mathcal{L}$ is called *exterior*,

tangent, or *secant* if it intersects the k-arc in 0, 1, or 2 points, respectively. A k-arc has exactly $\binom{q}{2} + \binom{q+2-k}{2}$ exterior lines, $k(q+2-k)$ tangents, and $\binom{k}{2}$ secants (see [28], page 147). A $(q+1)$-arc is called an *oval* and in the plane $PG(2,q)$, ovals always exist (see [28], Ch 1). The next lemma is known (cf [52], Ch 12). A short proof is included for completeness.

Lemma 2.2.1. *Let G be a polarity graph obtained from a projective plane of order q. If A is the adjacency matrix of G, then the eigenvalues of A are $q+1$ and $\pm\sqrt{q}$.*

Proof. In a projective plane, every pair of points is contained in a unique line. Therefore, in a polarity graph, there is a unique path of length 2 between any pair of vertices (this path may include a loop). This means that $(A^2)_{ij} = 1$ whenever $i \neq j$. Since any point is on exactly $q+1$ lines, every vertex of G has degree exactly $q+1$ where loops add 1 to the degree of a vertex. The diagonal entries of A^2 are all $q+1$ thus,

$$A^2 = J + qI.$$

The eigenvalues of $J + qI$ are $(q+1)^2$ with multiplicity 1, and q with multiplicity $q^2 + q$. □

We remark here that the multiplicity of $q+1$ is 1 and the multiplicities of $\pm\sqrt{q}$ are such that the sum of the eigenvalues is the trace of A, which is the number of absolute points of G. This implies that given two polarity graphs from projective planes of order q, if they have the same number of absolute points, then they are cospectral. Since not all polarity graphs with the same number of absolute points are isomorphic, this gives examples of graphs that are not determined by their spectrum, which may be of independent interest. For more information about determining graphs by their spectrum, see [84].

The next result is a consequence of Lemma 2.2.1 and the so-called Expander Mixing Lemma (cf [3] or [20]). We provide a proof which uses some basic ideas from linear algebra.

Lemma 2.2.2. *Let G be a polarity graph of a projective plane of order q, and let S be a subset of $V(G)$. Let $e(S)$ denote the number of edges in S, possibly including*

loops. Then

$$e(S) \geq \frac{(q+1)|S|^2}{2(q^2+q+1)} - \frac{\sqrt{q}|S|}{2}.$$

Proof. Let A be the adjacency matrix of G and let $n = q^2+q+1$. Let $\{x_i\}$ be an orthonormal set of eigenvectors of A. Since A has constant row sum, $x_1 = \frac{1}{\sqrt{n}}\mathbf{1}$ and $\lambda_1 = q+1$. By Lemma 2.2.1, the other eigenvalues of A are all $\pm\sqrt{q}$.

Now let S be a subset of $V(G)$ and let $\mathbf{1}_S$ be the characteristic vector for S. Let $\hat{e}(S)$ denote the number of non-loop edges of S and $l(S)$ denote the number of loops in S. Then

$$\mathbf{1}_S^T A \mathbf{1}_S = \sum_{i,j \in S} A_{ij} = 2\hat{e}(S) + l(S). \tag{2.1}$$

Next we give a spectral decomposition of $\mathbf{1}_S$:

$$\mathbf{1}_S = \sum_{i=1}^{n} \langle \mathbf{1}_S, x_i \rangle x_i.$$

Noting that $\langle \mathbf{1}_S, x_1 \rangle = \frac{|S|}{\sqrt{n}}$ and expanding (2.1), we see that

$$2\hat{e}(S) + l(S) = \sum_{i=1}^{n} \langle \mathbf{1}_S, x_i \rangle^2 \lambda_i = \frac{(q+1)|S|^2}{n} + \sum_{i=2}^{n} \langle \mathbf{1}_S, x_i \rangle^2 \lambda_i.$$

Therefore,

$$\left| 2\hat{e}(S) + l(S) - \frac{(q+1)|S|^2}{n} \right| \leq \sum_{i=2}^{n} \left| \langle \mathbf{1}_S, x_i \rangle^2 \lambda_i \right| \leq \sqrt{q} \sum_{i=2}^{n} \langle \mathbf{1}_S, x_i \rangle^2 \leq \sqrt{q}|S|.$$

Since $e(S) = \hat{e}(S) + l(S)$ and $l(S) \geq 0$, rearranging gives the result. □

Note that Lemma 2.2.2 does not give us any information when $|S| = O(q)$. Lemma 2.2.2 is not strong enough for our purposes in terms of proving Corollary 2.1.2.

2.3 Proof of Theorem 2.1.1 and Corollary 2.1.2

In this section we prove Theorem 2.1.1 and Corollary 2.1.2.

Proof of Theorem 2.1.1. Let Π be a finite projective plane of order q that contains an oval H. Let π be a polarity of Π and let G be the corresponding polarity graph. We omit the subscript π for notational convenience. For $v \in V(G)$, write $\Gamma(v)$ for the set of neighbors of v in G. Given $S \subset H$, let

$$Y_S = \{v \in V(G) : |\Gamma(v) \cap S| = 2\}$$

and $X_S = Y_S \backslash S$. Since H is an oval, the number of secants to H is $\binom{q+1}{2}$. Thus, for any pair of distinct vertices $s_i, s_j \in H$, there is a unique vertex $t_{i,j} \in Y_H$ such that $t_{i,j}$ is adjacent to both s_i and s_j. The vertex $t_{i,j}$ corresponds to the unique secant that intersects H at s_i and s_j. Further, the only neighbors of $t_{i,j}$ in H are s_i and s_j and so

$$|Y_S| = \binom{|S|}{2}$$

for any $S \subset H$. This implies

$$|S| + |X_S| \geq |Y_S| = \binom{|S|}{2}. \tag{2.2}$$

When $S = H$, we get that $|X_H| \geq \binom{q+1}{2} - (q+1)$ so by Lemma 2.2.2,

$$e(G[X_H]) \geq \frac{q^3}{8} - O(q^{5/2}). \tag{2.3}$$

Let $m \in \{1, 2, \ldots, q+1\}$. Choose $S \subset H$ uniformly at random from the set of all subsets of H of size m. If $e(S, X_S)$ is the number of edges with one endpoint in S and the other in X_S, then using (2.2),

$$e(S, X_S) = 2|X_S| \geq 2\binom{|S|}{2} - 2|S| = 2\binom{m}{2} - 2m. \tag{2.4}$$

If $e = uv \in E(G[X_H])$, then the at most four vertices in $(\Gamma(u) \cap H) \cup (\Gamma(v) \cap H)$ must be chosen in S in order to have $e \in E(G[X_S])$. Therefore,

$$\begin{aligned}\mathbb{P}(e \in E(G[X_S])) \geq \frac{\binom{q-3}{m-4}}{\binom{q+1}{m}} &= \frac{m(m-1)(m-2)(m-3)}{(q+1)q(q-1)(q-2)} \\ &\geq \frac{m(m-1)(m-2)(m-3)}{q^4}.\end{aligned}$$

By (2.3) and linearity of expectation,

$$\mathbb{E}(e(G[X_S])) \geq \frac{m(m-1)(m-2)(m-3)}{8q} - O\left(\frac{m^4}{q^{3/2}}\right). \tag{2.5}$$

Combining (2.4) and (2.5), we see that there is a choice of $S \subset H$ with $|S| = m$ and

$$e(G[S \cup X_S]) \geq 2\binom{m}{2} + \frac{m(m-1)(m-2)(m-3)}{8q} - O\left(\frac{m^4}{q^{3/2}} + m\right).$$

Lastly, observe $|S \cup X_S| \leq |S| + |Y_S| = m + \binom{m}{2}$. □

Now we use Theorem 2.1.1 to prove Corollary 2.1.2. We first prove a simple inequality that expresses the number of edges of an induced subgraph of a polarity graph in terms of the removed set of vertices.

Let G be a polarity graph of a projective plane of order q and let $X \subset V(G)$. The number of edges in the graph $G \setminus X$ is

$$e(G) - e(X) - e(X, X^c)$$

where $e(X)$ includes counting loops in G. Since

$$e(X) + e(X, X^c) = \sum_{x \in X} d(x) - e(X) \leq (q+1)|X| - e(X),$$

we have

$$e(G \setminus X) \geq e(G) - (q+1)|X| + e(X). \tag{2.6}$$

Proof of Corollary 2.1.2. Let q be a prime power and ER_q be the Erdős-Rényi orthogonal polarity graph. It is known that this graph has $\frac{1}{2}q(q+1)^2$ edges. Let m be the largest integer satisfying $m + \binom{m}{2} \leq 2q+3$. Then $m = \lfloor \sqrt{4q + 25/4} - 1/2 \rfloor$ and

$$2\binom{m}{2} + \frac{m(m-1)(m-2)(m-3)}{q^4} = 6q - O(q^{1/2}).$$

By Theorem 2.1.1, there is a set $S \subset V(ER_q)$ with $|S| = m + \binom{m}{2}$ such that S induces a subgraph with at least $6q - O(q^{1/2})$ edges. Let $X = S \cup S'$ where S' is an arbitrarily chosen set of $2q + 3 - |S|$ vertices disjoint from S. Then by (2.6),

$$e(ER_q \setminus X) \geq \frac{1}{2}q(q+1)^3 - (q+1)(2q+3) + 6q - O(q^{1/2}) = \frac{1}{2}q^3 - q^2 + \frac{3}{2}q - O\left(q^{1/2}\right).$$

Since ER_q is C_4-free, we have

$$\mathrm{ex}(q^2 - q - 2, C_4) \geq \frac{1}{2}q^3 - q^2 + \frac{3}{2}q - O\left(q^{1/2}\right).$$

□

2.4 Concluding remarks

There are two special circumstances in which one can improve Theorem 2.1.1. Each indicates the difficulty of finding exact values for the parameter $\mathrm{ex}(n, C_4)$.

- The first situation is when q is a square. In this case, $\mathbb{F}_q$ contains the subfield $\mathbb{F}_{\sqrt{q}}$ and this subfield may be used to find small graphs that contain many edges. For instance ER_q contains a subgraph F that is isomorphic to $ER_{\sqrt{q}}$. One can choose $m = \sqrt{q} + 1$ and let S be the set of absolute points in F. These m vertices will also be absolute points in ER_q and thus are contained in an oval (the absolute points of an orthogonal polarity of $PG(2, q)$ form an oval when q is odd). If we then consider the $\binom{m}{2}$ vertices in Y_S, these will be the vertices in F that are adjacent to the absolute points of F. The set Y_S induces a $\frac{1}{2}(\sqrt{q} - 1)$-regular graph in F (see [8]). The set $X = S \cup Y_S$ will span roughly $\frac{q^{3/2}}{8}$ edges which is much larger than the linear in q lower bound provided by Theorem 2.1.1 when $m = \sqrt{q} + 1$.

- The second situation is when q is a power of 2 and $q - 1$ is prime. Assume that this is the case and consider ER_{q-1}. Let F be a subgraph of ER_{q-1} obtained by deleting three vertices of degree $q - 1$. The number of vertices of F is $(q-1)^2 + (q-1) + 1 - 3 = q^2 - q - 2$, and the number of edges of F is at least $\frac{1}{2}(q-1)q^2 - 3(q-1) = \frac{1}{2}q^3 - \frac{1}{2}q^2 - 3q + 3$. This is better than the result of Corollary 2.1.2 by a factor of about $\frac{1}{2}q^2$. A prime of the form $2^m - 1$ with $m \in \mathbb{N}$ is known as a Mersenne Prime. It has been conjectured that there are infinitely many such primes, but this is a difficult open problem.

In [80], Sidon sets are used to construct C_4-free graphs. For a prime power q, these graphs have $q^2 - 1$ vertices, and $\frac{1}{2}q^3 - q + \frac{1}{2}$ edges when q is odd, and $\frac{1}{2}q^3 - q$ edges when q is even. These graphs have a degree sequence similar to the degree sequence of an orthgonal polarity graph and it seemed possible that these graphs could be extremal. However, Theorem 2.1.1 can be applied to show

$$\mathrm{ex}(q^2 - 1, C_4) \geq \frac{1}{2}q^3 - O(\sqrt{q}),$$

which shows that the graphs constructed in [80] are not extremal.

Chapter 2 is a version of material appearing in "Small dense subgraphs of polarity graphs and the extremal number for the 4-cycle, *Australasian Journal of Combinatorics*, 63(1), (2015), 107–114, co-authored with Craig Timmons. The author was the primary investigator and author of this paper.

3

Coloring ER_q

"Beautiful graphs are rare."

– László Babai and Péter Frankl

3.1 Introduction

In Chapter 2, we gave a geometric description of adjacency in ER_q. We now give an algebraic description that will be more suitable for our purposes in this chapter. Let q be a prime power and let V be a 3-dimensional vector space over $\mathbb{F}_q$. Let $PG(2,q)$ be the projective geometry whose points are the 1-dimensional subspaces of V and whose lines are the 2-dimensional subspaces of V. Recall that ER_q is the graph whose vertices are the points of $PG(2,q)$. Distinct vertices (x_0,x_1,x_2) and (y_0,y_1,y_2) are adjacent if and only if $x_0y_0+x_1y_1+x_2y_2=0$. One obtains an isomorphic graph if the equation for adjacency is $x_2y_0+x_0y_2=x_1y_1$ (see [65]) and it is this definition of ER_q that we will use.

In Chapter 2, we saw that the graph ER_q plays an important role in the study of the Turán number for C_4. Later these same graphs were used to solve other extremal problems in a variety of areas such as Ramsey theory [6, 21, 58], hypergraph Turán theory [60], and even the Cops and Robbers game on graphs [11]. We remark that graphs without short cycles are related to LDPC codes (cf [64]).

Because of its important place in extremal graph theory, many researchers have studied the graph ER_q as an interesting graph in its own right. Parsons [69] determined the automorphism group of ER_q and obtained several other results. In particular, Parsons showed that for $q \equiv 1 (\mathrm{mod}\ 4)$, ER_q contains a $\frac{1}{2}(q+1)$-regular graph on $\binom{q}{2}$ vertices with girth 5. This construction gives one of the best known lower bounds on the maximum number of edges in an n-vertex graph with girth 5. It is still an open problem to determine this maximum, and for more on this problem, see [2]; especially their Conjecture 1.7 and the discussion preceding it. Bachratý and Širáň [8] reproved several of the results of [69] and we recommend [8] for a good introduction to the graph ER_q. They also used ER_q to construct vertex-transitive graphs with diameter two.

Benny Sudakov posed the question of determining the independence number of ER_q (see [90]), and it has since been investigated in several papers. Mubayi and Williford [65] proved that if p is a prime, $n \geq 1$ is an integer, and $q = p^n$, then

$$\alpha(ER_q) \geq \begin{cases} \frac{1}{2}q^{3/2} + \frac{1}{2}q + 1 & \text{if } p \text{ is odd and } n \text{ is even,} \\ \frac{120q^{3/2}}{73\sqrt{73}} & \text{if } p \text{ is odd and } n \text{ is odd,} \\ \frac{q^{3/2}}{2\sqrt{2}} & \text{if } p = 2 \text{ and } n \text{ is odd,} \\ q^{3/2} - q + q^{1/2} & \text{if } p = 2 \text{ and } n \text{ is even.} \end{cases}$$

An upper bound on the independence number of ER_q may be obtained by eigenvalue techniques by the well-known Hoffman Ratio Bound.

Theorem 3.1.1 (Hoffman [50])**.** *Let G be a d-regular graph on n vertices and λ_n be the smallest eigenvalue of its adjacency matrix. Then*

$$\alpha(G) \leq n\frac{-\lambda_n}{d - \lambda_n}.$$

As the graph ER_q with loops on the absolute points is regular, Hoffman's theorem may be applied to obtain $\alpha(ER_q) \leq q^{3/2} + q^{1/2} + 1$. Therefore, the order of magnitude of $\alpha(ER_q)$ is $q^{3/2}$. Godsil and Newman refined the upper bound obtained from Hoffman's bound in [42]. Their result was then improved using the Lovász theta function in [26]. When q is even, Hobart and Williford [49] used coherent configurations to provide upper bounds for the independence number of

general orthogonal polarity graphs. When q is an even square, the known upper bound and lower bound for $\alpha(ER_q)$ differ by at most 1. In the case when p is odd or when $p = 2$ and n is odd, it is still an open problem to determine an asymptotic formula for $\alpha(ER_q)$.

Since the independence number has been well-studied and its order of magnitude is known, it is natural to investigate the chromatic number of ER_q which is closely related to $\alpha(ER_q)$. Let q be any prime power. Then ER_q has q^2+q+1 vertices and $\alpha(ER_q) = \Theta(q^{3/2})$, and so a lower bound for $\chi(ER_q)$ is $\frac{q^2+q+1}{\alpha(ER_q)} \geq q^{1/2}$. One may ask whether this lower bound actually gives the right order of magnitude of $\chi(ER_q)$. We confirm this for q being an even power of an odd prime.

Theorem 3.1.2. *If $q = p^{2r}$ where p is an odd prime and $r \geq 1$ is an integer, then*

$$\chi(ER_q) \leq 2q^{1/2} + O\left(q^{1/2}/\log q\right).$$

This upper bound is within a factor of 2 of the lower bound $\chi(ER_q) \geq \frac{q^2+q+1}{\alpha(ER_q)} \geq q^{1/2}$. Any improvement in the coefficient of $q^{1/2}$ would give an improvement to the best known lower bound on the independence number of ER_q from [65]. The lower order term $O(q^{1/2}/\log q)$ is obtained using probabilistic methods [5] and while the implied constant is absolute, we have not made an effort to compute it. By using Brooks' Theorem instead of the result of [5], we obtain the upper bound $\chi(ER_q) \leq 4q^{1/2} + 1$ for all $q = p^{2r}$ where $r \geq 1$ is an integer and p is an odd prime.

When q is not an even power, we first prove the following general theorem.

Theorem 3.1.3. *Let q be an odd power of an odd prime and let $r \geq 1$ be an integer. If there is a $\mu \in \mathbb{F}_q$ such that $x^{2r+1} - \mu$ is irreducible in $\mathbb{F}_q[x]$, then*

$$\chi(ER_{q^{2r+1}}) \leq \frac{2r+5}{3} q^{\frac{4r}{3}+1} + (2r+1)q^{r+1} + 1.$$

Given an odd integer $2r + 1 \geq 3$, there are infinitely many primes p for which there is a $\mu \in \mathbb{F}_q$ such that $x^{2r+1} - \mu \in \mathbb{F}_q[x]$ is irreducible (see Section 3.5 for more details), where q is an arbitrary odd power of p. Our method can also be used to prove that if q is a power of any odd prime, then

$$\chi(ER_{q^3}) \leq 6q^2 + 1.$$

Here we do not need the existence of an irreducible polynomial $x^3 - \mu \in \mathbb{F}_q[x]$.

For q an odd power of an odd prime, we have the following corollary.

Corollary 3.1.4. *Let $q = p^s$ for an odd prime p and an odd integer $s \geq 3$. If $t > 1$ is the smallest divisor of s such that $x^t - \mu$ is irreducible in $\mathbb{F}_{p^{s/t}}[x]$ for some $\mu \in \mathbb{F}_{p^{s/t}}$, then*

$$\chi(ER_q) \leq \frac{t+4}{3} p^{s(2t+1)/3t} + tp^{(t+1)/2} + 1.$$

We encountered difficulties in extending this upper bound to the general case. In particular, when p is a prime, we have not been able to improve the upper bound $\chi(ER_p) = O(p/\log p)$ which is obtained by applying the main result of [5].

Conjecture 3.1.5. *Let p be an odd prime. For any integer $r \geq 0$,*

$$\chi(ER_{p^{2r+1}}) = O(p^{r+1/2}).$$

Instead of working with ER_q, we work with a related graph that is a bit more suitable for our computations.

Definition 3.1.6. *Let q be a power of an odd prime and $A = \{(a, a^2) : a \in \mathbb{F}_q\}$. Let G_q be the graph with vertex set $\mathbb{F}_q \times \mathbb{F}_q$, and distinct vertices (x_1, x_2) and (y_1, y_2) are adjacent if and only if*

$$(x_1, x_2) + (y_1, y_2) \in A.$$

Let G_q° be the graph obtained from G_q by adding loops to all vertices (x_1, x_2) for which $(x_1, x_2) + (x_1, x_2) \in A$. Vinh [87] proved that the graph G_q° is a $(q^2, q, \sqrt{2q})$-graph. Recall an (n, d, λ) graph is an n-vertex d-regular graph whose second eigenvalue $\max\{|\lambda_2|, |\lambda_n|\}$ is at most λ. Vinh used the fact that G_q° is a $(q^2, q, \sqrt{2q})$-graph to count solutions to $x_1 + x_2 = (x_3 + x_4)^2$ where $(x_1, x_3) \subset B$, $(x_2, x_4) \subset C$, and $B, C \subset \mathbb{F}_q^2$. For similar results that are obtained using techniques from combinatorial number theory, see [24]. We prove that G_q is isomorphic to an induced subgraph of the Erdős-Rényi orthogonal polarity graph.

Theorem 3.1.7. *If q is a power of an odd prime, then the graph G_q is isomorphic to an induced subgraph of ER_q.*

In the course of proving Theorem 3.1.7 we will show how to obtain ER_q from G_q by adding vertices and edges to G_q. This will allow us to translate upper bounds on $\chi(G_q)$ to upper bounds on $\chi(ER_q)$.

In addition to finding a proper coloring of ER_q, we also investigate proper colorings of small subgraphs of ER_q. In particular, we obtain the following result concerning small subgraphs of ER_q that are not 3-colorable.

Theorem 3.1.8. *If q is sufficiently large, then ER_q contains a subgraph H with at most 36 vertices and $\chi(H) \geq 4$.*

Let $\mathcal{C}^r$ be the family of graphs with chromatic number r, and $\mathcal{C}^r_k$ be the family of graphs with at most k vertices and chromatic number r. Theorem 3.1.8 is motivated by the following problem of Allen, Keevash, Sudakov, and Verstraëte [2].

Problem 3.1.9 (Allen, et al. [2])**.** *Let $\mathcal{F}$ be a family of bipartite graphs. Determine if there is an integer k such that*

$$\mathrm{ex}(n, \mathcal{F} \cup \mathcal{C}^r_k) \sim \mathrm{ex}(n, \mathcal{F} \cup \mathcal{C}^r).$$

When considering Problem 3.1.9, a question that arises is if every extremal $\mathcal{F}$-free n-vertex graph (here n is tending to infinity) must contain some member of $\mathcal{C}^r_k$? In other words, does forbidding $\mathcal{C}^r_k$ actually have an effect on extremal $\mathcal{F}$-free graphs. By Theorem 3.1.8, one cannot take ER_q to obtain a lower bound on the Turán number $\mathrm{ex}(n, \{C_4\} \cup \mathcal{C}^3_k)$ for $k \geq 36$ without modifying ER_q in some way. It seems likely that for any integer $r \geq 5$, there exists integers q_r and $f(r)$ such that for any $q \geq q_r$, the graph ER_q contains a subgraph with at most $f(r)$ vertices and chromatic number at least r.

In Section 3.2 we prove Theorem 3.1.7. In Section 3.3 we prove Theorems 3.1.2 and 3.1.3. In Section 3.4 we prove Theorem 3.1.8. Section 3.5 contains some concluding remarks.

3.2 Proof of Theorem 3.1.7

Let q be a power of an odd prime power and $A = \{(a, a^2) : a \in \mathbb{F}_q\}$. Let $\mathbb{F}_q = \{b_1, \ldots, b_q\}$ and assume that $b_q = 0$. Let $F = \{b_q\} \times \mathbb{F}_q$. Then F is a subgroup of $\mathbb{F}_q^2$ and we let

$$F_i = F + (b_i, 0)$$

be the cosets of F where $F_q = F$. Add new vertices $z_1, \ldots, z_q, y$ to G_q. Make z_i adjacent to all vertices in F_i, and make y adjacent to each z_i. Call this graph H_q. Observe that G_q is an induced subgraph of H_q. We define an isomorphism ϕ from H_q to ER_q as follows.

1. For any $b_j \in \mathbb{F}_q$, let $\phi((0, b_j)) = (1, 0, 2^{-1}b_j)$.
2. For any $b_i, b_j \in \mathbb{F}_q$ with $b_i \neq 0$, let $\phi((b_i, b_j)) = (1, b_i, 2^{-1}(b_j - b_i^2))$.
3. Let $\phi(y) = (0, 0, 1)$ and $\phi(z_i) = (0, 1, b_i)$ for $1 \leq i \leq q$.

We will show that ϕ is an isomorphism by considering the different types of vertices in H_q. Recall that the rule for adjacency in ER_q is that (x_0, x_1, x_2) is adjacent to (y_0, y_1, y_2) if and only if $x_0y_2 + x_2y_0 = x_1y_1$.

Case 1: Vertices of type $(0, b_j)$.

Let $b_j \in \mathbb{F}_q$. In H_q, the neighborhood of $(0, b_j)$ is $\{z_q\} \cup \{(x, x^2 - b_j) : x \in \mathbb{F}_q\}$. In ER_q, the neighborhood of $(1, 0, 2^{-1}b_j)$ is

$$\{(0, 1, 0)\} \cup \{(1, x, -2^{-1}b_j) : x \in \mathbb{F}_q\}. \tag{3.1}$$

By definition, $\phi((0, -b_j)) = (1, 0, -2^{-1}b_j)$ and for $x \neq 0$,

$$\phi((x, x^2 - b_j)) = (1, x, 2^{-1}(x^2 - b_j - x^2)) = (1, x, -2^{-1}b_j).$$

This shows that (3.1) coincides with the set

$$\{\phi(z_q)\} \cup \{\phi((x, x^2 - b_j)) : x \in \mathbb{F}_q\}.$$

We conclude that for any $b_j \in \mathbb{F}_q$, $(0, b_j)$ is adjacent to u in H_q if and only if $\phi((0, b_j))$ is adjacent to $\phi(u)$ in ER_q.

Case 2: Vertices of type (b_i, b_j) with $b_i \neq 0$.

Let $b_i, b_j \in \mathbb{F}_q$ with $b_i \neq 0$. In H_q, the neighborhood of (b_i, b_j) is

$$\{z_i\} \cup \{(x - b_i, x^2 - b_j) : x \in \mathbb{F}_q\}.$$

In ER_q, the neighborhood of $(1, b_i, 2^{-1}(b_j - b_i^2))$ is

$$\{(0, 1, b_i)\} \cup \{(1, x, xb_i - 2^{-1}(b_j - b_i^2)) : x \in \mathbb{F}_q\}. \tag{3.2}$$

We have $\phi(z_i) = (0, 1, b_i)$ and

$$\phi((b_i - b_i, b_i^2 - b_j)) = (1, 0, -2^{-1}(b_j - b_i^2)).$$

For $y \neq b_i$,

$$\begin{aligned} \phi((y - b_i, y^2 - b_j)) &= (1, y - b_i, 2^{-1}(y^2 - b_j - (y - b_i)^2)) \\ &= (1, y - b_i, yb_i - 2^{-1}(b_j + b_i^2)). \end{aligned}$$

If we take $x = y - b_i$ in (3.2), we obtain

$$(1, y - b_i, yb_i - 2^{-1}(b_j + b_i^2))$$

using the fact that $2^{-1} - 1 = -2^{-1}$. We conclude that for any $b_i, b_j \in \mathbb{F}_q$ with $b_i \neq 0$, (b_i, b_j) is adjacent to u in H_q if and only if $\phi((b_i, b_j))$ is adjacent to $\phi(u)$ in ER_q.

Case 3: Vertices of type z_i.

Let $1 \leq i \leq q$ and consider z_i. The neighborhood of z_i is $\{y\} \cup \{(b_i, x) : x \in \mathbb{F}_q\}$. In ER_q, the neighborhood of $(0, 1, b_i)$ is

$$\{(0, 0, 1)\} \cup \{(1, b_i, x) : x \in \mathbb{F}_q\} = \{\phi(y)\} \cup \{(1, b_i, x) : x \in \mathbb{F}_q\}.$$

If $i = q$, then $\phi((0, y)) = (1, 0, 2^{-1}y)$. If $i \neq q$, then $\phi((b_i, y)) = (1, b_i, 2^{-1}(y - b_i^2))$. As y ranges over $\mathbb{F}_q$, we obtain $(1, b_i, x)$ for all $x \in \mathbb{F}_q$.

We have not checked the neighborhood condition for $y \in V(H_q)$ but since we have considered all other vertices, this is not necessary.

3.3 Proof of Theorems 3.1.2 and 3.1.3

Throughout this section p is an odd prime and q is a power of p. The set $\mathbb{F}_q^*$ consisting of the nonzero elements of $\mathbb{F}_q$ can be partitioned into two sets $\mathbb{F}_q^+$ and $\mathbb{F}_q^-$ where

$$a \in \mathbb{F}_q^+ \text{ if and only if } -a \in \mathbb{F}_q^-.$$

Observe that the vertices (x_1, x_2) and (y_1, y_2) are adjacent in G_q if and only if $x_1 + y_1 = a$ and $x_2 + y_2 = a^2$ for some $a \in \mathbb{F}_q$. This is equivalent to $(x_1 + y_1)^2 = x_2 + y_2$. It is often this relation that we will use in our calculations.

Lemma 3.3.1. *(i) If $\mathbb{F}_{q^2} = \{a\theta + b : a, b \in \mathbb{F}_q\}$ for some $\theta \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q$, then both*

$$\{(x, y\theta + z) : x, z \in \mathbb{F}_q, y \in \mathbb{F}_q^+\} \text{ and } \{(x, y\theta + z) : x, z \in \mathbb{F}_q, y \in \mathbb{F}_q^-\}$$

are independent sets in G_q.
(ii) If $t \geq 3$ is odd and $\mathbb{F}_{q^t} = \{a_0 + \cdots + a_{t-1}\theta^{t-1} : a_i \in \mathbb{F}_q\}$ for some $\theta \in \mathbb{F}_{q^t}$, then both

$$\{(x_0 + \cdots + x_{(t-3)/2}\theta^{\frac{t-3}{2}}, y_0 + \cdots + y_{t-1}) : x_i, y_j \in \mathbb{F}_q, y_{t-1} \in \mathbb{F}_q^+\}$$

and

$$\{(x_0 + \cdots + x_{(t-3)/2}\theta^{\frac{t-3}{2}}, y_0 + \cdots + y_{t-1}) : x_i, y_j \in \mathbb{F}_q, y_{t-1} \in \mathbb{F}_q^-\}$$

are independent sets in G_q.

Proof. We prove the first case of (i) as the proofs of the remaining statements are very similar. Suppose $(x_1, y_1\theta + z_1)$ and $(x_2, y_2\theta + z_2)$ are vertices in G_q with $x_1, x_2, z_1, z_2 \in \mathbb{F}_q$ and $y_1, y_2 \in \mathbb{F}_q^+$. Then $(x_1+x_2)^2 \in \mathbb{F}_q$ but $(y_1+y_2)\theta+(z_1+z_2) \notin \mathbb{F}_q$ since $y_1 + y_2 \neq 0$. Therefore, the vertices $(x_1, y_1\theta + z_1)$ and $(x_2, y_2\theta + z_2)$ are not adjacent. □

Lemma 3.3.2. *For any $k \in \mathbb{F}_q^*$, the maps $\psi_k, \phi_k : V(G_q) \to V(G_q)$ given by*

$$\psi_k((x, y)) = (x + k, y + 4kx + 2k^2) \text{ and } \phi_k((x, y)) = (kx, k^2y)$$

are automorphisms of G_q.

Proof. Let $k \in \mathbb{F}_q^*$. Suppose (x_1, x_2) is adjacent to (y_1, y_2) so that $(x_1 + y_1)^2 = x_2 + y_2$. In this case,

$$\begin{aligned}(x_1 + k + y_1 + k)^2 &= (x_1 + y_1)^2 + 4kx_1 + 4ky_1 + 4k^2 \\ &= (x_2 + 4kx_1 + 2k^2) + (y_2 + 4ky_1 + 2k^2).\end{aligned}$$

This shows that $(x_1 + k, x_2 + 4kx_1 + 2k^2)$ is adjacent to $(y_1 + k, y_2 + 4ky_1 + 2k^2)$. Conversely, if $(x_1 + k, x_2 + 4kx_1 + 2k^2)$ is adjacent to $(y_1 + k, y_2 + 4ky_1 + 2k^2)$, then it must be the case that $(x_1 + y_1)^2 = x_2 + y_2$ and so (x_1, y_1) is adjacent to (x_2, y_2).

To show that ϕ_k is an isomorphism it is enough to observe that $(x_1 + y_1)^2 = x_2 + y_2$ is equivalent to $(kx_1 + ky_1)^2 = k^2x_2 + k^2y_2$. □

3.3.1 q a square

In this subsection we prove the following.

Theorem 3.3.3. *Let q be a power of an odd prime. The chromatic number of G_{q^2} satisfies*

$$\chi(G_{q^2}) \leq 2q + O(q/\log q).$$

Proof. Let θ be a root of an irreducible quadratic polynomial in $\mathbb{F}_q[x]$ so that $\mathbb{F}_{q^2} = \{a\theta + b : a, b, \in \mathbb{F}_q\}$. Assume that $\theta^2 = \mu_1\theta + \mu_0$ where $\mu_0, \mu_1 \in \mathbb{F}_q$. Let $I^+ = \{(x, y\theta + z) : x, z \in \mathbb{F}_q, y \in \mathbb{F}_q^+\}$, $I^- = \{(x, y\theta + z) : x, z \in \mathbb{F}_q, y \in \mathbb{F}_q^-\}$, and $J = I^+ \cup I^-$. By Lemma 3.3.1, J is the union of two independent sets and so $\chi(G_{q^2}[J]) \leq 2$. Let

$$S = \bigcup_{k \in \mathbb{F}_q} \psi_{k\theta}(J).$$

By Lemma 3.3.2, each $\psi_{k\theta}$ is an isomorphism and so $\chi(G_{q^2}[S]) \leq 2q$. Let $X = V(G_{q^2}) \backslash S$. Since $\mathbb{F}_q^+ \cup \mathbb{F}_q^- = \mathbb{F}_q^*$, we can write

$$S = \{(x + k\theta, y\theta + z + 4k\theta x + 2k^2\theta^2) : x, k, y, z \in \mathbb{F}_q, y \neq 0\}.$$

Given a vertex $(s, t) \in V(G_{q^2})$, say with $s = s_0 + s_1\theta$ and $t = t_0 + t_1\theta$, we can take $x = s_0$ and $k = s_1$ to obtain

$$\{(s_0 + s_1\theta, y\theta + z + 4s_1s_0\theta + 2s_1^2(\mu_1\theta + \mu_0)) : y, z \in \mathbb{F}_q, y \neq 0\} \subset S.$$

The second coordinate in the above subset of S simplifies to

$$(z + 2s_1^2\mu_0) + (y + 4s_1s_0 + 2s_1^2\mu_1)\theta.$$

We can choose $z = t_0 - 2s_1^2\mu_0$ and as long as $t_1 \neq 4s_1s_0 + 2s_1^2\mu_1$, we can take $y = t_1 - 4s_1s_0 - 2s_1^2\mu_1$. Otherwise, $t_1 = 4s_1s_0 + 2s_1^2\mu_1$ and so

$$X = \{(s_0 + s_1\theta, t_0 + (4s_1s_0 + 2s_1^2\mu_1)\theta) : s_0, s_1, t_0 \in \mathbb{F}_q\}.$$

Partition X into q sets X_s where $s \in \mathbb{F}_q$ and

$$X_s = \{(s\theta + s_2, (2s^2\mu_1 + 4ss_2)\theta + t_2 : s_2, t_2 \in \mathbb{F}_q\}.$$

Claim 1: For any $s \in \mathbb{F}_q$, $\Delta(G_{q^2}[X_s]) \leq q$.

Let $s \in \mathbb{F}_q$. A pair of vertices

$$(s\theta + s_2, (2s^2\mu_1 + 4ss_2)\theta + t_2) \text{ and } (s\theta + u_2, (2s^2\mu_1 + 4su_2)\theta + v_2),$$

both in X_s, are adjacent if and only if $4s^2\mu_2 + (s_2 + u_2)^2 = t_2 + v_2$. If s_2 and t_2 are fixed, then there are q choices for u_2 and once u_2 is fixed, v_2 is determined. Therefore, the maximum degree of $G_{q^2}[X_s]$ is q.

Claim 2: $\Delta(G_{q^2}[X]) \leq 2q - 1$.

By Claim 1, a vertex in X_s has at most q other neighbors in X_s. Let $s, t \in \mathbb{F}_q$ where $s \neq t$. The vertex $(s\theta + s_2, (2s^2\mu_1 + 4ss_2)\theta + t_2) \in X_s$ is adjacent to the vertex $(t\theta + u_2, (2t^2\mu_1 + 4tu_2)\theta + v_2) \in X_t$ if and only if

$$\mu_1(s^2 + 2st + t^2) + 2(s + t)s_2 + 2(s + t)u_2 = \mu_1(2s^2 + 2t^2) + 4ss_2 + 4tu_2 \quad (3.3)$$

and

$$(s + t)^2\mu_0 + (s_2 + u_2)^2 = t_2 + v_2. \quad (3.4)$$

Equation (3.3) can be rewritten as

$$\mu_1(s - t)^2 = 2(t - s)s_2 + 2(s - t)u_2. \quad (3.5)$$

Thus if s_2 and t_2 are fixed, then (3.5) and (3.4) determine u_2 and v_2 since $2(s-t) \neq 0$. This shows that a vertex in X_s has exactly one neighbor in X_t whenever $s \neq t$. Namely, given the vertex $(s\theta + s_2, (2s^2\mu_1 + 4ss_2)\theta + t_2) \in X_s$, its unique neighbor in X_t where $t \neq s$ is $(t\theta + u_2, (2t^2\mu_1 + 4tu_2)\theta + v_2)$ where

$$u_2 = 2^{-1}\mu_1(s-t) + s_2 \text{ and } v_2 = (s+t)^2\mu_0 + (2s_2 + 2^{-1}\mu_1(s-t))^2 - t_2.$$

We conclude that a vertex $x \in X$ has at most q neighbors in X_s when $x \in X_s$, and one neighbor in each X_t for $t \neq s$. Since $X = \cup_{s\in\mathbb{F}_q} X_s$, we have proved Claim 2.

Alon, Krivelevich, and Sudakov [5] proved that any graph with maximum degree d with the property that the neighborhood of every vertex contains at most d^2/f edges has chromatic number at most $c(d/\log f)$ where c is an absolute constant. A C_4-free graph with maximum degree d has the property that the neighborhood of every vertex contains at most $d/2$ edges. Applying the result of [5] to $G_{q^2}[X]$, we obtain $\chi(G_{q^2}[X]) = O(q/\log q)$. Combining this coloring with our coloring of S, we obtain a proper coloring of G_{q^2} with $2q + O(q/\log q)$ colors. □

To obtain a coloring of $ER_{q^2} \cong H_{q^2}$, we only need one additional color for the vertices $z_1, \ldots, z_{q^2}, y$. The vertices $z_1, \ldots, z_{q^2}$ form an independent set in H_{q^2} and so we use one new color on these vertices. The vertex y has no neighbors in G_{q^2} and so we may use any one of the $2q + O(q/\log q)$ colors used to G_{q^2} to color y. This proves Theorem 3.1.2.

3.3.2 q not a square

In this subsection we prove the following result.

Theorem 3.3.4. *Let q be a power of an odd prime. If $r \geq 1$ and for some $\mu \in \mathbb{F}_q$, the polynomial $x^{2r+1} - \mu \in \mathbb{F}_q[x]$ is irreducible, then*

$$\chi(G_{q^t}) \leq \frac{2r+5}{3} q^{\frac{4r}{3}+1} + (2r+1)q^{r+1}.$$

Proof. Suppose there is a $\mu \in \mathbb{F}_q^*$ such that the polynomial $x^t - \mu \in \mathbb{F}_q[x]$ is irreducible. Let θ be a root of $x^t - \mu$ in an extension field of $\mathbb{F}_q$. We may view θ as an element of $\mathbb{F}_{q^t}$ and $\{1, \theta, \ldots, \theta^{2r}\}$ is a basis for $\mathbb{F}_{q^t}$ over $\mathbb{F}_q$. For $2r+1 \leq l \leq 6r+3$,

$$\theta^l = \begin{cases} \mu\theta^{l-2r-1} & \text{if } 2r+1 \leq l < 4r+2, \\ \mu^2\theta^{l-4r-2} & \text{if } 4r+2 \leq l < 6r+3. \end{cases}$$

This identity will be used frequently throughout this subsection. Define

$$I^+ = \{(x_0 + x_1\theta + \cdots + x_{r-1}\theta^{r-1}, y_0 + \cdots + y_{2r}\theta^{2r}) : x_i, y_j \in \mathbb{F}_q, y_{2r} \in \mathbb{F}_q^+\}$$

and

$$I^- = \{(x_0 + x_1\theta + \cdots + x_{r-1}\theta^{r-1}, y_0 + \cdots + y_{2r}\theta^{2r}) : x_i, y_j \in \mathbb{F}_q, y_{2r} \in \mathbb{F}_q^-\}.$$

By Lemma 3.3.1, both I^+ and I^- are independent sets. Let $J = I^+ \cup I^-$. Since J is the union of two independent sets, $\chi(G_{q^t}[J]) \leq 2$. For $k \in \mathbb{F}_{q^t}$, the map $\psi_k((x, y)) = (x + k, y + 4kx + 2k^2)$ is an isomorphism of G_{q^t} by Lemma 3.3.2. Let

$$S = \bigcup_{(x_r,\ldots,x_{2r}) \in \mathbb{F}_q^{r+1}} \psi_{x_r\theta^r + \cdots + x_{2r}\theta^{2r}}(J).$$

We properly color the vertices of S with at most $2q^{r+1}$ colors. Let $X = \mathbb{F}_{q^t}^2 \backslash S$. It remains to color the vertices in X. To do this, we will proceed as follows. By Lemma 3.3.2, for any $k \in \mathbb{F}_{q^t}^*$, the map $\phi_k((x, y)) = (kx, k^2y)$ is an isomorphism of G_{q^t}. Let $1 \leq l \leq 2r$ and consider $\phi_{\theta^l}(X)$. Let $Y_l = S \cap \phi_{\theta^l}(X)$. The graph $G_{q^t}[Y_l]$ is isomorphic to a subgraph of $G_{q^t}[S]$. We have shown that $\chi(G_{q^t}[S]) \leq 2q^{r+1}$ and so $\chi(G_{q^t}[Y_l]) \leq 2q^{r+1}$ for any $1 \leq l \leq 2r$. Therefore, we can properly color the vertices in

$$\phi_{\theta^l}^{-1}(Y_l) = \phi_{\theta^l}^{-1}(S) \cap X$$

with at most $2q^{r+1}$ colors. This gives a proper coloring that uses at most $(2r + 1)2q^{r+1}$ colors. The only vertices that have not been colored are those that are in the set

$$Z := X \cap \phi_\theta(X) \cap \phi_{\theta^2}(X) \cap \cdots \cap \phi_{\theta^{2r}}(X).$$

We are now going to show that if $(s_0 + \cdots + s_{2r}\theta^{2r}, t_0 + \cdots + t_{2r}\theta^{2r}) \in Z$, then each t_i is determined by $s_0, \ldots, s_{2r}$. This will allow us to prove an upper bound on the maximum degree of $G_{q^t}[Z]$ and we can then color $G_{q^t}[Z]$ by applying Brooks' Theorem.

We will use the following notation for the rest of this subsection. If $s \in \mathbb{F}_{q^t}$, then $s_0, \ldots, s_{2r}$ will be the coefficients of s in the unique representation $s = s_0 + s_1\theta + \cdots + s_{2r}\theta^{2r}$ where $s_i \in \mathbb{F}_q$. Given a $2r + 1$-tuple $(z_0, z_1, \ldots, z_{2r}) \in \mathbb{F}_q^{2r+1}$, define

$$\alpha(z_0, z_1, \ldots, z_{2r}) = 2z_r^2 + 4\sum_{j=0}^{r-1} z_j z_{2r-j}.$$

Claim 1: If $(s_0 + \cdots + s_{2r}\theta^{2r}, t_0 + \cdots + t_{2r}\theta^{2r}) \in X$, then

$$t_{2r} = \alpha(s_0, s_1, \ldots, s_{2r}).$$

Proof of Claim 1. A vertex in S is of the form

$$(x_0 + \cdots + x_{r-1}\theta^{r-1} + x_r\theta^r + \cdots + x_{2r}\theta^{2r}, y_0 + \cdots + y_{2r}\theta^{2r} \\ +4(x_r\theta^r + \cdots + x_{2r}\theta^{2r})(x_0 + \cdots + x_{r-1}\theta^{r-1}) + 2(x_r\theta^r + \cdots + x_{2r}\theta^{2r})^2)$$

for some $x_i, y_j \in \mathbb{F}_q$, and $y_{2r} \in \mathbb{F}_q^+ \cup \mathbb{F}_q^- = \mathbb{F}_q^*$. The coefficient of θ^{2r} in the second coordinate is

$$y_{2r} + 2x_r^2 + 4\sum_{j=0}^{r-1} x_j x_{2r-j}.$$

Thus, given any vertex $(s,t) \in \mathbb{F}_{q^t}^2$, we have that $(s,t) \in S$ unless

$$t_{2r} = 2s_r^2 + \sum_{j=0}^{r-1} s_j s_{2r-j}.$$

□

Claim 2: If $1 \leq l \leq 2r$ and $(s,t) \in X \cap \phi_{\theta^l}(X)$, then

$$t_{2l-1} = \mu\alpha(s_l, s_{l+1}, \ldots, s_{2r}, \mu^{-1}s_0, \ldots, \mu^{-1}s_{l-1}) \text{ if } 1 \leq l \leq r,$$

and

$$t_{2l-2r-2} = \mu^2\alpha(s_l, s_{l+1}, \ldots, s_{2r}, \mu^{-1}s_0, \ldots, \mu^{-1}s_{l-1}) \text{ if } r+1 \leq l \leq 2r.$$

Proof of Claim 2. Suppose $(s,t) \in X \cap \phi_{\theta^l}(X)$. There is an $(x,y) \in X$ such that $(s,t) = \phi_{\theta^l}((x,y))$. From the equation $(s,t) = (\theta^l x, \theta^{2l} y)$ we obtain by equating coefficients of $\theta^0, \theta^1, \ldots, \theta^{2r}$ in the first component,

$$x_i = s_{l+i} \text{ for } 0 \leq i \leq 2r-l \text{ and } \mu x_i = s_{i-2r+l-1} \text{ for } 2r-l+1 \leq i \leq 2r. \quad (3.6)$$

If $1 \leq l \leq r$, then we obtain $t_{2l-1} = \mu y_{2r}$ by considering the coefficient of θ^{2l-1} in the second component. Similarly, if $r+1 \leq l \leq 2r$, we obtain $t_{2l-2r-2} = \mu^2 y_{2r}$ by

considering the coefficient of $\theta^{2l-2r-2}$ in the second component. Since $(x, y) \in X$, we have by Claim 1 that

$$y_{2r} = \alpha(x_0, x_1, \ldots, x_{2r}). \tag{3.7}$$

Using (3.6), we can solve for the x_i's in terms of the s_j's and then substitute into (3.7) to complete the proof of Claim 2. □

For $0 \leq k \leq 2r$, let

$$U_k = \{\{i, j\} \subset \{0, 1, \ldots, 2r\} : i + j \equiv k (\text{mod } 2r + 1)\}.$$

Given $\{i, j\} \subset \{0, 1, \ldots, 2r\}$, let

$$\mu_{\{i,j\}} = \begin{cases} 1 & \text{if } 1 \leq i + j \leq 2r, \\ \mu & \text{if } 2r + 1 \leq i + j \leq 4r - 1. \end{cases}$$

Claim 3: Suppose $(s, t) \in Z$. If $1 \leq l \leq r$, then

$$t_{2l-1} = 2\mu s_{l+r}^2 + 4 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}} s_i s_j.$$

If $0 \leq l \leq r - 1$, then

$$t_{2l} = 2s_l^2 + 4 \sum_{\{i,j\} \in U_{2l}} \mu_{\{i,j\}} s_i s_j.$$

Proof of Claim 3. First suppose $1 \leq l \leq r$. By Claim 2,

$$t_{2l-1} = \mu\alpha(s_l, s_{l+1}, \ldots, s_{2r}, \mu^{-1}s_0, \ldots, \mu^{-1}s_{l-1}).$$

Using the definition of α, we get that

$$\begin{aligned} t_{2l-1} &= \mu(2s_{l+r}^2 + 4(s_l\mu^{-1}s_{l-1} + s_{l+1}\mu^{-1}s_{l-2} + \cdots + s_{2l-1}\mu^{-1}s_0 \\ &+ s_{2l}s_{2r} + \cdots + s_{l+r-1}s_{l+r+1})) \\ &= 2\mu s_{l+r}^2 + 4 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}} s_i s_j. \end{aligned}$$

Assume now that $0 \leq l \leq r - 1$. By Claim 2,

$$t_{2l} = \mu^2\alpha(s_{l+r+1}, s_{l+r+2}, \ldots, s_{2r}, \mu^{-1}s_0, \ldots, \mu^{-1}s_{l+r}).$$

We can now proceed as before using the definition of α. □

Claim 4: Let $s, x \in \mathbb{F}_{q^t}$. If $0 \leq l \leq 2r$, then the coefficient of θ^l in $(s+x)^2$ is

$$(s_{l/2} + x_{l/2})^2 + 2 \sum_{\{i,j\} \in U_l} \mu_{\{i,j\}}(s_i + x_i)(s_j + x_j) \text{ if } l \text{ is even,}$$

and

$$\mu(s_{r+l/2+1/2} + x_{r+l/2+1/2})^2 + 2 \sum_{\{i,j\} \in U_l} \mu_{\{i,j\}}(s_i + x_i)(s_j + x_j) \text{ if } l \text{ is odd.}$$

Proof of Claim 4. Consider

$$(s+x)^2 = \sum_{i=0}^{2r} (s_i + x_i)^2 \theta^{2i} + 2 \sum_{0 \leq i < j \leq 2r} (s_i + x_i)(s_j + x_j)\theta^{i+j}.$$

The claim follows from the definitions of $\mu_{\{i,j\}}$, U_l, and the identity $\theta^{2r+k} = \mu\theta^{k-1}$ for $1 \leq k \leq 2r$. □

Claim 5: If $(s,t), (x,y) \in Z$ and $(s+x)^2 = t + y$, then

$$\mu(s_{l+r} - x_{l+r})^2 + 2 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}}(s_i - x_i)(s_j - x_j) = 0 \text{ for } 1 \leq l \leq r,$$

and

$$(s_l - x_l)^2 + 2 \sum_{\{i,j\} \in U_{2l}} \mu_{\{i,j\}}(s_i - x_i)(s_j - x_j) = 0 \text{ for } 0 \leq l \leq r.$$

Proof of Claim 5. By Claim 4, equating coefficients of $1, \theta, \ldots, \theta^{2r}$ in the equation $(s+x)^2 = t + y$ gives

$$t_{2l-1} + y_{2l-1} = \mu(s_{l+r} + x_{l+r})^2 + 2 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}}(s_i + x_i)(s_j + x_j) \text{ if } 1 \leq l \leq r,$$

and

$$t_{2l} + y_{2l} = (s_l + x_l)^2 + 2 \sum_{\{i,j\} \in U_{2l}} \mu_{\{i,j\}}(s_i + x_i)(s_j + x_j) \text{ if } 0 \leq l \leq r.$$

Now we apply Claim 3 to t_{2l-1} and y_{2l-1}. This gives

$$\begin{aligned} 2\mu(s_{l+r}^2 + x_{l+r}^2) \quad &+ \quad 4 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}}(s_i s_j + x_i x_j) = \\ \mu(s_{l+r} + x_{l+r})^2 \quad &+ \quad 2 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}}(s_i + x_i)(s_j + x_j) \end{aligned}$$

for $1 \leq l \leq r$. This can be rewritten as

$$\mu(s_{l+r} - x_{l+r})^2 + 2 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}}(s_i - x_i)(s_j - x_j) = 0.$$

A similar application of Claim 3 (and Claim 1 in the case of t_{2r} and y_{2r}) gives

$$(s_l - x_l)^2 + 2 \sum_{\{i,j\} \in U_{2l}} \mu_{\{i,j\}}(s_i - x_i)(s_j - x_j) = 0$$

for $0 \leq l \leq r$. □

We are now ready to find an upper bound on the maximum degree of the subgraph of G_{q^t} induced by Z. Fix a vertex $(s,t) \in Z$. Suppose (x,y) is a neighbor of (s,t) with $(x,y) \in Z$. By Claim 5, $(x_0, \ldots, x_{2r}) \in \mathbb{F}_q^{2r+1}$ is a solution to the system

$$\mu(s_{l+r} - x_{l+r})^2 + 2 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}}(s_i - x_i)(s_j - x_j) = 0 \text{ for } 1 \leq l \leq r,$$

and

$$(s_l - x_l)^2 + 2 \sum_{\{i,j\} \in U_{2l}} \mu_{\{i,j\}}(s_i - x_i)(s_j - x_j) = 0 \text{ for } 0 \leq l \leq r.$$

If we set $z_i = s_i - x_i$ for $0 \leq i \leq 2r$, then we see that we have a solution to the following system of $2r+1$ homogeneous quadratic equations in the $2r+1$ unknowns $z_0, \ldots, z_{2r+1}$:

$$\mu z_{l+r}^2 + 2 \sum_{\{i,j\} \in U_{2l-1}} \mu_{\{i,j\}} z_i z_j = 0 \text{ for } 1 \leq l \leq r,$$

and

$$z_l^2 + 2 \sum_{\{i,j\} \in U_{2l}} \mu_{\{i,j\}} z_i z_j = 0 \text{ for } 0 \leq l \leq r.$$

Lemma 3.3.5. *The number of solutions $(z_0, \ldots, z_{2r}) \in \mathbb{F}_q^{2r+1}$ to the above system of $2r+1$ homogeneous quadratic equations is at most*

$$\frac{2r+5}{3} q^{\frac{4t}{3}+1}.$$

Proof. Let m be the largest integer such that $m \leq \frac{2(r+1)}{3}$. If there is set T of size m such that each z_i' in the set $\{z_i : i \in T\}$ either is zero or is determined uniquely

by the z_j's in the set $\{z_j : j \in \{0,1,\ldots,2r\}\backslash T\}$, then there are at most q^{2r+1-m} solutions. We will show there are at most $(m+1)$ choices for the index set T which implies that we have at most $(m+1)q^{2r+1-m}$ solutions in total.

Let A be the $2(r-m+1)\times m$ matrix with entries in $\mathbb{F}_q$, where for $1 \le i \le 2(r-m+1)$ and $1 \le j \le m$, the (i,j) entry of A is the coefficient of z_{j-1} in the equation

$$\mu z_{m+r+(i-1)/2}^2 + 2 \sum_{\{k,l\}\in U_{2(m+(i-1)/2)-1}} \mu_{\{k,l\}} z_k z_l = 0$$

if i is odd, and the coefficient of z_{j-1} in the equation

$$z_{m+(i-2)/2}^2 + 2 \sum_{\{k,l\}\in U_{2(m+(i-2)/2)}} \mu_{\{k,l\}} z_k z_l = 0$$

if i is even. If A is the matrix formed in this way, then one check that

$$A = \begin{pmatrix} z_{2m-1} & z_{2m-2} & z_{2m-3} & \cdots & z_m \\ z_{2m} & z_{2m-1} & z_{2m-2} & \cdots & z_{m+1} \\ z_{2m+1} & z_{2m} & z_{2m-1} & \cdots & z_{m+2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ z_{2r} & z_{2r-1} & z_{2r-2} & \cdots & z_{2r-m+1} \end{pmatrix}$$

As $m \le \frac{2(r+1)}{3}$, we have $2(r-m+1) \ge m$. Let $x = (z_0, z_1, \ldots, z_{m-1})^T$ and

$$b_i = \begin{cases} -2^{-1}\mu z_{m+r+(i-1)/2} - \sum_{\substack{\{k,l\}\in U_{2(m+(i-1)/2)-1} \\ \{k,l\}\cap\{0,1,\ldots,m-1\}=\emptyset}} \mu_{\{k,l\}} z_k z_l & \text{if } i \text{ is odd} \\ -2^{-1} z_{m+(i-2)/2} - \sum_{\substack{\{k,l\}\in U_{2(m+(i-2)/2)} \\ \{k,l\}\cap\{0,1,\ldots,m-1\}=\emptyset}} \mu_{\{k,l\}} z_k z_l & \text{if } i \text{ is even} \end{cases}$$

for $1 \le i \le 2(r-m+1)$. Let $b = (b_1, b_2, \ldots, b_{2(r-m+1)})^T$.

We next show an upper bound $m+1$ for the possible choices for the index set T. Let r_i be the i-th row of A so that

$$r_i = (z_{2m-1+(i-1)}, z_{2m-2+(i-1)}, z_{2m-3+(i-1)}, \ldots, z_{m+(i-1)}).$$

If $r_1 = \mathbf{0}$, then we take $T = \{m, m+1, \ldots, 2m-1\}$. We assume $r_1 \ne \mathbf{0}$ for the rest of the proof of the lemma.

Claim: If $i \ge 1$ and $r_{i+1} \in \mathrm{Span}_{\mathbb{F}_q}\{r_1, \ldots, r_i\}$, then

$$z_{m+i+j} \in \mathrm{Span}_{\mathbb{F}_q}\{z_m, z_{m+1}, \ldots, z_{m+i-1}\} \text{ for } j = 0, 1, \ldots, m-1.$$

Proof of Claim. We prove the claim by induction on j. Suppose

$$r_{i+1} = \alpha_1 r_1 + \cdots + \alpha_i r_i \tag{3.8}$$

for some $\alpha_j \in \mathbb{F}_q$. By considering the last coordinate, we get that

$$z_{m+i} = \sum_{j=1}^{i} \alpha_j z_{m+(j-1)} \in \mathrm{Span}_{\mathbb{F}_q}\{z_m, \ldots, z_{m+i-1}\}$$

establishing the base case $j = 0$. If $z_{m+i+j_0} \in \mathrm{Span}_{\mathbb{F}_q}\{z_m, \ldots, z_{m+i-1}\}$ for $0 \leq j_0 \leq m-2$, then by (3.8),

$$z_{m+i+j_0+1} = \sum_{j=1}^{i} \alpha_j z_{m+j_0+1+(j-1)} = \alpha_i z_{m+i+j_0} + \sum_{j=1}^{i-1} \alpha_j z_{m+j+j_0}.$$

By the inductive hypothesis, this is in $\mathrm{Span}_{\mathbb{F}_q}\{z_m, \ldots, z_{m+i-1}\}$. □

By the Claim, if there is an $i \in \{1, 2, \ldots, m-1\}$ such that

$$r_{i+1} \in \mathrm{Span}_{\mathbb{F}_q}\{r_1, \ldots, r_i\},$$

then there exist m z_i's that are uniquely determined by the other z_j's and we can take $T = \{z_{m+i}, z_{m+i+1}, \ldots, z_{2m+i-1}\}$. Otherwise, $r_1, \ldots, r_m$ are linearly independent which implies that the rank of A is at least m. It is at this step where we need $m \leq \frac{2(r+1)}{3}$ as we require the number of rows of A, which is $2(r-m+1)$, to be at least m. Since the rank of A is at least m, there is at most one solution x to $Ax = b$. In this case we take $T = \{0, 1, \ldots, m-1\}$ and each of $\{z_0, z_1, \ldots, z_{m-1}\}$ is determined by $\{z_m, z_{m+1}, \ldots, z_{2r}\}$.

Altogether, we have at most

$$(m+1)q^{\frac{4r}{3}-\frac{1}{3}} \leq \frac{2r+5}{3} q^{\frac{4r}{3}+1}$$

solutions which proves the lemma.

□

By Lemma 3.3.5, the maximum degree of $G_{q^t}[Z]$ is at most $\frac{2r+5}{3} q^{\frac{4r}{3}+1}$. Therefore,

$$\chi(G_{q^t}) \leq \frac{2r+5}{3} q^{\frac{4r}{3}+1} + (2r+1)q^{r+1}$$

□

We obtain a coloring of ER_{q^t} from a coloring of G_{q^t} as before. We use one new color on the vertices $z_1, \ldots, z_t$, and then give y any color that is used on G_{q^t}. This gives a coloring of ER_{q^t} that uses at most $\frac{2r+5}{3}q^{\frac{4r}{3}+1} + (2r+1)q^{r+1} + 1$ colors which proves Theorem 3.1.3.

3.4 Proof of Theorem 3.1.8

The following lemma is easily proved using the definition of adjacency in G_q.

Lemma 3.4.1. *Suppose $\alpha_i, \alpha_j, \alpha_k$ are distinct elements of $\mathbb{F}_q$ such that*

$$\alpha_i + \alpha_j = a^2, \alpha_j + \alpha_k = b^2, \text{ and } \alpha_k + \alpha_i = c^2$$

for some $a, b, c \in \mathbb{F}_q$. If $x + y = a$, $y + z = b$, and $z + x = c$, then

$$\{(x, \alpha_i), (y, \alpha_j), (z, \alpha_k)\}$$

induces a triangle in G_q.

Given an odd prime power q, let $\chi : \mathbb{F}_q \to \{0, \pm 1\}$ be the quadratic character on $\mathbb{F}_q$. That is, $\chi(0) = 0$, $\chi(a) = 1$ if a is a nonzero square in $\mathbb{F}_q$, and $\chi(a) = -1$ otherwise. For the next lemma, we require some results on finite fields (see Chapter 5 of [61]).

Proposition 3.4.2. *Let q be an odd prime and $f(x) = a_2x^2 + a_1x + a_0 \in \mathbb{F}_q[x]$ where $a_2 \neq 0$. If $a_1^2 - 4a_0a_2 \neq 0$, then*

$$\sum_{c \in \mathbb{F}_q} \chi(f(c)) = -\chi(a_2).$$

Proposition 3.4.3 (Weil)**.** *If $f(x) \in \mathbb{F}_q[x]$ is a degree $d \geq 1$ polynomial that is not the square of another polynomial, then*

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

Lemma 3.4.4. *If $q > 487$ is a power of an odd prime, then there are elements $\alpha_1, \ldots, \alpha_5 \in \mathbb{F}_q^*$ such that $\alpha_1, \ldots, \alpha_5$ are all distinct, and*

$$\chi(\alpha_i + \alpha_j) = 1$$

for $1 \leq i < j \leq 5$.

Proof. Choose $\alpha_1 \in \mathbb{F}_q^*$ arbitrarily. There are $\frac{q-1}{2}$ nonzero squares in $\mathbb{F}_q^*$ so we can easily find an $\alpha_2 \in \mathbb{F}_q \backslash \{0, \alpha_1\}$ such that $\chi(\alpha_1 + \alpha_2) = 1$. Observe that this implies $\alpha_2 \neq -\alpha_1$ otherwise $\chi(\alpha_1 + \alpha_2) = 0$. Assume that we have chosen $\alpha_1, \ldots, \alpha_k \in \mathbb{F}_q^*$ so that $\alpha_1, \ldots, \alpha_k$ are all distinct and

$$\chi(\alpha_i + \alpha_j) = 1$$

for $1 \leq i < j \leq k$. Let

$$f(x) = \prod_{i=1}^{k} (1 + \chi(\alpha_i + x))$$

and $X = \{\beta \in \mathbb{F}_q : f(\beta) = 2^k\}$. If $\beta \in \mathbb{F}_q$ and $f(\beta) > 0$, then $\chi(\alpha_i + \beta) \in \{0, 1\}$ for $1 \leq i \leq k$. We have $\chi(\alpha_i + \beta) = 0$ if and only if $\beta = -\alpha_i$. Therefore, there are at most k distinct β's in $\mathbb{F}_q$ such that $0 < f(\beta) < 2^k$ which implies

$$2^k |X| + k 2^{k-1} \geq \sum_{x \in \mathbb{F}_q} f(x) = q + \sum_{\emptyset \neq S \subset [k]} \sum_{x \in \mathbb{F}_q} \chi\left(\prod_{\alpha \in S} (x + \alpha) \right).$$

For any $i \in [k]$, $\sum_{x \in \mathbb{F}_q} \chi(\alpha_i + x) = 0$. For any $1 \leq i < j \leq k$,

$$\sum_{x \in \mathbb{F}_q} \chi(x^2 + (\alpha_i + \alpha_j)x + \alpha_i \alpha_j) = -1$$

by Proposition 3.4.2. When $k = 2$, if $\frac{q-3-3 \cdot 2^2}{2^3} \geq 3 + 1$, then $|X| \geq 4$ and we can choose an $\alpha_3 \in \mathbb{F}_q \backslash \{0, \alpha_1, \alpha_2\}$ that has the desired properties. When $k \in \{3, 4\}$, we use Weyl's inequality to obtain a lower bound on $|X|$. Observe that since $\alpha_1, \ldots, \alpha_k$ are distinct, no product $(x + \alpha_{i_1}) \cdots (x + \alpha_{i_l})$ for $1 \leq i_1 < \cdots < i_l \leq k$ is the square of a polynomial in $\mathbb{F}_q[x]$. By Weyl's inequality, for any $1 \leq i_1 < \cdots < i_l \leq k$,

$$\left| \sum_{x \in \mathbb{F}_q} \chi((x + \alpha_{i_1}) \cdots (x + \alpha_{i_l})) \right| \leq l\sqrt{q}.$$

The hypothesis on q implies that q is large enough so that $|X| \geq 5$ when $k = 3$, and $|X| \geq 6$ when $k = 4$. Therefore, we can inductively choose α_4 and α_5 so that $\alpha_1, \ldots, \alpha_5$ satisfy all of the required properties. □

Choose elements $\alpha_1, \ldots, \alpha_5 \in \mathbb{F}_q^*$ satisfying the properties of Lemma 3.4.4. Let

$$\alpha_i + \alpha_j = a_{i,j}^2$$

for $1 \leq i < j \leq 5$. Since $\alpha_i \neq -\alpha_j$, no $a_{i,j}$'s is zero. For $1 \leq i < j < k \leq 5$, let $x_{i,j,k}$, $y_{i,j,k}$, and $z_{i,j,k}$ be any elements of $\mathbb{F}_q$ that satisfy

$$x_{i,j,k} + y_{i,j,k} = a_{i,j}, \quad y_{i,j,k} + z_{i,j,k} = a_{j,k}, \quad \text{and} \quad z_{i,j,k} + x_{i,j,k} = a_{i,k}.$$

Then the vertices $(x_{i,j,k}, \alpha_i)$, $(y_{i,j,k}, \alpha_j)$, and $(z_{i,j,k}, \alpha_k)$ form a triangle in G_q and this holds for any $1 \leq i < j < k \leq 5$.

Now we use these triangles, which are in G_q, together with the new vertices $z_1, \ldots, z_q, y$ that are added to G_q to from $H_q \cong ER_q$ to obtain a subgraph with chromatic number at least four. For $1 \leq i \leq 5$, the vertex z_{α_i} is adjacent to all vertices of the form (x, α_i). The vertex y is adjacent to each z_i. Consider the subgraph H_q whose vertices are $y, z_{\alpha_1}, \ldots, z_{\alpha_5}$ together with all $(x_{i,j,k}, \alpha_i)$, $(y_{i,j,k}, \alpha_j)$, and $(z_{i,j,k}, \alpha_k)$ for $1 \leq i < j < k \leq 5$. Suppose we have a proper 3-coloring of this subgraph, say with colors 1, 2, and 3. If the color 1 is given to three distinct vertices z_{α_i}'s, say $z_{\alpha_i}, z_{\alpha_j}$, and z_{α_k}, then only colors 2 and 3 may be used on the triangle whose vertices are $(x_{i,j,k}, \alpha_i)$, $(y_{i,j,k}, \alpha_j)$, and $(z_{i,j,k}, \alpha_k)$. Therefore, all three colors must be used to color the vertices in the set $\{z_{\alpha_1}, \ldots, z_{\alpha_5}\}$ but then no color may be used on y. The number of vertices in this subgraph is at most $1 + 5 + \binom{5}{3}3 = 36$.

3.5 Concluding remarks on coloring ER_q

The upper bounds of Theorems 3.3.4 and 3.1.3 can be improved for large q by applying the main result of [5] to the graph $G_{q^t}[Z]$ instead of using Brooks' Theorem. We have chosen to use Brooks' Theorem as then there is no issue of

how large the implicit constant is, and because we believe that the upper bound should be closer to $O(q^{t/2})$.

Using a similar argument as the one used to prove Theorem 3.1.3, we can prove the following.

Theorem 3.5.1. *If q is a power of an odd prime, then*

$$\chi(G_{q^3}) \leq 6q^2.$$

A consequence is that $\chi(ER_{q^3}) \leq 6q^2 + 1$ whenever q is a power of an odd prime. Unfortunately, we were not able to extend this bound to the general case. In the q^3 case, one can explicitly compute the relations satisfied by vertices in X (see Section 3.3.2)) and then use these equations to bound the maximum degree of $G_{q^3}[X]$. Dealing with the set X is one of the main obstacles in our approach.

We remark that if one could improve the bound in Lemma 3.3.5, it would improve our result in Theorem 3.1.3. It seems likely that Lemma 3.3.5 could be strengthened enough to improve the bound in Theorem 3.1.3 all the way down to

$$\chi(ER_{q^{2r+1}}) \leq (2r + 1 + o(1))q^{r+1}.$$

Perhaps this can be done using techniques from algebraic geometry.

The conditions on q for which there exists an irreducible polynomial $x^t - \mu \in \mathbb{F}_q[x]$ are known (see Theorem 3.75 of [61]). Let q be a power of an odd prime and let $t \geq 3$ be an odd integer. Let $\text{ord}(\mu, q)$ be the order of μ in group $\mathbb{F}_q^*$. Then $x^t - \mu \in \mathbb{F}_q[x]$ is irreducible if and only if each prime factor of t divides $\text{ord}(\mu, q)$ but does not divide $\frac{q-1}{\text{ord}(\mu,q)}$. Since $\mathbb{F}_q^*$ is cyclic, for any divisor d of $q - 1$, there is an element $a \in \mathbb{F}_q^*$ with $\text{ord}(a, q) = d$. As long as t divides $q - 1$, we can choose an element $\mu \in \mathbb{F}_q^*$ so that t divides $\text{ord}(\mu, q)$ but t does not divide $\frac{q-1}{\text{ord}(\mu,q)}$. Therefore, if $q \equiv 1 (\text{mod } t)$, then Theorem 3.1.3 applies and we obtain the upper bound $\chi(ER_{q^t}) \leq \frac{2r+5}{3} q^{\frac{4r}{3}+1} + (2r + 1)q^{r+1} + 1$ in this case. For a fixed $t \geq 3$, Dirichlet's Theorem on primes in arithmetic progressions implies that there are infinitely many primes p such that $p \equiv 1 (\text{mod } t)$. Then for any q which is an odd power of such p, we have $q \equiv 1 (\text{mod } t)$.

We end this chapter with a problem that, if solved, would significantly strengthen our results. In Chapter 4 we give some evidence that such a theorem might be true.

Problem 3.5.2. *Determine if there is an absolute constant C such that the following holds. If G is an orthogonal polarity graph of a projective plane of order q, then*

$$\chi(G) \leq Cq^{1/2}.$$

Chapter 3 is a version of the material appearing in "On the chromatic number of the Erdős-Rényi orthogonal polarity graph", *Electronic Journal of Combinatorics*, P2.21, (2011), 1–19, co-authored with Xing Peng and Craig Timmons. The author was the primary investigator and author of this paper.

4

Chromatic and Independence Numbers of General Polarity Graphs

"Swimming instruction, which in time became swimming practice, was grueling, but there was the deep pleasure of doing a stroke with increasing ease and speed, over and over, till hypnosis practically, the water turning from molten lead to liquid light."

– Piscine Molitor Patel

4.1 Introduction

In Chapter 3, it was noted that an upper bound on the independence number of ER_q of the correct order of magnitude is given by the Hoffman Ratio Bound (Theorem 3.1.1). In Chapter 2, we computed the eigenvalues of the adjacency matrix of any polarity graph, and so Hoffman's Theorem applies in this more general setting, which we now describe.

Let $\Sigma = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be a projective plane of order q. Recall that a bijection $\theta : \mathcal{P} \cup \mathcal{L} \to \mathcal{P} \cup \mathcal{L}$ is a *polarity* if $\theta(\mathcal{P}) = \mathcal{L}$, $\theta(\mathcal{L}) = \mathcal{P}$, θ^2 is the identity map, and $p\mathcal{I}l$ if and only if $l^\theta \mathcal{I} p^\theta$. A point $p \in \mathcal{P}$ is called an *absolute point* if $p\mathcal{I}p^\theta$. A

classical result of Baer is that any polarity of a projective plane of order q has at least $q+1$ absolute points. A polarity with $q+1$ points is called an *orthogonal polarity*, and such polarities exist in the Desarguesian projective plane as well as in other non-Desarguesian planes. For more on polarities see [52], Chapter 12. Given a projective plane $\Sigma = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ of order q and an orthogonal polarity θ, the corresponding *orthogonal polarity graph* $G(\Sigma, \theta)$ is the graph with vertex set $\mathcal{P}$ where two distinct vertices p_1 and p_2 are adjacent if and only if $p_1 \mathcal{I} p_2^{\theta}$. Let $G^{\circ}(\Sigma, \theta)$ be the graph obtained from $G(\Sigma, \theta)$ by adding loops to the absolute points of θ. In Chapter 2, we showed that the integer $q+1$ is an eigenvalue of $G^{\circ}(\Sigma, \theta)$ with multiplicity 1, and all other eigenvalues are $\sqrt{q}$ or $-\sqrt{q}$. Then Theorem 3.1.1 yields

$$\alpha(G^{\circ}(\Sigma, \theta)) \leq \frac{-(q^2+q+1)(-q^{1/2})}{q+1-\sqrt{q}} \tag{4.1}$$

which gives $\alpha(G(\Sigma, \theta)) \leq q^{3/2} + q^{1/2} + 1$. An improved estimate in the case that q is even was obtained by Hobart and Williford [49] using association schemes. They conjectured that the upper bound (4.1) can be improved to

$$\alpha(G(\Sigma, \theta)) \leq q(q^{1/2}+1) - 2(q^{1/2}-1)(q+q^{1/2})^{1/2}$$

but this is still open.

In Chapter 3, we discussed Mubayi and Williford's result [65] giving a lower bound for $\alpha(ER_q)$ of the correct order of magnitude. In this chapter we obtain a strengthening of their result to a wider class of orthogonal polarity graphs which we introduce now and will be the focus of much of our investigations. We remark that the study of polarity graphs coming from non-Desarguesian planes was suggested in [8].

Let q be a power of an odd prime and $f(X) \in \mathbb{F}_q[X]$. The polynomial $f(X)$ is a *planar polynomial* if for each $a \in \mathbb{F}_q^*$, the map

$$x \mapsto f(x+a) - f(x)$$

is a bijection on $\mathbb{F}_q$. Planar polynomials were introduced by Dembowski and Ostrom [29] in their study of projective planes of order q that admit a collineation group of order q^2. Given a planar polynomial $f(X) \in \mathbb{F}_q[X]$, one can construct a

projective plane as follows. Let $\mathcal{P} = \{(x,y) : x,y \in \mathbb{F}_q\} \cup \{(x) : x \in \mathbb{F}_q\} \cup \{(\infty)\}$. For $a,b,c \in \mathbb{F}_q$, let

$$[a,b] = \{(x, f(x-a)+b) : x \in \mathbb{F}_q\} \cup \{(a)\},$$
$$[c] = \{(c,y) : y \in \mathbb{F}_q\} \cup \{(\infty)\},$$
$$[\infty] = \{(c) : c \in \mathbb{F}_q\} \cup \{(\infty)\}.$$

Let $\mathcal{L} = \{[a,b] : a,b \in \mathbb{F}_q\} \cup \{[c] : c \in \mathbb{F}_q\} \cup \{[\infty]\}$. Define Π_f to be the incidence structure whose points are $\mathcal{P}$, whose lines are $\mathcal{L}$, and incidence $\mathcal{I}$ is given by containment. When f is a planar polynomial, Π_f is a projective plane. For instance if $f(X) = X^2$ and q is any power of an odd prime, Π_f is isomorphic to the Desarguesian plane $PG(2,q)$. For other examples, see [25].

Assume that $f(X) \in \mathbb{F}_q[X]$ is a planar polynomial. The plane Π_f possesses an orthogonal polarity ω given by

$$(\infty)^\omega = [\infty], \quad [\infty]^\omega = (\infty), \quad (c)^\omega = [-c], \quad [c]^\omega = (-c)$$
$$(x,y)^\omega = [-x,-y], \text{ and } [a,b]^\omega = (-a,-b)$$

where $a,b,c \in \mathbb{F}_q$. We write G_f for the corresponding orthogonal polarity graph. This is the graph whose vertices are the points of Π_f and two distinct vertices p_1 and p_2 are adjacent in G_f if and only if p_1 is incident to p_2^ω in Π_f. For vertices of the form (x,y) the adjacency relation is easily described in terms of f. The distinct vertices (x_1,y_1) and (x_2,y_2) are adjacent if and only if

$$f(x_1+x_2) = y_1+y_2.$$

Our first result is a generalization of Mubayi and Williford's result in [65] to orthogonal polarity graphs which need not come from a Desarguesian plane.

Theorem 4.1.1. *If q is a power of an odd prime and $f(X) \in \mathbb{F}_{q^2}[X]$ is a planar polynomial all of whose coefficients belong to the subfield $\mathbb{F}_q$, then*

$$\alpha(G_f) \geq \frac{1}{2}q^2(q-1)$$

Even though we have the restriction that the coefficients of f belong to $\mathbb{F}_q$, many of the known examples of planar functions have this property. Most of

the planar functions discussed in [25], including those that give rise to the famous Coulter-Matthews plane, satisfy our requirement.

It is still an open problem to determine an asymptotic formula for the independence number of ER_p for odd prime p. However, given the results of [65] and Theorem 4.1.1, it would be quite surprising to find an orthogonal polarity graph of a projective plane of order q whose independence number is $o(q^{3/2})$. We believe that the lower bound $\Omega(q^{3/2})$ is a property shared by all polarity graphs, including polarity graphs that come from polarities which are not orthogonal.

Conjecture 4.1.2. *If $G(\Sigma, \theta)$ is a polarity graph of a projective plane of order q, then*

$$\alpha(G(\Sigma, \theta)) = \Omega(q^{3/2}).$$

There are polarity graphs which are not orthogonal polarity graphs for which Conjecture 4.1.2 holds. If $G(\Sigma, \theta)$ is a polarity graph where θ is unitary and Σ has order q, then $\alpha(G(\Sigma, \theta)) \geq q^{3/2} + 1$. Indeed, the absolute points of any polarity graph form an independent set and a unitary polarity has $q^{3/2}+1$ absolute points. In Section 4.3 we show that there is a polarity graph $G(\Sigma, \theta)$ where θ is neither orthogonal or unitary and Conjecture 4.1.2 holds.

Theorem 4.1.3. *Let p be an odd prime, $n \geq 1$ be an integer, and $q = p^{2n}$. There is a polarity graph $G(\Sigma, \theta)$ such that Σ has order q, θ is neither orthogonal nor unitary, and*

$$\alpha(G(\Sigma, \theta)) \geq \frac{1}{2}q(\sqrt{q} - 1).$$

In connection with Theorem 4.1.1 and Conjecture 4.1.2, we would like to mention the work of De Winter, Schillewaert, and Verstraëte [27] and Stinson [79]. In these papers the problem of finding large sets of points and lines such that there is no incidence between these sets is investigated. Finding an independent set in a polarity graph is related to this problem as an edge in a polarity graph corresponds to an incidence in the geometry. The difference is that when one finds an independent set in a polarity graph, choosing the points determines the lines. In [27] and [79], one can choose the points and lines independently.

As mentioned above, Conjecture 4.1.2 holds for unitary polarity graphs as the absolute points form an independent set. Mubayi and Williford [65] asked whether or not there is an independent set in the graph U_q of size $\Omega(q^{3/2})$ that contains no absolute points. For q a square of a prime power, the graph U_q has the same vertex set as ER_q and two distinct vertices (x_0, x_1, x_2) and (y_0, y_1, y_2) are adjacent if and only if $x_0y_0^{\sqrt{q}} + x_1y_1^{\sqrt{q}} + x_2y_2^{\sqrt{q}} = 0$. We could not answer their question, but we were able to produce an independent set of size $\Omega(q^{5/4})$ that contains no absolute points. We remark that a lower bound of $\Omega(q)$ is trivial.

Theorem 4.1.4. *Let q be an even power of an odd prime. The graph U_q has an independent set I that contains no absolute points and*

$$|I| \geq 0.19239q^{5/4} - O(q).$$

Related to the independence number is the chromatic number. In Chapter 3, it is shown that $\chi(ER_{q^2}) \leq 2q + O(\frac{q}{\log q})$ whenever q is a power of an odd prime. Here we prove that this upper bound holds for another family of orthogonal polarity graphs.

Definition 4.1.5. *Let p be an odd prime. Let n and s be positive integers such that $s < 2n$ and $\frac{2n}{s}$ is an odd integer. Let $d = p^s$ and $q = p^n$. We call the pair $\{q, d\}$ an* admissible pair*.*

If $\{q, d\}$ is an admissible pair, then the polynomial $f(X) = X^{d+1} \in \mathbb{F}_{q^2}[X]$ is a planar polynomial. For a nice proof, see Theorem 3.3 of [25].

Theorem 4.1.6. *Let q be a power of an odd prime and $\{q, d\}$ be an admissible pair. If $f(X) = X^{d+1}$, then*

$$\chi(G_f) \leq 2q + O\left(\frac{q}{\log q}\right).$$

The eigenvalue bound (4.1) gives a lower bound of $\chi(G_f) \geq \frac{q^4+q^2+1}{q^3+q+1}$ so that the leading term in the upper bound of Theorem 4.1.6 is best possible up to a constant factor. Not only does this bound imply that $\alpha(G_f) \geq \frac{1}{2}q^3 - o(q^3)$, but shows that most of the vertices of G_f can be partitioned into large independent sets.

The technique that is used to prove Theorem 4.1.6 is the same as the one used in [70] and can be applied to other orthogonal polarity graphs. In Section 4.6, we sketch an argument that the bound of Theorem 4.1.6 also holds for a plane coming from a Dickson commutative division ring (see [52]). It is quite possible that the technique applies to more polarity graphs, but in order to obtain a general result, some new ideas will be needed. Furthermore, showing that every polarity graph of a projective plane of order q has chromatic number $O(\sqrt{q})$ is a significant strengthening of Conjecture 4.1.2. When p is prime, it is still unknown whether $\chi(ER_p) = O(\sqrt{p})$.

4.2 Proof of Theorem 4.1.1

Let q be a power of an odd prime and $f(X) \in \mathbb{F}_{q^2}[X]$ be a planar polynomial, all of whose coefficients are in the subfield $\mathbb{F}_q$. Let G_f be the orthogonal polarity graph whose construction is given before the statement of Theorem 4.1.1. Partition $\mathbb{F}_q^*$ into two sets $\mathbb{F}_q^+$ and $\mathbb{F}_q^-$ where $a \in \mathbb{F}_q^+$ if and only if $-a \in \mathbb{F}_q^-$. Let μ be a root of an irreducible quadratic over $\mathbb{F}_q$ and so $\mathbb{F}_{q^2} = \{a + \mu b : a, b \in \mathbb{F}_q\}$. Let

$$I = \{(x, y + z\mu) : x, y \in \mathbb{F}_q, z \in \mathbb{F}_q^+\}.$$

Note that $|I| = \frac{1}{2}q^2(q-1)$ and we claim that I is an independent set. Suppose $(x_1, y_1 + z_1\mu)$ and $(x_2, y_2 + z_2\mu)$ are distinct vertices in I and that they are adjacent. Then

$$f(x_1 + x_2) = y_1 + y_2 + (z_1 + z_2)\mu. \tag{4.2}$$

The left-hand side of (4.2) belongs to $\mathbb{F}_q$ since the coefficients of f are in $\mathbb{F}_q$ and $x_1 + x_2 \in \mathbb{F}_q$. The right-hand side of (4.2) is not in $\mathbb{F}_q$ since $z_1 + z_2 \neq 0$. We have a contradiction so no two vertices in I are adjacent.

4.3 Proof of Theorem 4.1.3

Let p be an odd prime, $n \in \mathbb{N}$, and $q = p^{2n}$. Let $\{1, \lambda\}$ be a basis for a 2-dimensional vector space over $\mathbb{F}_q$. Let $\sigma : \mathbb{F}_q \to \mathbb{F}_q$ be the map $x^\sigma = x^{p^n}$. Observe

that σ is a field automorphism of order 2, and the fixed elements of σ are precisely the elements of the subfield $\mathbb{F}_{p^n}$ in $\mathbb{F}_q$. Let θ be a generator of $\mathbb{F}_q^*$ which is the group of non-zero elements of $\mathbb{F}_q$ under multiplication. Let D be the division ring whose elements are $\{x + \lambda y : x, y \in \mathbb{F}_q\}$ where addition is done componentwise, and multiplication is given by the rule

$$(x + \lambda y) \cdot (z + \lambda t) = xz + \theta t y^\sigma + \lambda(yz + x^\sigma t).$$

Here we are following the presentation of [52]. Define the map $\alpha : D \to D$ by

$$(x + \lambda y)^\alpha = x + \lambda y^\sigma.$$

Let $\Pi_D = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be the plane coordinatized by D. That is,

$$\mathcal{P} = \{(x, y) : x, y \in D\} \cup \{(x) : x \in D\} \cup \{(\infty)\}$$

and

$$\mathcal{L} = \{[m, k] : m, k \in D\} \cup \{[m] : m \in D\} \cup \{[\infty]\}$$

where

$$\begin{aligned} [m, k] &= \{(x, y) : m \cdot x + y = k\} \cup \{(m)\}, \\ [k] &= \{(k, y) : y \in D\} \cup \{(\infty)\}, \\ [\infty] &= \{(m) : m \in D\} \cup \{(\infty)\}. \end{aligned}$$

The incidence relation $\mathcal{I}$ is containment. A polarity of Π_D is given by the map ω where

$$(\infty)^\omega = [\infty], \quad [\infty]^\omega = (\infty), \quad (m)^\omega = [m^\alpha], \quad [k]^\omega = (k^\alpha)$$

and

$$(x, y)^\omega = [x^\alpha, -y^\alpha], \qquad [m, k] = (m^\alpha, -k^\alpha).$$

The polarity ω has $|D|^{5/4} + 1$ absolute points. Let $G(\Pi_D, \omega)$ be the corresponding polarity graph.

We now derive an algebraic condition for when the distinct vertices

$$u = (x_1 + \lambda x_2, y_1 + \lambda y_2) \text{ and } v = (z_1 + \lambda z_2, t_1 + \lambda t_2)$$

are adjacent. The vertex u is adjacent to v if and only if $u\mathcal{I}v^{\omega}$. This is equivalent to

$$(x_1 + \lambda x_2, y_1 + \lambda y_2)\mathcal{I}[z_1 + \lambda(z_2)^{\sigma}, -t_1 + \lambda(-(t_2)^{\sigma})]$$

which in turn, is equivalent to

$$(z_1 + \lambda(z_2)^{\sigma}) \cdot (x_1 + \lambda x_2) = -y_1 - t_1 + \lambda(-y_2 - (t_2)^{\sigma}). \tag{4.3}$$

Using the definition of multiplication in D, (4.3) can be rewritten as

$$z_1x_1 + \theta x_2z_2 + \lambda((z_2)^{\sigma}x_1 + (z_1)^{\sigma}x_2) = -y_1 - t_1 + \lambda(-y_2 - (t_2)^{\sigma}).$$

This gives the pair of equations

$$x_1z_1 + \theta x_2z_2 = -y_1 - t_1 \tag{4.4}$$

and

$$x_1(z_2)^{\sigma} + x_2(z_1)^{\sigma} = -y_2 - (t_2)^{\sigma}.$$

Let $\square_q$ be the set of nonzero squares in $\mathbb{F}_q$. Note that any element of $\mathbb{F}_{p^n}$ is a square in $\mathbb{F}_q$. Define

$$I = \{(x_1 + \lambda x_2, y_1 + \lambda y_2) : x_1, y_1 \in \mathbb{F}_{p^n}, x_2 \in \square_q, y_2 \in \mathbb{F}_q\}.$$

Then $|I| = \frac{1}{2}(q-1)q(p^n)^2 = \frac{1}{2}q^2(q-1)$. We now show that I is an independent set. Suppose that $(x_1 + x_2\lambda, y_1 + y_2\lambda)$ and $(z_1 + z_2\lambda, t_1 + t_2\lambda)$ are distinct vertices in I that are adjacent. Then (4.4) holds so

$$\theta = (x_2z_2)^{-1}(-y_1 - t_1 - x_1z_1). \tag{4.5}$$

The left hand side of (4.5) is not a square in $\mathbb{F}_q$. Since x_2 and z_2 belong to $\square_q$, we have that $(x_2z_2)^{-1}$ is a square in $\mathbb{F}_q$. Since $y_1, t_1, x_1, z_1 \in \mathbb{F}_{p^n}$, we have that $-y_1 - t_1 - x_1z_1$ is in $\mathbb{F}_{p^n}$ and thus is a square in $\mathbb{F}_q$. We conclude that the right hand side of (4.5) is a square. This is a contradiction and so I must be an independent set. This shows that

$$\alpha(G(\Pi_D, \omega)) \geq \frac{1}{2}q^2(q-1).$$

4.4 Proof of Theorem 4.1.4

Let p be an odd prime, $n \in \mathbb{N}$, and $q = p^{2n}$. Let θ be a generator of $\mathbb{F}_q^*$. The field $\mathbb{F}_q$ contains a subfield with $\sqrt{q}$ elements and we write $\mathbb{F}_{\sqrt{q}}$ for this subfield. We will use the fact that $x^{\sqrt{q}} = x$ if and only if $x \in \mathbb{F}_{\sqrt{q}}$ and that the characteristic of $\mathbb{F}_q$ is a divisor of $\sqrt{q}$ without explicitly saying so.

Let U_q be the graph whose vertex set is $V(ER_q)$ and two vertices (x_0, x_1, x_2) and (y_0, y_1, y_2) are adjacent if and only if

$$x_0 y_0^{\sqrt{q}} + x_1 y_1^{\sqrt{q}} + x_2 y_2^{\sqrt{q}} = 0.$$

In [65], it is shown that U_q has an independent set J of size q^3+1. This independent set consists of the absolute points in U_q; namely

$$J = \{(x_0, x_1, x_2) : x_0^{\sqrt{q}+1} + x_1^{\sqrt{q}+1} + x_2^{\sqrt{q}+1} = 0\}.$$

To find an independent set in U_q with no absolute points and size $\Omega(q^{5/4})$, we will work with a graph that is isomorphic to U_q. Let U_q^* be the graph whose vertex set is $V(ER_q)$ where (x_0, x_1, x_2) and (y_0, y_1, y_2) are adjacent if and only if

$$x_0 y_2^{\sqrt{q}} + x_2 y_0^{\sqrt{q}} = x_1 y_1^{\sqrt{q}}.$$

The proof of Proposition 3 of [65] is easily adapted to prove the following.

Lemma 4.4.1. *The graph U_q is isomorphic to the graph U_q^*.*

For any $\mu \in \mathbb{F}_q \backslash \mathbb{F}_{\sqrt{q}}$, we have $\mathbb{F}_q = \{a + b\mu : a, b \in \mathbb{F}_{\sqrt{q}}\}$. The next lemma shows that we can find a μ that makes many of our calculations significantly easier.

Lemma 4.4.2. *There is a $\mu \in \mathbb{F}_q \backslash \mathbb{F}_{\sqrt{q}}$ such that $\mu^{\sqrt{q}} + \mu = 0$.*

Proof. Let $\mu = \theta^{\frac{1}{2}(\sqrt{q}+1)}$. Since $\mathbb{F}_{\sqrt{q}}^* = \langle \theta^{\sqrt{q}+1} \rangle$, we have that $\mu \notin \mathbb{F}_{\sqrt{q}}$. Using the fact that $-1 = \theta^{\frac{1}{2}(q-1)}$, we find that

$$\begin{aligned} \mu^{\sqrt{q}} + \mu &= \theta^{\frac{1}{2}\sqrt{q}(\sqrt{q}+1)} + \theta^{\frac{1}{2}(\sqrt{q}+1)} = \theta^{\frac{1}{2}\sqrt{q}(\sqrt{q}+1)} - \theta^{\frac{1}{2}(q-1)+\frac{1}{2}(\sqrt{q}+1)} \\ &= \theta^{\frac{1}{2}(q+\sqrt{q})} - \theta^{\frac{1}{2}(q+\sqrt{q})} = 0. \end{aligned}$$

□

For the rest of this section we fix a $\mu \in \mathbb{F}_q \backslash \mathbb{F}_{\sqrt{q}}$ that satisfies the statement of Lemma 4.4.2. Given $c \in \mathbb{F}_{\sqrt{q}}$, define

$$X_c = \{(1, a, b + c\mu) : a, b \in \mathbb{F}_{\sqrt{q}}\}.$$

Lemma 4.4.3. *If c_1 and c_2 are elements of $\mathbb{F}_{\sqrt{q}}$ with $c_1 \neq c_2$, then the graph U_q^* has no edge with one endpoint in X_{c_1} and the other in X_{c_2}.*

Proof. Suppose that $(1, a_1, b_1 + c_1\mu)$ is adjacent to $(1, a_2, b_2 + c_2\mu)$ where $a_i, b_i, c_i \in \mathbb{F}_{\sqrt{q}}$. By definition of adjacency in U_q^*,

$$b_2 + c_2\mu^{\sqrt{q}} + b_1 + c_1\mu = a_1a_2.$$

By Lemma 4.4.2, this can be rewritten as

$$(c_1 - c_2)\mu = a_1a_2 - b_1 - b_2. \tag{4.6}$$

The right hand side of (4.6) belongs to the subfield $\mathbb{F}_{\sqrt{q}}$. Therefore, $c_1 - c_2 = 0$ since $\mu \notin \mathbb{F}_{\sqrt{q}}$. □

Now we consider the subgraph $U_q^*[X_c]$ where $c \in \mathbb{F}_{\sqrt{q}}$. The vertex set of $U_q^*[X_c]$ is

$$\{(1, a, b + c\mu) : a, b \in \mathbb{F}_{\sqrt{q}}\}$$

and two vertices $(1, a_1, b_1 + c\mu)$ and $(1, a_2, b_2 + c\mu)$ are adjacent if and only if

$$b_2 + c(\mu^{\sqrt{q}} + \mu) + b_1 = a_1a_2.$$

By Lemma 4.4.2, this is equivalent to

$$b_2 - a_1a_2 + b_1 = 0. \tag{4.7}$$

Let $ER_{\sqrt{q}}^*$ be the graph whose vertex set is $V(ER_{\sqrt{q}})$ and (x_0, x_1, x_2) is adjacent to (y_0, y_1, y_2) if and only if

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

Proposition 3 of [65] shows that $ER_{\sqrt{q}}^*$ is isomorphic to $ER_{\sqrt{q}}$. It follows from (4.7) that the graph $U_q^*[X_c]$ is isomorphic to the subgraph of $ER_{\sqrt{q}}^*$ induced by

$\{(1, x_1, x_2) : x_1, x_2 \in \mathbb{F}_{\sqrt{q}}\}$. Note that $ER^*_{\sqrt{q}}$ has exactly $\sqrt{q}+1$ vertices more than $U_q^*[X_c]$. By Theorem 5 of [65], we can find an independent set in $U_q^*[X_c]$ with at least $.19239q^{3/4} - q^{1/2} - 1$ vertices. Call this independent set I_c.

We want to throw away the absolute points in U_q^* that are in I_c. In $U_q^*[X_c]$, the vertex $(1, a, b + c\mu)$ is an absolute point if and only if

$$b + c\mu + b + c\mu^{\sqrt{q}} = a^2$$

which, again by Lemma 4.4.2, is equivalent to

$$2b = a^2.$$

There are $\sqrt{q}$ choices for a and a given a uniquely determines b. Thus I_c contains at most $q^{1/2}$ absolute points in U_q. Let J_c be the set I_c with the absolute points removed so that $|J_c| \geq .19239q^{3/4} - 2q^{1/2} - 1$.

Define

$$I = \bigcup_{c \in \mathbb{F}_{\sqrt{q}}} J_c.$$

By Lemma 4.4.3, I is an independent set in U_q^*. Observe that

$$|I| \geq \sqrt{q}(0.19239q^{3/4} - 2q^{1/2} - 1) = 0.19239q^{5/4} - O(q)$$

and I contains no absolute points.

We note that when q is a fourth power, the coefficient 0.19239 may be raised to $\frac{1}{2}$, as Theorem 5 in [65] is stronger in this case.

4.5 Proof of Theorem 4.1.6

Let s and n be positive integers with $\frac{2n}{s} = r \geq 3$ an odd integer. Let $q = p^n$, $d = p^s$, and note that $\{q, d\}$ is an admissible pair. Let $\mathbb{F}^*_{q^2}$ be the non-zero elements of $\mathbb{F}_{q^2}$ and θ be a generator of the cyclic group $\mathbb{F}^*_{q^2}$. Write $\mathbb{F}_q$ and $\mathbb{F}_d$ for the unique subfields of $\mathbb{F}_{q^2}$ of order q and d, respectively. An identity that will be used is

$$\frac{p^{2n} - 1}{p^s - 1} = (p^s)^{r-1} + (p^s)^{r-2} + \cdots + p^s + 1.$$

It will be convenient to let

$$t = \frac{p^{2n}-1}{p^s-1} \tag{4.8}$$

and observe that t is odd since $r = \frac{2n}{s}$ is odd.

Lemma 4.5.1. *There is a $\mu \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ such that when μ^d is written in the form $\mu^d = u_1 + u_2\mu$ with $u_1, u_2 \in \mathbb{F}_q$, the element u_2 is a $(d-1)$-th power.*

Proof. Let $h(X) = X^d + (\theta^{q+1})^{d-1}X$. We claim that the roots of h are the elements in the set $Z = \{0\} \cup \{\theta^{q+1+it} : 0 \le i \le d-2\}$. Clearly 0 is a root. Let $0 \le i \le d-2$. Note that since $2n = sr$,

$$\begin{aligned} dt &\equiv p^s\left((p^s)^{r-1} + (p^s)^{r-2} + \cdots + p^s + 1\right) \\ &\equiv p^{2n} + (p^s)^{r-1} + \cdots + p^{2s} + p^s \\ &\equiv 1 + (p^s)^{r-1} + \cdots + p^{2s} + p^s \equiv t (\text{mod } p^{2n}-1). \end{aligned}$$

This implies $d(q+1+it) \equiv (q+1)(d-1) + (q+1) + it (\text{mod } q^2-1)$ so that

$$(\theta^{q+1+it})^d - (\theta^{q+1})^{d-1}\theta^{q+1+it} = 0.$$

We conclude that the roots of h are the elements in Z.

Let $\mu = \theta^{q+1+t}$. The non-zero elements of the subfield $\mathbb{F}_q$ are the elements of the subgroup $\langle\theta^{q+1}\rangle$ in $\mathbb{F}_{q^2}^*$. Since t is odd and $q+1$ is even, $q+1+t$ is not divisible by $q+1$ thus $\mu \notin \mathbb{F}_q$. Let $u_2 = (\theta^{q+1})^{d-1}$ and $u_1 = 0$. We have

$$0 = h(\mu) = \mu^d - (\theta^{q+1})^{d-1}\mu = \mu^d - u_1 - u_2\mu$$

so $\mu^d = u_1 + u_2\mu$. By construction, $\mu \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, $\mu^d = u_1 + u_2\mu$ with $u_1, u_2 \in \mathbb{F}_q$, and u_2 is a $(d-1)$-th power. □

The next lemma is known (see Exercise 7.4 in [61]). A proof is included for completeness.

Lemma 4.5.2. *If $u_2, \delta \in \mathbb{F}_{q^2}^*$ and u_2 is a $(d-1)$-th power, then for any $\xi \in \mathbb{F}_{q^2}$, the equation*

$$X^d + u_2\delta^{d-1}X = \xi$$

has a unique solution in $\mathbb{F}_{q^2}$.

Proof. Let $u_2, \delta \in \mathbb{F}_{q^2}^*$ and $g(X) = X^d + u_2\delta^{d-1}X$. The polynomial g is a permutation polynomial if and only if the only root of g is 0 (see Theorem 7.9 of [61]). If $g(X) = 0$, then $X(X^{d-1} + u_2\delta^{d-1}) = 0$. It suffices to show that $-u_2\delta^{d-1}$ is not a $(d-1)$-th power of any element of $\mathbb{F}_{q^2}$ as this would imply that the equation $X^{d-1} + u_2\delta^{d-1} = 0$ has no solutions. By hypothesis, $u_2 = w^{d-1}$ for some $w \in \mathbb{F}_{q^2}^*$. Since -1 is not a $(d-1)$-th power, the product $-u_2\delta^{d-1} = -(w\delta)^{d-1}$ is not a $(d-1)$-th power. We conclude that g is a permutation polynomial on $\mathbb{F}_{q^2}$. In particular, given any $\xi \in \mathbb{F}_{q^2}$, there is a unique solution to the equation $X^d + u_2\delta^{d-1}X = \xi$. □

For the rest of this section, we fix a $\mu \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ that satisfies the conclusion of Lemma 4.5.1; that is,

$$\mu^d = u_1 + u_2\mu$$

where $u_1, u_2 \in \mathbb{F}_q$ and u_2 is a $(d-1)$-th power in $\mathbb{F}_{q^2}$. Let

$$\mu^{d+1} = w_1 + w_2\mu$$

where $w_1, w_2 \in \mathbb{F}_q$. We fix a partition of $\mathbb{F}_q^*$ into two sets

$$\mathbb{F}_q^* = \mathbb{F}_q^+ \cup \mathbb{F}_q^- \tag{4.9}$$

where $a \in \mathbb{F}_q^+$ if and only if $-a \in \mathbb{F}_q^-$.

It will be convenient to work with a graph that is isomorphic to a large induced subgraph of G_f. By Lemma 4.5.2, the map $x \mapsto x^d + x$ is a permutation on $\mathbb{F}_{q^2}$. Therefore, every element of $\mathbb{F}_{q^2}$ can be written in the form $a^d + a$ for some $a \in \mathbb{F}_{q^2}$ and this representation is unique. Let $\mathcal{A}_{q^2,d}$ be the graph with vertex set $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ where distinct vertices $(a^d + a, x)$ and $(b^d + b, y)$ are adjacent if and only if

$$a^d b + ab^d = x + y.$$

Working with this equation defining our adjacencies will be particularly helpful for the rather technical Lemma 4.5.8 below.

Lemma 4.5.3. *The graph $\mathcal{A}_{q^2,d}$ is isomorphic to the subgraph of G_f induced by $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$.*

Proof. One easily verifies that the map $\tau : V(\mathcal{A}_{q^2,d}) \to \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ defined by

$$\tau((a^d + a, x)) = (a, x + a^{d+1})$$

is a graph isomorphism from $\mathcal{A}_{q^2,d}$ to the subgraph of G_f induced by $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$. □

Lemma 4.5.4. *If*

$$I^+ = \{(a^d + a, x_1 + x_2\mu) : a, x_1 \in \mathbb{F}_q, x_2 \in \mathbb{F}_q^+\},$$

then I^+ is an independent set in the graph $\mathcal{A}_{q^2,d}$. The same statement holds with I^- and $\mathbb{F}_q^-$ in place of I^+ and $\mathbb{F}_q^+$, respectively.

Proof. Suppose that $(a^d+a, x_1+x_2\mu)$ is adjacent to $(b^d+b, y_1+y_2\mu)$ where $a, b \in \mathbb{F}_q$. The left hand side of

$$a^d b + ab^d = (x_1 + y_1) + (x_2 + y_2)\mu$$

is in $\mathbb{F}_q$ so $x_2 + y_2 = 0$. If $x_2, y_2 \in \mathbb{F}_q^+$, then $x_2 + y_2 \neq 0$ and so no two vertices in I^+ can be adjacent. Similarly, no two vertices in I^- can be adjacent. □

Lemma 4.5.5. *For any $k = \alpha^d + \alpha \in \mathbb{F}_{q^2}$, the map*

$$\phi_k((a^d + a, x)) = (a^d + a + k, x + a^d\alpha + a\alpha^d + \alpha^{d+1})$$

is an automorphism of the graph $\mathcal{A}_{q^2,d}$.

Proof. The vertex $\phi_k((a^d + a, x))$ is adjacent to $\phi_k((b^d + b, y))$ if and only if

$$v = (a^d + a + \alpha^d + \alpha, x + a^d\alpha + a\alpha^d + \alpha^{d+1})$$

is adjacent to

$$w = (b^d + b + \alpha^d + \alpha, y + b^d\alpha + b\alpha^d + \alpha^{d+1}).$$

Since d is a power of p, $v = ((a + \alpha)^d + (a + \alpha), x + a^d\alpha + a\alpha^d + \alpha^{d+1})$. Similarly,

$$w = ((b + \alpha)^d + (b + \alpha), y + b^d\alpha + b\alpha^d + \alpha^{d+1}).$$

From this we see that v is adjacent to w if and only if

$$\begin{aligned} (a + \alpha)^d(b + \alpha) + (a + \alpha)(b + \alpha)^d = \\ x + a^d\alpha + a\alpha^d + \alpha^{d+1} + y + b^d\alpha + b\alpha^d + \alpha^{d+1}. \end{aligned} \tag{4.10}$$

A routine calculation shows that (4.10) is equivalent to the equation $a^d b + ab^d = x + y$ which holds if and only if $(a^d + a, x)$ is adjacent to $(b^d + b, y)$ in $\mathcal{A}_{q^2,d}$. □

Let $J = I^+ \cup I^-$ and observe that $J = \{(a^d + a, x_1 + x_2\mu) : a, x_1 \in \mathbb{F}_q, x_2 \in \mathbb{F}_q^*\}$. Let

$$K = \bigcup_{\beta \in \mathbb{F}_q} \phi_{(\beta\mu)^d + (\beta\mu)}(J).$$

Lemma 4.5.6. *If $\mathcal{A}_{q^2,d}[K]$ is the subgraph of $\mathcal{A}_{q^2,d}$ induced by K, then*

$$\chi(\mathcal{A}_{q^2,d}[K]) \leq 2q.$$

Proof. By Lemma 4.5.4, the vertices in J may be colored using at most 2 colors. By Lemma 4.5.5, the vertices in $\phi_k(J)$ can also be colored using at most 2 colors. Since K is the union of q sets of the form $\phi_k(J)$ where $k \in \mathbb{F}_{q^2}$, we may color K using at most $2q$ colors. □

Lemma 4.5.6 shows that we can color all but at most $O(q^3)$ vertices of $\mathcal{A}_{q^2,d}$ with at most $2q$ colors. We now show that the remaining vertices can be colored with $o(q)$ colors. Before stating the next lemma we recall that $\mu^d = u_1 + u_2\mu$ and we let $\mu^{d+1} = w_1 + w_2\mu$ where $u_1, u_2, w_1, w_2 \in \mathbb{F}_q$.

Lemma 4.5.7. *If $X = (\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}) \backslash K$, then*

$$X = \{((a + \beta\mu)^d + (a + \beta\mu), t_1 + (a^d\beta + a\beta^d u_2 + \beta^{d+1} w_2)\mu) : a, \beta, t_1 \in \mathbb{F}_q\}.$$

Proof. For any $\beta \in \mathbb{F}_q$, the set $\phi_{(\beta\mu)^d + (\beta\mu)}(J)$ can be written as

$$\{(a^d + a + (\beta\mu)^d + (\beta\mu), x_1 + x_2\mu + a^d(\beta\mu) + a(\beta\mu)^d + (\beta\mu)^{d+1}) : a, x_1 \in \mathbb{F}_q, x_2 \in \mathbb{F}_q^*\}.$$

Let $(s_1 + s_2\mu, t_1 + t_2\mu) \in \mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ where $s_1, s_2, t_1, t_2 \in \mathbb{F}_q$. The vertex $(s_1 + s_2\mu, t_1 + t_2\mu)$ is in K if we can find $a, x_1, \beta \in \mathbb{F}_q$ and $x_2 \in \mathbb{F}_q^*$ such that

$$s_1 + s_2\mu = (a + \beta\mu)^d + a + \beta\mu, \tag{4.11}$$

$$t_1 + t_2\mu = x_1 + x_2\mu + a^d(\beta\mu) + a(\beta\mu)^d + (\beta\mu)^{d+1}. \tag{4.12}$$

Since every element of $\mathbb{F}_{q^2}$ can be written as $z^d + z$ for some $z \in \mathbb{F}_{q^2}$, we can write $s_1 + s_2\mu = z^d + z$ and then choose a and β in $\mathbb{F}_q$ so that $z = a + \beta\mu$. With this choice of a and β, equation (4.11) holds.

Since $\mu^{d+1} = w_1 + w_2\mu$, equation (4.12) can be rewritten as

$$t_1 + t_2\mu = (x_1 + a\beta^d u_1 + \beta^{d+1} w_1) + (x_2 + a^d\beta + a\beta^d u_2 + \beta^{d+1} w_2)\mu. \tag{4.13}$$

Let $x_1 = t_1 - a\beta^d u_1 - \beta^{d+1} w_1$. If $t_2 \neq a^d\beta + a\beta^d u_2 + \beta^{d+1} w_2$, then we can take $x_2 = t_2 - a^d\beta - a\beta^d u_2 - \beta^{d+1} w_2$ and (4.12) holds. Therefore, the vertices in $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ not in K are those vertices in the set

$$\{((a+\beta\mu)^d + (a+\beta\mu), t_1 + (a^d\beta + a\beta^d u_2 + \beta^{d+1} w_2)\mu) : a, \beta, t_1 \in \mathbb{F}_q\}.$$

□

Lemma 4.5.8. *If $\mathcal{A}_{q^2,d}[X]$ is the subgraph of $\mathcal{A}_{q^2,d}$ induced by $X = (\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}) \backslash K$, then*

$$\chi(\mathcal{A}_{q^2,d}[X]) = O\left(\frac{q}{\log q}\right).$$

Proof. For $\beta \in \mathbb{F}_q$, partition X into the sets X_β where

$$X_\beta = \{((a+\beta\mu)^d + (a+\beta\mu), t_1 + (a^d\beta + a\beta^d u_2 + \beta^{d+1} w_2)\mu) : a, t_1 \in \mathbb{F}_q\}.$$

Fix a $\beta \in \mathbb{F}_q$ and a vertex

$$v = ((a+\beta\mu)^d + (a+\beta\mu), t_1 + (a^d\beta + a\beta^d u_2 + \beta^{d+1} w_2)\mu)$$

in X_β. Let $\gamma \in \mathbb{F}_q$. We want to count the number of vertices

$$w = ((x+\gamma\mu)^d + (x+\gamma\mu), y_1 + (x^d\gamma + x\gamma^d u_2 + \gamma^{d+1} w_2)\mu)$$

in X_γ that are adjacent to v. The vertices v and w are adjacent if and only if

$$\begin{aligned} &(a+\beta\mu)^d(x+\gamma\mu) + (a+\beta\mu)(x+\gamma\mu)^d \\ &= t_1 + y_1 + (a^d\beta + a\beta^d u_2 + \beta^{d+1} w_2 + x^d\gamma + x\gamma^d u_2 + \gamma^{d+1} w_2)\mu. \end{aligned} \tag{4.14}$$

If $\gamma = \beta$, then we can choose $x \in \mathbb{F}_q$ in q different ways and the above equation uniquely determines y_1. We conclude that the vertex $v \in X_\beta$ has at most q other neighbors in X_β.

Assume now that $\gamma \neq \beta$. We need to count how many $x, y_1 \in \mathbb{F}_q$ satisfy (4.14). A computation using the relations $\mu^d = u_1 + u_2\mu$ and $\mu^{d+1} = w_1 + w_2\mu$ shows that (4.14) is equivalent to

$$\begin{aligned} &a^d x + a^d\gamma\mu + \beta^d x(u_1 + u_2\mu) + \beta^d\gamma(w_1 + w_2\mu) \\ &+ax^d + a\gamma^d(u_1 + u_2\mu) + \beta x^d\mu + \beta\gamma^d(w_1 + w_2\mu) \\ &= t_1 + y_1 + (a^d\beta + a\beta^d u_2 + \beta^{d+1}w_2 + x^d\gamma + x\gamma^d u_2 + \gamma^{d+1}w_2)\mu. \end{aligned}$$

Equating the coefficients of μ gives

$$\begin{aligned} &a^d\gamma + \beta^d x u_2 + \beta^d\gamma w_2 + a\gamma^d u_2 + \beta x^d + \beta\gamma^d w_2 = \\ &a^d\beta + a\beta^d u_2 + \beta^{d+1}w_2 + x^d\gamma + x\gamma^d u_2 + \gamma^{d+1}w_2. \end{aligned}$$

This equation can be rewritten as

$$x^d(\gamma - \beta) + x(\gamma^d - \beta^d)u_2 = \xi \tag{4.15}$$

for some $\xi \in \mathbb{F}_q$ that depends only on a, γ, β, and μ. Since $\gamma - \beta \neq 0$, equation (4.15) is equivalent to

$$x^d + u_2(\gamma - \beta)^{d-1}x = \xi(\gamma - \beta)^{-1}. \tag{4.16}$$

By Lemma 4.5.2, (4.16) has a unique solution for x since u_2 is a $(d-1)$-power and $\gamma - \beta \in \mathbb{F}_q^*$. Once x is determined, (4.14) gives a unique solution for y_1. Therefore, v has at most one neighbor in X_β. We conclude that the degree of v in X is at most $q + (q-1) < 2q$.

The graph $\mathcal{A}_{q^2,d}[X]$ does not contain a 4-cycle and has maximum degree at most $2q$. This implies that the neighborhood of any vertex contains at most q edges. By a result of Alon, Krivelevich, and Sudakov [5], the graph $\mathcal{A}_{q^2,d}[X]$ can be colored using $O\left(\frac{q}{\log q}\right)$ colors. □

Proof of Theorem 4.1.6. Partition the vertex set of $\mathcal{A}_{q^2,d}$ as

$$V(\mathcal{A}_{q^2,d}) = K \cup X.$$

By Lemmas 4.5.6 and 4.5.8, we can color the vertices in $K \cup X$ using $2q + O\left(\frac{q}{\log q}\right)$ colors. This gives a coloring of the vertices in $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ in G_f and it only remains to color the vertices in the set $\{(m) : m \in \mathbb{F}_{q^2}\} \cup \{(\infty)\}$.

The vertex (∞) is adjacent to (m) for every $m \in \mathbb{F}_{q^2}$. Since G_f is C_4-free, the subgraph of G_f induced by the neighborhood of (∞) induces a a graph with maximum degree at most 1. We may color the vertices in $\{(m) : m \in \mathbb{F}_{q^2}\} \cup \{(\infty)\}$ using three new colors not used to color $\mathbb{F}_{q^2} \times \mathbb{F}_{q^2}$ to obtain a $2q + O(\frac{q}{\log q})$ coloring of G_f. □

4.6 Dickson Commutative Division Rings

Let p be an odd prime, $n > 1$ be an integer, $q = p^n$, and a be any element of $\mathbb{F}_q$ that is not a square. Let $1 \leq r < n$ be an integer. Let D be a 2-dimensional vector space over $\mathbb{F}_q$ with basis $\{1, \lambda\}$. Define a product $\cdot$ on D by the rule

$$(x + \lambda y) \cdot (z + \lambda t) = xz + ay^{p^r} t^{p^r} + \lambda(yz + st).$$

With this product and the usual addition, D is a commutative division ring (see [52], Theorem 9.12 and note that it is common to call such a structure a semifield). We can use D to define a projective plane Π (see [52], Theorem 5.2). This plane also has an orthogonal polarity (see [52], page 248). Let $\mathcal{GD}_{q^2}$ be the corresponding orthogonal polarity graph. Using the argument of Section 4.5, one can prove that

$$\chi(\mathcal{GD}_{q^2}) \leq 2q + \left(\frac{q}{\log q}\right).$$

A rough outline is as follows. Let $\mathcal{AD}_{q^2}$ be the subgraph of $\mathcal{GD}_{q^2}$ induced by the vertices

$$\{((x_1 + \lambda x_2, y_1 + \lambda y_2) : x_1, x_2, y_1, y_2 \in \mathbb{F}_q\}.$$

Partition $\mathbb{F}_q^*$ into the sets $\mathbb{F}_q^+$ and $\mathbb{F}_q^-$ where $a \in \mathbb{F}_q^+$ if and only if $-a \in \mathbb{F}_q^-$. The sets

$$I^+ = \{(x_2\lambda, y_1 + y_2\lambda) : x_2, y_1 \in \mathbb{F}_q, y_2 \in \mathbb{F}_q^+\}$$

and

$$I^- = \{(x_2\lambda, y_1 + y_2\lambda) : x_2, y_1 \in \mathbb{F}_q, y_2 \in \mathbb{F}_q^-\}$$

are independent sets in $\mathcal{GD}_{q^2}$. For any $k \in \mathbb{F}_q$, the map

$$\phi_k(x_1 + \lambda x_2, y_1 + \lambda y_2) = (x_1 + \lambda x_2 + k, y_1 + \lambda y_2 + kx_1 + 2^{-1}k^2 + \lambda x_2 k)$$

is an automorphism of $\mathcal{AG}_{q^2}$.

Let $J = I^+ \cup I^-$ and $K = \bigcup_{k \in \mathbb{F}_q} \phi_k(J)$ and observe that

$$K = \{(k + x_2\lambda, y_1 + y_2\lambda + 2^{-1}k^2 + \lambda x_2 k) : x_1, y_1, k \in \mathbb{F}_q, y_2 \in \mathbb{F}_q^*\}.$$

If $X = (D \times D) \backslash K$, then

$$X = \{(s_1 + s_2\lambda, t_1 + (s_2 s_1)\lambda) : s_1, s_2, t_1 \in \mathbb{F}_q\}.$$

It can then be shown that the subgraph of $\mathcal{GD}_{q^2}$ induced by X has maximum degree at most $2q$. The remaining details are left to the reader.

4.7 Concluding Remarks

The argument used to prove Theorem 4.1.4 can be extended to other unitary polarity graphs. We illustrate with an example. Let a and e be integers with $a \not\equiv \pm(\text{mod } 2e)$, $e \equiv 0(\text{mod } 4)$, and $\gcd(a, e) = 1$. Let $f : \mathbb{F}_q \to \mathbb{F}_q$ be the polynomial $f(X) = X^n$ where $n = \frac{1}{2}(3^a + 1)$ and $q = 3^e$. The map f is a planar polynomial and the corresponding plane is the Coulter-Matthews plane [25]. This plane has a unitary polarity whose action on the affine points and lines is given by

$$(x, y)^\theta = [-x^{\sqrt{q}}, -y^{\sqrt{q}}] \text{ and } (a, b)^\theta = (-a^{\sqrt{q}}, -b^{\sqrt{q}}).$$

The proof of Theorem 4.1.4 can be modified to show that the corresponding unitary polarity graph has an independent set of size $\frac{1}{2}q^{5/4} - o(q^{5/4})$ that contains no absolute points. The reason for the condition $e \equiv 0(\text{mod } 4)$ instead of $e \equiv 0(\text{mod } 2)$, which is the condition given in [25] for f to be planar, is that we need $\sqrt{q}$ to be a square in order to apply Theorem 4.1.1 to the subgraphs that correspond to the $U_q^*[X_c]$ in the proof of Theorem 4.1.4.

Chapter 4 is a version of the material in "Independent sets in polarity graphs", co-authored with Craig Timmons, which has been submitted for publication. The author was the primary investigator and author of this paper.

5

Sidon Sets

"Which way does Jensen's inequality go again?"

– anonymous second-year graduate student

5.1 Introduction

The study of Sidon sets dates back to the 1930s, when Simon Sidon [75] studied sets of integers A with the property that $|\{a_1, a_2 \in A : a_1 + a_2 = k\}|$ is bounded. He then asked Erdős how large a subset of $[n]$ can be if all of its sums are distinct. Such a set is now called a *Sidon set*. That is, A is a Sidon set if for $a, b, c, d \in A$, $a + b = c + d$ implies that $\{a, b\} = \{c, d\}$. Since Sidon asked this question, hundreds of papers have been written on Sidon sets and their generalizations (see [4, 12, 19, 31, 34, 43, 62, 63, 66, 72, 77] for an incomplete list).

One such generalization is to introduce a graph to the question. A Sidon set is when *all* pairs of sums are distinct. By specifying a graph, one may choose which pairs of sums must be distinct. Given a graph G, a *sum-injective labeling* of G is an injection $\chi : V(G) \to \mathbb{Z}$ such that $\chi(u) + \chi(v) \neq \chi(x) + \chi(y)$ for distinct edges $uv, xy \in E(G)$. A Sidon set then represents a sum-injective labeling of the complete graph with loops on each vertex. Let $S(G)$ be the smallest integer N such that G admits a sum-injective labeling from $V(G)$ to $[N]$. Old results on Sidon sets imply that $S(K_n) = (1+o(1))n^2$. Surprisingly, Bollobás and Pikhurko [10] showed

that there are graphs with only $n^{3/2+o(1)}$ edges also giving $S(G) = (1+o(1))n^2$.

The main result of this chapter shows that a similar phenomenon happens when one considers products instead of sums. Let G be a graph. We analogously define a *product-injective labeling* of G to be an injection $\chi : V(G) \to \mathbb{Z}$ such that $\chi(u) \cdot \chi(v) \neq \chi(x) \cdot \chi(y)$ for distinct edges $uv, xy \in E(G)$. Let $P(G)$ denote the smallest positive integer N such that there is a product-injective labeling $\chi : V(G) \to [N]$. Our main results of the chapter give asymptotically tight bounds on $P(G)$ relative to the maximum degree d and number of vertices of the graph G, for all but a small range of values of $d \leq n-1$. Let $P(n,d)$ be the maximum possible value of $P(G)$ over n-vertex graphs G of maximum degree at most d. Specifically, we prove the following theorem:

Theorem 5.1.1. *There exist constants $a, b > 0$ such that* (i) $P(n,d) \sim n$ *if* $d \leq n^{1/2}(\log n)^{-a}$ *and* (ii) $P(n,d) \sim n \log n$ *if* $d \geq n^{1/2}(\log n)^{b}$.

An old result of Erdős [31] implies $P(K_n) \sim n \log n$, whereas Theorem 5.1.1 shows that $P(G) \sim n \log n$ for graphs which are much sparser than K_n. The labeling of the vertices of any n-vertex graph G with the first n prime numbers is always a product-injective labeling from $[N]$ where $N \sim n \log n$, via the Prime Number Theorem. Theorem 5.1.1 then is an analogous result for products that Bollobás and Pikhurko [10] proved for sums and differences, where a change in behavior was also observed around $d = n^{1/2}$. Theorem 5.1.1 will be proved with $a > \log 2$ and $b > 5.5$; while our method allows these values to be slightly improved, new ideas would be needed to determine $P(n,d)$ for all the intermediate values of d. In fact, the proof of Theorem 5.1.1(ii) establishes the much stronger result that if G is the random graph on n vertices with edge-probability d/n and $d \geq n^{1/2}(\log n)^{b}$, then $P(G) \sim n \log n$ almost surely as $n \to \infty$. We also remark that Theorem 5.1.1 determines the maximum value of $P(G)$ over n-vertex graphs with m edges for almost all possible values of m.

It is a natural question to ask about other functions besides sums and products. Let H be a k-uniform hypergraph and denote by K_n^k the complete k-uniform hypergraph on n vertices. If ϕ is a general symmetric function of k variables, then $S_\phi(H)$ is the minimum integer N such that there exists an injection

$c : V(H) \to [N]$ such that whenever $\{v_1, v_2, \ldots, v_k\}, \{w_1, w_2, \ldots, w_k\} \in E(H)$ are distinct hyperedges, $\phi(c(v_1), c(v_2), \ldots, c(v_k)) \neq \phi(c(w_1), c(w_2), \ldots, c(w_k))$.

The question of determining $S(G)$ and $P(G)$ then is the case when $k = 2$ and $\phi(x, y) = x+y$ or $\phi(x, y) = x \cdot y$ respectively. For general H and ϕ, this quantity depends on number theoretic questions involving the number of representations of integers as evaluations of ϕ. For instance, if $k = 2$ and $\phi(x, y) = (xy)^2 + x + y$ and $\phi(x, y) = \phi(u, v)$, then it is not hard to show $\{x, y\} = \{u, v\}$ and therefore $S_\phi(G) = n$ for every n-vertex graph G. Define

$$R_\phi(N) = \sum_{\substack{x,y \in [N]^k \\ x \neq y}} \mathbf{1}_{\phi(x)=\phi(y)}.$$

This is the number of ways of writing integers in two ways as evaluations of ϕ on $[N]^k$. We prove the following general theorem:

Theorem 5.1.2. *Let $\phi : \mathbb{Z}^k \to \mathbb{Z}$ be a symmetric function, and let H be an n-vertex k-uniform graph of maximum degree $d \geq 1$ such that for $N \geq 8kn$,*

$$\frac{R_\phi(N)}{N^{2k}} \leq \frac{1}{4d^2 n}.$$

Then $S_\phi(H) \leq \max\{N, 4n\}$.

A difficult open question in combinatorial number theory is to determine the largest Sidon subset of the integer squares $\{x^2 : x^2 \leq N\}$, which is equivalent to determining $S_\phi(K_n)$ when $\phi(x, y) = x^2 + y^2$. In 1990, Cilleruelo [23] constructed a Sidon sequence of squares $\{a_k\}$, where $a_k \ll k^4$. Theorem 5.1.2 applies to $\phi(x, y) = x^2 + y^2$, and in this case $R_\phi(N) = O(N^2 \log N)$ [59], and therefore if G is an n-vertex graph of maximum degree d:

$$S_\phi(G) = O(d\sqrt{n \log n} + n). \tag{5.1}$$

Note that this gives $S_\phi(G) = O(n)$ for G with maximum degree $O(\sqrt{n/\log n})$. If $\phi_r(x_1, x_2, \ldots, x_k) = x_1^r + x_2^r + \cdots + x_k^r$, then Euler's Extended Conjecture states that $\phi_r(x) = \phi_r(y)$ has no non-trivial solutions if $r > 2k$, which would show $S_\phi(K_n^k) = n$. It seems plausible that for $k < r \leq 2k$, the number of solutions $(x, y) \in [N]^k \times [N]^k$ is $O(N)$, which would give $S_\phi(K_n^k) = O(n)$. In the special case

$\phi(x,y) = x^3 + y^3$, Euler (see Hardy and Wright [46], pages 199-200) determined all solutions to $x^3 + y^3 = z^3 + w^3$ in the rationals. A complete solution in the positive integers is given by Choudhry [18]. Hooley [51], showed that for $\phi(x,y) = x^3 + y^3$, $R_\phi(N) = cN^{4/3} + o(N^{4/3})$ and therefore if G is an n-vertex graph of maximum degree d, then

$$S_\phi(G) = O(d^{3/4}n^{3/8} + n). \tag{5.2}$$

Note that this gives $S_\phi(G) = O(n)$ for G with maximum degree $O(n^{5/6})$. Using (5.1) and (5.2) we have the following theorem as a corollary:

Theorem 5.1.3. *There is a Sidon set $A \subset [n^2]$ such that every term of A is a square and $|A| \gg n^{1/3-o(1)}$. There is a Sidon set $B \subset [n^3]$ such that every term of B is a cube and $|B| \gg n^{8/9}$.*

The chapter is organized as follows. The proof of Theorem 5.1.1 uses the modified local lemma, which we state in Section 5.2, together with some facts on the distribution of the number of divisors function τ. The proof of Theorem 5.1.1(i) is given in Section 5.3, and Theorem 5.1.1(ii) is proved in Section 5.4. Theorem 5.1.2 is proved in Section 5.5.

5.2 Preliminaries

To prove Theorem 5.1.1, we make use of a probabilistic result known as the modified local lemma, together with some well-known facts from analytic number theory regarding the number of divisors of positive integers.

Modified local lemma. The modified local lemma, which is a version of the Lovász Local Lemma (see Alon and Spencer [7], page 65), is used in the following form:

Proposition 5.2.1. *Let $A_1, ..., A_n$ be events in a probability space and for each $i \in [n]$, let (J_i, K_i) be a partition of $[n]\backslash\{i\}$. If there exists $\gamma \in [0,1)$ such that for all i and any choice $K_i' \subset K_i$,*

$$\mathbb{P}\left(A_i \mid \bigcap_{k \in K_i'} \overline{A}_k\right) \leq \gamma(1 - |J_i|\gamma)$$

then

$$\mathbb{P}\left(\bigcap_{i=1}^{n} \overline{A}_i\right) > 0.$$

We note that Proposition 5.2.1 can be made stronger as well as nonsymmetric, but we will not require this.

Distribution of the number of divisors. For a natural number k, let $\tau(k)$ be the number of divisors of k, and let $\Omega(k)$ be the number of prime power divisors of k. The Hardy-Ramanujan Theorem [45] gives $|\{x \leq N : |\Omega(x) - \log\log N| \gg \sqrt{\log\log N}\}| \ll N$ as $N \to \infty$. Since $\tau(n) \leq 2^{\Omega(n)}$, one has the following result:

Proposition 5.2.2.

$$|\{n \leq N : \tau(n) \geq (\log N)^{\log 2} 2^{\kappa(N)\sqrt{\log\log N}}\}| \ll N,$$

for any function κ with $\kappa(N) \to \infty$ as $N \to \infty$.

In fact it turns out that Ω and $\log\tau$ have normal orders – for more on normal orders see Tenenbaum [83].

5.3 Proof of Theorem 5.1.1(i)

We show that $P(G) \sim n$ for any graph G with $V(G) = [n]$ and maximum degree

$$d \leq n^{1/2}(\log n)^{-\log 2} 2^{-\kappa(n)\sqrt{\log\log n}},$$

where $\kappa(n) \to \infty$ and $\kappa(n) \leq (\log\log n)^{1/4}$. This in turn shows that Theorem 5.1.1(i) holds for any $a > \log 2$. Let $m = \lceil 4n/\kappa(n) \rceil$, and let L be the set of the first $n + m$ natural numbers with at most

$$t = \kappa(n)^{-1}(\log n)^{\log 2} 2^{\kappa(n)\sqrt{\log\log n}}$$

divisors. Since $\kappa(n) \leq (\log\log n)^{1/4}$ and $m \ll n$, Proposition 5.2.2 shows that

$$\max L \sim n + m \sim n.$$

Now uniformly and randomly select an n-element subset $\{\ell_1, \ell_2, \ldots, \ell_n\}$ of L and define the injective labeling $\chi(i) = \ell_i$. For an unordered pair $\{xy, uv\} \in \binom{E(G)}{2}$ of distinct edges of G, let $A_{xy,uv}$ be the event that $\chi(x)\chi(y) = \chi(u)\chi(v)$ and define

$$J_{xy,uv} = \{A_{jk,rs} : \{j,k,r,s\} \cap \{x,y,u,v\} \neq \emptyset\}$$

and

$$K_{xy,uv} = \{A_{jk,rs} : \{j,k,r,s\} \cap \{x,y,u,v\} = \emptyset\}.$$

We apply the modified local lemma, Proposition 5.2.1, to the events $A_{xy,uv}$. The set

$$M := L \backslash \{\chi(z) : z \in V(G) \backslash \{u,v,x,y\}\}$$

has size $m+4$. For any labels $\chi(u), \chi(v)$, the number of ways of choosing

$$\chi(x), \chi(y) \in M$$

such that $\chi(x)\chi(y) = \chi(u)\chi(v)$ is at most

$$\tau(\chi(u)\chi(v)) \leq \tau(\chi(u))\tau(\chi(v)) \leq t^2.$$

Now, given a labeling of $\{z \in V(G) \setminus \{u,v,x,y\}\}$, the set M is fixed. Therefore, given any labeling of $\{z \in V(G) \setminus \{u,v,x,y\}\}$, choosing the labels of x, y, u, v uniformly from M yields that the probability that $\chi(x)\chi(y) = \chi(u)\chi(v)$ is bounded above by

$$\frac{t^2}{\binom{|M|}{2}} < \frac{2t^2}{m^2}.$$

Since this upper bound did not depend on the choice of M, it holds for any labeling of $\{z \in V(G) \setminus \{u,v,x,y\}\}$. Note that once M has been determined, labeling x, y, u, v from M does not affect whether or not events in $K_{xy,uv}$ occur. Therefore, given any choice of $K \subset K_{xy,uv}$

$$\mathbb{P}(A_{xy,uv} \mid \bigcap_{\{jk,rs\} \in K} \overline{A}_{jk,rs}) \leq \mathbb{P}(A_{xy,uv} \text{ occurs when labeling from } M) < \frac{2t^2}{m^2}.$$

For any $\{xy, uv\} \in \binom{E(G)}{2}$,

$$|J_{xy,uv}| \leq 4d|E(G)| \leq 2d^2 n.$$

Taking $\gamma = 1/(4d^2n)$, and using $m^2 \geq 16d^2t^2n$, we find

$$\gamma(1 - \gamma|J_{xy,uv}|) \geq \frac{1}{8d^2n} \geq \frac{2t^2}{m^2}.$$

By the modified local lemma, the probability that none of the events $A_{xy,uv}$ occur is positive. In other words, there exists a product-injective labeling $\chi : V(G) \to [N]$ where $N = \max L \sim n$. □

5.4 Proof of Theorem 5.1.1(ii)

In this section, we prove that labeling with primes is asymptotically optimal for graphs that are much less dense than K_n, namely for the random graph $G_{n,d/n}$ with $d \geq n^{1/2}(\log n)^b$ and $b > 5.5$. Since $G_{n,d/n}$ for $d \geq n^{1/2}(\log n)^b$ has maximum degree asymptotic to d, this is enough for Theorem 5.1.1(ii). Throughout this section, if H is a graph then $C_4(H)$ is the number of 4-cycles in H.

5.4.1 Counting 4-cycles

Lemma 5.4.1. *Let $B = B(U, V)$ be a bipartite graph with $|U| = m$ and $|V| = n$, and let d be the average degree of the vertices in V. If $nd^2 \geq 4m^2$ and $d \geq 2$, then*

$$C_4(B) \geq \frac{n^2d^4}{64m^2}.$$

Proof. This is a standard exercise in applying Jensen's Inequality, but we include the proof for completeness. Let $d(u, v)$ be the codegree of u and v, that is, the number of vertices of B adjacent to both u and v. Then the number $C_4(B)$ of 4-cycles in B is precisely

$$C_4(B) = \sum_{\{u,v\} \subset U} \binom{d(u,v)}{2}.$$

Let $M = \binom{m}{2}$. By Jensen's Inequality, and since

$$\sum_{\{u,v\} \subset U} d(u, v) = \sum_{w \in V} \binom{d(w)}{2},$$

we have

$$C_4(B) \geq M\binom{\frac{1}{M}\sum_{w\in V}\binom{d(w)}{2}}{2}.$$

By Jensen's Inequality again,

$$\sum_{w\in V}\binom{d(w)}{2} \geq n\binom{d}{2}.$$

Therefore

$$C_4(B) \geq M\binom{\frac{n}{M}\binom{d}{2}}{2}.$$

Since $nd^2 \geq 4m^2$, and $\binom{x}{2} \geq \frac{1}{4}x^2$ for $x \geq 2$,

$$\frac{n}{M}\binom{d}{2} \geq \frac{nd^2}{2m^2} \geq 2.$$

Using $\binom{x}{2} \geq \frac{1}{4}x^2$ again for $x \geq 2$,

$$C_4(B) \geq \frac{n^2d^4}{64M} \geq \frac{n^2d^4}{64m^2}.$$

This proves the lemma. □

5.4.2 Counting solutions to $uv = xy$

A solution to $uv = xy$ is non-trivial if $\{u, v\} \neq \{x, y\}$.

Lemma 5.4.2. *For all $\varepsilon > 0$, there exist $\delta > 0$ and $n_0(\varepsilon)$ such that for $n \geq n_0(\varepsilon)$, if $A \subset [n]$ and $|A| \geq (1+\varepsilon)n/\log n$, then the number of non-trivial quadruples $\{a, b, c, d\} \in \binom{A}{4}$ satisfying $ab = cd$ is at least $\delta n^2(\log n)^{-10}(\log\log n)^{-2}$.*

Proof. We shall prove the lemma with $\delta = 2^{-14}\varepsilon^4$ and $n \geq n_0(\varepsilon)$, where $n_0(\varepsilon)$ is the smallest positive integer such that for $n \geq n_0(\varepsilon)$,

$$\frac{\varepsilon\sqrt{n}}{(2\log n)^2} \geq 2. \tag{5.3}$$

$$\frac{1}{\log\log n} \leq \frac{\varepsilon^2}{2^7}. \tag{5.4}$$

$$(1+\tfrac{1}{2}\varepsilon)\frac{n}{\log n} \geq \pi(n). \tag{5.5}$$

$$8(\log n)^{12}(\log\log n)^3 < 16\delta^{1/2}n/\log n. \tag{5.6}$$

Note that (5.5) is possible since $\pi(n) \sim n/\log n$ by the Prime Number Theorem.

Consider the bipartite graph $H = H(U, V)$ with parts $U = [n^{2/3}] \cup P$ and $V = \left[n^{1/2}\right]$, where P comprises the primes in the interval $[n^{2/3}, n]$. Erdős [31] made the following observation:

for any $a \in [n]$, there exist $u_a \in U$ and $v_a \in V$ such that $a = u_a v_a$ and $u_a \geq v_a$.

Therefore, for each $a \in A$, choose a unique representation $u_a v_a = a$ with $u_a \in U$ and $v_a \in V$ (note that there may be many choices; choose one arbitrarily).

Now define $E(H)$ by $uv \in E(H)$ if there exists an $a \in A$ with $u = u_a$ and $v = v_a$.

Consequently, $|E(H)| = |A|$. If $\{uv, vw, wx, xu\}$ is a 4-cycle in H, then $uv, wx \in A$ and $vw, xu \in A$ and $(uv)(wx) = (vw)(ux)$. Therefore $C_4(H)$ is a lower bound for the number of non-trivial solutions to $ab = cd$ with $a, b, c, d \in A$. For the remainder of the proof, we show $C_4(H) \geq \delta n^2 (\log n)^{-10} (\log\log n)^{-2}$.

Let k_0 be the largest integer k such that $2^{k+1} < n^{1/2}(\log n)^{-4}(\log\log n)^{-1}$. For $1 \leq k \leq k_0$, let

$$U_k := \{u \in U : 2^{k-1} n^{1/2} \leq u < 2^k n^{1/2}\} \quad \text{and} \quad V_k := \{v \in V : v \leq 2^{1-k} n^{1/2}\}.$$

Denote by H_k the subgraph of H induced by U_k and V_k. Also, let H_0 be the subgraph of H induced by U_0 and V_0, where

$$U_0 = \{u \in U : u \leq n^{1/2}\} \quad \text{and} \quad V_0 = \{v \in V : v \leq n^{1/2}\}.$$

Finally, let H_* be the subgraph of H induced by U_* and V_*, where

$$U_* = \left\{u \in U : u > \frac{n}{2(\log n)^4 \log\log n}\right\}$$
$$V_* = \left\{v \in V : v \leq 2(\log n)^4 \log\log n\right\}.$$

Then $H = H_* \bigcup_{k=0}^{k_0} H_k$. We consider the subgraphs $H_k : k \geq 0$ separately from H_*.

Claim 1. *If for some* $k \in \{0\} \cup [k_0]$, $|E(H_k)| \geq \varepsilon n/(2\log n)^2$, *then* $C_4(H_k) \geq \delta n^2(\log n)^{-10}(\log\log n)^{-2}$.

Proof. The average degree in H_k of vertices in V_k is

$$d = \frac{|E(H_k)|}{|V_k|} \geq \frac{\varepsilon 2^{k-1} n^{1/2}}{(2\log n)^2}.$$

Since $n \geq n_0(\varepsilon)$, (5.3) gives $d \geq 2$. Now

$$|V_k|d^2 = \frac{|E(H_k)|^2}{|V_k|} \geq \frac{\varepsilon^2 2^{k-1} n^{3/2}}{(2\log n)^4},$$

and so (5.4) and $2^{k_0} < n^{1/2}(\log n)^{-4}(\log\log n)^{-1}$ gives

$$|V_k|d^2 = |E(H_k)|^2/|V_k| \geq 4|U_k|^2.$$

By Lemma 5.4.1 with $m = |U_k|$,

$$C_4(H_k) \geq \frac{\varepsilon^4 n^2}{2^{14}(\log n)^8} = \delta n^2(\log n)^{-8} > \delta n^2(\log n)^{-10}(\log\log n)^{-2}.$$

This proves the claim. □

Since $C_4(H) \geq C_4(H_k)$, we are done if $|E(H_k)| \geq \varepsilon n/(2\log n)^2$ for some $k \in [k_0]$, so we assume this is not the case for any $k \in [k_0]$. Then

$$\sum_{k=1}^{k_0} |E(H_k)| \leq \frac{\varepsilon k_0 n}{(2\log n)^2} < \frac{\varepsilon n}{4\log n}. \tag{5.7}$$

Next we consider H_*.

Claim 2. *If* $C_4(H) < \delta n^2(\log n)^{-10}(\log\log n)^{-2}$, *then*

$$|E(H_*)| < \pi(n) + \frac{16\delta^{1/2} n}{\log n}. \tag{5.8}$$

Proof. Let $\tilde{U}_*$ comprise all vertices of U_* of degree at least two in H_* and let $\tilde{H}_*$ be the subgraph of H_* induced by $\tilde{U}_* \cup V_*$. Then

$$|E(H_* \backslash \tilde{H}_*)| \leq |U_*| \leq \pi(n). \tag{5.9}$$

Now we will have proved the claim if we can show that $|E(\tilde{H}_*)| \leq 16\delta^{1/2} n/\log n$. First we show that we may assume that $|\tilde{U}_*| \geq |V_*|^2$. For if not, then we have

$$|E(\tilde{H}_*)| \le |V_*|^3 = 8(\log n)^{12}(\log\log n)^3$$

and we would be done by (5.6). Therefore we may assume $|\tilde{U}_*| \ge |V_*|^2$.

Let d be the average degree in $\tilde{H}_*$ of the vertices in $\tilde{U}_*$. Then $d \ge 2$ and $|\tilde{U}_0|d^2 \ge 4|\tilde{U}_0| \ge 4|V_0|^2$. By Lemma 5.4.1 with $m = |V_0|$,

$$C_4(\tilde{H}_0) \ge \frac{|\tilde{U}_0|^2 d^4}{64m^2} \ge \frac{|E(\tilde{H}_0)|^2}{64m^2}. \tag{5.10}$$

Since $C_4(H_*) < \delta n^2(\log n)^{-10}(\log\log n)^{-2}$ and $m \le 2(\log n)^4 \log\log n$, (5.10) gives

$$|E(\tilde{H}_0)| < 8\delta^{1/2}(\log n)^{-5}(\log\log n)^{-1}mn < \frac{16\delta^{1/2}n}{\log n}.$$

Together with (5.9), this completes the proof of Claim 2. □

We now complete the proof of the lemma. By (5.7) and (5.8),

$$|E(H)| \le |E(H_*) + \sum_{k=0}^{k_0} |E(H_k)| < \pi(n) + \frac{16\delta^{1/2}n}{\log n} + \frac{\varepsilon n}{4\log n}.$$

Since $\delta = 2^{-14}\varepsilon^4$, the last two terms above are at most $\varepsilon n/2\log n$. By (5.5), $\pi(n) \le (1+\varepsilon/2)n/\log n$, so we conclude $|E(H)| < (1+\varepsilon)n/\log n$. Since $|A| = |E(H)|$ and $|A| \ge (1+\varepsilon)n/\log n$, this contradiction completes the proof. □

5.4.3 Proof of Theorem 5.1.1(ii)

Let $\varepsilon > 0$, and let δ be given by Lemma 5.4.2. Let $p = (\log n)^b/\sqrt{n}$ with $b > 5.5$. For a fixed labeling $\chi : V(G_{n,p}) \to \mathbb{Z}$, let $\mathbb{P}(\chi)$ denote the probability that χ is a product-injective labeling of $G = G_{n,p}$. To prove Theorem 5.1.1(ii), we show that if $n \ge (1+\varepsilon)N/\log N$, then the expected number E of product-injective labelings $\chi : V(G) \to [N]$ satisfies

$$E = \sum_{\chi : V(G) \to [N]} \mathbb{P}(\chi) \le \binom{N}{n} \max_{\chi} \mathbb{P}(\chi) \ll 1. \tag{5.11}$$

To prove this, we show $\mathbb{P}(\chi) \ll N^{-n}$ for every fixed labeling $\chi : V(G) \to [N]$. Let $k \in [N^2]$, and let g_k be the number of representations (for the given function χ) of the form $k = \chi(i)\chi(j)$. That is g_k is the number of pairs $\{i,j\}$ with $i \ne j$

such that $k = \chi(i)\chi(j)$. Then for χ to be product-injective, for each k, at most one of the g_k possible edges $\{i, j\}$ with $k = \chi(i)\chi(j)$ may be selected to be in the random graph G. For each k, let A_k be the event that at most one edge $\{i, j\}$ with $\chi(i)\chi(j) = k$ is selected to be an edge of the random graph. Then by the union bound, $\mathbb{P}(A_k) \leq (1-p)^{g_k} + g_k p(1-p)^{g_k-1}$. Since the events $\{A_k\}$ are independent, we have

$$\mathbb{P}(\chi) \leq \prod_{k=1}^{N^2} \left((1-p)^{g_k} + g_k p(1-p)^{g_k-1}\right). \tag{5.12}$$

For a real-valued function f, let $f_+ = \max\{f, 0\}$. Then by Lemma 5.4.2, if $n \geq n_0(\varepsilon)$, then

$$\sum_{k=1}^{N^2} (g_k - 1)_+ \geq \frac{\delta n^2}{(\log n)^{10}(\log\log n)^2}. \tag{5.13}$$

For $x \geq 1$ let $h(x) = ((1-p)^x + xp(1-p)^{x-1})$. One may check that $\log h(x)$ is a concave function. Thus, if $g_i \geq g_j + 2$ and $g_j \geq 1$, we have $h(g_j)h(g_i) \leq h(g_j + 1)h(g_i - 1)$.

Therefore, if $g_i \geq g_j + 2$ and $g_j \geq 1$, then (5.12) increases by replacing g_i with $g_i - 1$ and g_j with $g_j + 1$. So by (5.13)

$$\mathbb{P}(\chi) \leq \left((1-p)^2 + 2p(1-p)\right)^g = (1-p^2)^g \leq e^{-p^2 g},$$

where $g = \delta n^2(\log n)^{-10}(\log\log n)^{-2}$. Since $p^2 g = \delta n(\log n)^{2b-10}(\log\log n)^{-2} \gg n\log n$, $\mathbb{P}(\chi) \ll n^{-2n} \ll N^{-n}$. This proves (5.11), and completes the proof of Theorem 5.1.1(ii). □

5.5 Proof of Theorem 5.1.2

The proof is similar to that of Theorem 5.1.1(i). We show that if H is an n-vertex k-uniform hypergraph of maximum degree d, then

$$S_\phi(G) \leq N$$

whenever $R_\phi(N)/N^{2k} \leq 1/4d^2 n$ and $N \geq 8kn$. Randomly label the vertices of G with integers in $[N]$, and let $l(v)$ be the label of vertex v. Let $A_{u,v}$ be the event

that vertices $u, v \in V(G)$ receive the same label, and let $B_{e,f}$ be the event that $\phi(l(v) : v \in e) = \phi(l(v) : v \in f)$ for edges $e, f \in H$. Then

$$\mathbb{P}(A_{u,v}) = \frac{1}{N} \quad \text{and} \quad \mathbb{P}(B_{e,f}) = \frac{R_\phi(N)}{N^{2k}}.$$

An event $A_{u,v}$ or $B_{e,f}$ is mutually independent with any set of events $A_{x,y}$ and $B_{g,h}$ such that $\{x, y\} \cap \{u, v\} = \emptyset$ and $(g \cup h) \cap \{u, v\} = \emptyset$. Therefore $A_{u,v}$ is mutually independent with a set of at least $\binom{n}{2} - 2n$ other events $A_{x,y}$ and a set of at least $2d \cdot |H| \leq 2d^2n/k$ events $B_{g,h}$, and $B_{e,f}$ is mutually independent with a set of at least $\binom{|H|}{2} - 2kd \cdot |H| \geq \binom{|H|}{2} - 2d^2n$ other events $B_{g,h}$ and at least $\binom{n}{2} - 2kn$ events $A_{x,y}$. By the local lemma, if for some $\gamma, \delta \in (0, 1)$ we have

$$\frac{1}{N} \leq \gamma(1-\gamma)^{2n}(1-\delta)^{2d^2n/k} \quad \frac{R_\phi(N)}{N^{2k}} \leq \delta(1-\gamma)^{2kn}(1-\delta)^{2d^2n}$$

then with positive probability none of the events $A_{u,v}$ and $B_{g,h}$ occur, in which case the coloring has a chance of being ϕ-injective. Select $\gamma = 1/2kn$ and $\delta = 1/2d^2n$. Then it is sufficient that

$$\frac{1}{N} \leq \frac{1}{8kn} \quad \text{and} \quad \frac{R_\phi(N)}{N^{2k}} \leq \frac{1}{8d^2n}$$

and these are satisfied by the assumptions in the theorem. This proves Theorem 5.1.2. □

Chapter 5 is a version of the material appearing in "On sets of integers with restrictions on their products", *European Journal of Combinatorics*, 51, (2016), 268–274, co-authored with Jacques Verstraëte. The author was the primary investigator and author of this paper.

6

Equations and Sum-Product Estimates in Finite Quasifields

"It's exactly like linear algebra. Linear algebra's an unbelievably specific subject. And in fact, there's only, like, two things in all of linear algebra. There's all these definitions and mumbo-jumbo. But basically, there's only Gaussian elimination and the eigenvalue problem. And absolutely every single problem in linear algebra is some variant on Gaussian elimination or the eigenvalue problem. And yet despite being able to describe linear algebra in such a banal way, it's one of the most important subjects in mathematics because of its applications."

– Jim Agler

6.1 Introduction

Let R be a ring and $A \subset R$. The *sum set* of A is the set $A + A = \{a + b : a, b \in A\}$, and the *product set* of A is the set $A \cdot A = \{a \cdot b : a, b \in A\}$. A well-studied problem in arithmetic combinatorics is to prove non-trivial lower bounds on the quantity

$$\max\{|A + A|, |A \cdot A|\}$$

under suitable hypotheses on R and A. One of the first results of this type is due to Erdős and Szemerédi [33]. They proved that if $R = \mathbb{Z}$ and A is finite, then there are positive constants c and ϵ, both independent of A, such that

$$\max\{|A + A|, |A \cdot A|\} \geq c|A|^{1+\epsilon}.$$

This improves the trivial lower bound of $\max\{|A + A|, |A \cdot A|\} \geq |A|$. Erdős and Szemerédi conjectured that the correct exponent is $2 - o(1)$ where $o(1) \to 0$ as $|A| \to \infty$. Despite a significant amount of research on this problem, this conjecture is still open. For some time the best known exponent was $4/3 - o(1)$ due to Solymosi [78] who proved that for any finite set $A \subset \mathbb{R}$,

$$\max\{|A + A|, |A \cdot A|\} \geq \frac{|A|^{4/3}}{2(\log |A|)^{1/3}}.$$

Another case that has received attention is when R is a finite field. Let p be a prime and let $A \subset \mathbb{Z}_p$. Bourgain, Katz, and Tao [13] proved that if $p^\delta < |A| < p^{1-\delta}$ where $0 < \delta < 1/2$, then

$$\max\{|A + A|, |A \cdot A|\} \geq c|A|^{1+\epsilon} \tag{6.1}$$

for some positive constants c and ϵ depending only on δ. Hart, Iosevich, and Solymosi [48] obtained bounds that give an explicit dependence of ϵ on δ. Let q be a power of an odd prime, $\mathbb{F}_q$ be the finite field with q elements, and $A \subset \mathbb{F}_q$. In [48], it is shown that if $|A + A| = m$ and $|A \cdot A| = n$, then

$$|A|^3 \leq \frac{cm^2 n|A|}{q} + cq^{1/2}mn \tag{6.2}$$

where c is some positive constant. Inequality (6.2) implies a non-trival sum-product estimate when $q^{1/2} \ll |A| \ll q$. The most general setting where a sum-product estimate has been shown to hold is in [81], where Tao shows that such an estimate holds in an arbitrary ring as long as, roughly speaking, A is not too close to a subring and does not contain too many zero divisors. Using a graph theoretic approach, Vinh [86] and Vu [89] improved (6.2) and as a result, obtained a better sum-product estimate.

Theorem 6.1.1 ([86]). *Let q be a power of an odd prime. If $A \subset \mathbb{F}_q$, $|A+A| = m$ and $|A \cdot A| = n$, then*

$$|A|^2 \leq \frac{mn|A|}{q} + q^{1/2}\sqrt{mn}.$$

Corollary 6.1.2 ([86]). *If q is a power of an odd prime and $A \subset \mathbb{F}_q$, then there is a positive constant c such that the following hold. If $q^{1/2} \ll |A| < q^{2/3}$, then*

$$\max\{|A+A|, |A \cdot A|\} \geq \frac{c|A|^2}{q^{1/2}}.$$

If $q^{2/3} \leq |A| \ll q$, then

$$\max\{|A+A|, |A \cdot A|\} \geq c(q|A|)^{1/2}.$$

In the case that q is a prime, Corollary 6.1.2 was proved by Garaev [41] using exponential sums. Cilleruelo [24] also proved related results using dense Sidon sets in finite groups involving $\mathbb{F}_q$ and $\mathbb{F}_q^*$. In particular, versions of Theorem 6.1.3 and (6.3) (see below) are proved in [24], as well as several other results concerning equations in $\mathbb{F}_q$ and sum-product estimates.

Theorem 6.1.1 was proved using the following Szemerédi-Trotter type theorem in $\mathbb{F}_q$.

Theorem 6.1.3 ([86]). *Let q be a power of an odd prime. If P is a set of points and L is a set of lines in $\mathbb{F}_q^2$, then*

$$|\{(p,l) \in P \times L : p \in l\}| \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|}.$$

We remark that a Szemerédi-Trotter type theorem in $\mathbb{Z}_p$ was obtained in [13] using the sum-product estimate (6.1).

In this chapter, we generalize Theorem 6.1.1, Corollary 6.1.2, and Theorem 6.1.3 to finite quasifields. Any finite field is a quasifield. There are many examples of quasifields which are not fields; see for example, Chapter 5 of [28] or Chapter 9 of [52]. Quasifields appear extensively in the theory of projective planes.

Theorem 6.1.4. *Let Q be a finite quasifield with q elements. If $A \subset Q\backslash\{0\}$, $|A+A| = m$ and $|A \cdot A| = n$, then*

$$|A|^2 \leq \frac{mn|A|}{q} + q^{1/2}\sqrt{mn}.$$

Theorem 6.1.4 gives the following sum-product estimate.

Corollary 6.1.5. *Let Q be a finite quasifield with q elements and $A \subset Q\backslash\{0\}$. There is a positive constant c such that the following hold.*

If $q^{1/2} \ll |A| < q^{2/3}$, then

$$\max\{|A+A|, |A\cdot A|\} \geq c\frac{|A|^2}{q^{1/2}}.$$

If $q^{2/3} \leq |A| \ll q$, then

$$\max\{|A+A|, |A\cdot A|\} \geq c(q|A|)^{1/2}.$$

From Corollary 6.1.5 we conclude that any algebraic object that is rich enough to coordinatize a projective plane must satisfy a non-trivial sum-product estimate. Following [86], we prove a Szemerédi-Trotter type theorem and then use it to deduce Theorem 6.1.4.

Theorem 6.1.6. *Let Q be a finite quasifield with q elements. If P is a set of points and L is a set of lines in Q^2, then*

$$|\{(p,l) \in P \times L : p \in l\}| \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|}.$$

Another consequence of Theorem 6.1.6 is the following corollary.

Corollary 6.1.7. *If Q is a finite quasifield with q elements and $A \subset Q$, then there is a positive constant c such that*

$$|A\cdot(A+A)| \geq c\min\left\{q, \frac{|A|^3}{q}\right\}.$$

Furthermore, if $|A| \gg q^{2/3}$, then one may take $c = 1 + o(1)$.

The next result generalizes Theorem 1.1 from [88].

Theorem 6.1.8. *Let Q be a finite quasifield with q elements. If $A, B, C \subset Q$, then*

$$|A + B\cdot C| \geq q - \frac{q^3}{|A||B||C| + q^2}$$

Our methods in proving the above results can be used to generalize theorems concerning the solvability of equations over finite fields. Let p be a prime and let $A, B, C, D \subset \mathbb{Z}_p$. Sárközy [73] proved that if $N(A, B, C, D)$ is the number of solutions to $a + b = cd$ with $(a, b, c, d) \in A \times B \times C \times D$, then

$$\left| N(A, B, C, D) - \frac{|A||B||C||D|}{p} \right| \leq p^{1/2} \sqrt{|A||B||C||D|}. \tag{6.3}$$

In particular, if $|A||B||C||D| > p^3$, then there is an $(a, b, c, d) \in A \times B \times C \times D$ such that $a + b = cd$. This is best possible up to a constant factor (see [73]). It was generalized to finite fields of odd prime power order by Gyarmati and Sárközy [44], and then by the Vinh [85] to systems of equations over $\mathbb{F}_q$. Here we generalize the result of Gyarmati and Sárközy to finite quasifields.

Theorem 6.1.9. *Let Q be a finite quasifield with q elements and let $A, B, C, D \subset Q$. If $\gamma \in Q$ and $N_\gamma(A, B, C, D)$ is the number of solutions to $a + b + \gamma = c \cdot d$ with $a \in A$, $b \in B$, $c \in C$, and $d \in D$, then*

$$\left| N_\gamma(A, B, C, D) - \frac{(q+1)|A||B||C||D|}{q^2 + q + 1} \right| \leq q^{1/2} \sqrt{|A||B||C||D|}.$$

Theorem 6.1.9 implies the following Corollary which generalizes Corollary 3.5 in [87].

Corollary 6.1.10. *If Q is a finite quasifield with q elements and $A, B, C, D \subset Q$ with $|A||B||C||D| > q^3$, then*

$$Q = A + B + C \cdot D.$$

We also prove a higher dimensional version of Theorem 6.1.9.

Theorem 6.1.11. *Let $d \geq 1$ be an integer. If Q is a finite quasifield with q elements and $A \subset Q$ with $|A| > q^{\frac{d+2}{2d+2}}$, then*

$$Q = A + A + \underbrace{A \cdot A + \cdots + A \cdot A}_{d \text{ terms}}.$$

Another problem considered by Sárközy was the solvability of the equation $ab + 1 = cd$ over $\mathbb{Z}_p$. Sárközy [74] proved a result in $\mathbb{Z}_p$ which was later generalized to the finite field setting in [44].

Theorem 6.1.12 (Gyarmati, Sárközy)**.** *Let q be a power of a prime and*

$$A, B, C, D \subset \mathbb{F}_q.$$

If $N(A, B, C, D)$ is the number of solutions to $ab + 1 = cd$ with $a \in A$, $b \in B$, $c \in C$, and $d \in D$, then

$$\left| N(A, B, C, D) - \frac{|A||B||C||D|}{q} \right| \leq 8q^{1/2}(|A||B||C||D|)^{1/2} + 4q^2.$$

Our generalization to quasifields is as follows.

Theorem 6.1.13. *Let Q be a finite quasifield with q elements and kernel K. Let $\gamma \in Q\backslash\{0\}$, and $A, B, C, D \subset Q$. If $N_\gamma(A, B, C, D)$ is the number of solutions to $a \cdot b + c \cdot d = \gamma$, then*

$$\left| N_\gamma(A, B, C, D) - \frac{|A||B||C||D|}{q} \right| \leq q \left(\frac{|A||B||C||D|}{|K| - 1} \right)^{1/2}.$$

Corollary 6.1.14. *Let Q be a quasifield with q elements whose kernel is K. If $A, B, C, D \subset Q$ and $|A||B||C||D| > q^4(|K| - 1)^{-1}$, then*

$$Q\backslash\{0\} \subset A \cdot B + C \cdot D.$$

By appropriately modifying the argument used to prove Theorem 6.1.13, we can prove a higher dimensional version.

Theorem 6.1.15. *Let Q be a finite quasifield with q elements whose kernel is K. If $A \subset Q$ and $|A| > q^{\frac{1}{2}+\frac{1}{d}}(|K| - 1)^{-1/2d}$, then*

$$Q\backslash\{0\} \subset \underbrace{A \cdot A + \cdots + A \cdot A}_{d \text{ terms}}.$$

If Q is a finite field, then $|K| = q$, and the bounds of Theorems 6.1.13 and 6.1.15 match the bounds obtained by Hart and Iosevich in [47].

The rest of the chapter is organized as follows. In Section 6.2 we collect some preliminary results. Section 6.3 contains the proof of Theorem 6.1.4, 6.1.6, and 6.1.9, as well as Corollary 6.1.5, 6.1.7, and 6.1.10. Section 6.4 contains the proof of Theorems 6.1.8, 6.1.11, 6.1.13, and 6.1.15.

6.2 Preliminaries

We begin this section by recalling the definition of a quasifield. A set L with a binary operation $\cdot$ is called a *loop* if

1. the equation $a \cdot x = b$ has a unique solution in x for every $a, b \in L$,
2. the equation $y \cdot a = b$ has a unique solution in y for every $a, b \in L$, and
3. there is an element $e \in L$ such that $e \cdot x = x \cdot e = x$ for all $x \in L$.

A *(left) quasifield* Q is a set with two binary operations $+$ and $\cdot$ such that $(Q, +)$ is a group with additive identity 0, $(Q^*, \cdot)$ is a loop where $Q^* = Q \backslash \{0\}$, and the following three conditions hold:

1. $a \cdot (b + c) = a \cdot b + a \cdot c$ for all $a, b, c \in Q$,
2. $0 \cdot x = 0$ for all $x \in Q$, and
3. the equation $a \cdot x = b \cdot x + c$ has exactly one solution for every $a, b, c \in Q$ with $a \neq b$.

We use 1 to denote the identity in the loop $(Q^*, \cdot)$. It is a consequence of the definition that $(Q, +)$ must be an abelian group. One also has $x \cdot 0 = 0$ and $x \cdot (-y) = -(x \cdot y)$ for all $x, y \in Q$ (see [52], Lemma 7.1). For more on quasifields, see Chapter 9 of [52]. A *(right) quasifield* is required to satisfy the right distributive law instead of the left distributive law. The *kernel* K of a quasifield Q is the set of all elements $k \in Q$ that satisfy

1. $(x + y) \cdot k = x \cdot k + y \cdot k$ for all $x, y \in Q$, and
2. $(x \cdot y) \cdot k = x \cdot (y \cdot k)$ for all $x, y \in Q$.

Note that $(K, +)$ is an abelian subgroup of $(Q, +)$ and $(K^*, \cdot)$ is a group.

Lemma 6.2.1. *If $a \in Q$ and $\lambda \in K$, then $-(a \cdot \lambda) = (-a) \cdot \lambda$.*

Proof. First we show that $a \cdot (-1) = -a$. Indeed, $a \cdot (1 + (-1)) = a \cdot 0 = 0$ and so $a + a \cdot (-1) = 0$. We conclude that $-a = a \cdot (-1)$. If $\lambda \in K$, then

$$\begin{aligned} -(a \cdot \lambda) &= a \cdot (-\lambda) = a \cdot (0 - \lambda) = a \cdot ((0-1) \cdot \lambda) \\ &= (a \cdot (0-1)) \cdot \lambda = (0 + a \cdot (-1)) \cdot \lambda = (-a) \cdot \lambda. \end{aligned}$$

□

For the rest of this section, we assume that Q is a finite quasifield with $|Q| = q$. We can construct a projective plane $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ that is coordinatized by Q. We will follow the notation of [52] and refer the reader to Chapter 5 of [52] for more details. Let ∞ be a symbol not in Q. The points of Π are

$$\mathcal{P} = \{(x, y) : x, y \in Q\} \cup \{(x) : x \in Q\} \cup \{(\infty)\}.$$

The lines of Π are

$$\mathcal{L} = \{[m, k] : m, k \in Q\} \cup \{[m] : m \in Q\} \cup \{[\infty]\}.$$

The incidence relation $\mathcal{I}$ is defined according to the following rules:

1. $(x, y)\mathcal{I}[m, k]$ if and only if $m \cdot x + y = k$,
2. $(x, y)\mathcal{I}[k]$ if and only if $x = k$,
3. $(x)\mathcal{I}[m, k]$ if and only if $x = m$,
4. $(x)\mathcal{I}[\infty]$ for all $x \in Q$, $(\infty)\mathcal{I}[k]$ for all $k \in Q$, and $(\infty)\mathcal{I}[\infty]$.

Since $|Q| = q$, the plane Π has order q.

Next we associate a graph to the plane Π. Let $\mathcal{G}(\Pi)$ be the bipartite graph with parts $\mathcal{P}$ and $\mathcal{L}$ where $p \in \mathcal{P}$ is adjacent to $l \in \mathcal{L}$ if and only if $p\mathcal{I}l$ in Π. The first lemma is known (see [14], page 432).

Lemma 6.2.2. *The graph $\mathcal{G}(\Pi)$ has eigenvalues $q + 1$ and $-(q + 1)$, each with multiplicity one. All other eigenvalues of $\mathcal{G}(\Pi)$ are $\pm q^{1/2}$.*

The next lemma is a bipartite discrepancy inequality.

Lemma 6.2.3 (Bipartite Expander Mixing Lemma)**.** *Let G be a d-regular bipartite graph on $2n$ vertices with parts X and Y. Let M be the adjacency matrix of G. Let $d = \lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_{2n} = -d$ be the eigenvalues of M and define $\lambda = \max_{i \neq 1,2n} |\lambda_i|$. If $S \subset X$ and $T \subset Y$, then*

$$\left| e(S,T) - \frac{d|S||T|}{n} \right| \leq \lambda \sqrt{|S||T|}.$$

Proof. Assume that the columns of M have been been ordered so that the columns corresponding to the vertices of X come before the columns corresponding to the vertices of Y. For a subset $B \subset V(G)$, let χ_B be the characteristic vector for B. Let $\{x_1, \ldots, x_{2n}\}$ be an orthonormal set of eigenvectors for M. Note that since G is a d-regular bipartite graph, we have

$$x_1 = \frac{1}{\sqrt{2n}} (\chi_X + \chi_Y), \tag{6.4}$$

$$x_{2n} = \frac{1}{\sqrt{2n}} (\chi_X - \chi_Y). \tag{6.5}$$

Now $\chi_S^T M \chi_T = e(S,T)$. Expanding χ_S and χ_T as linear combinations of eigenvectors yields

$$e(S,T) = \left(\sum_{i=1}^{2n} \langle \chi_S, x_i \rangle x_i \right)^T M \left(\sum_{i=1}^{2n} \langle \chi_T, x_i \rangle x_i \right) = \sum_{i=1}^{2n} \langle \chi_S, x_i \rangle \langle \chi_T, x_i \rangle \lambda_i.$$

Now by (6.4) and (6.5), $\langle \chi_S, x_1 \rangle = \langle \chi_S, x_{2n} \rangle = \frac{1}{\sqrt{2n}}|S|$ and $\langle \chi_T, x_1 \rangle = -\langle \chi_T, x_{2n} \rangle = \frac{1}{\sqrt{2n}}|T|$. Since $\lambda_1 = -\lambda_{2n} = d$, we have

$$\begin{aligned}
\left| e(S,T) - \frac{2d|S||T|}{2n} \right| &= \left| \sum_{i=2}^{2n-1} \langle \chi_S, x_i \rangle \langle \chi_T, x_i \rangle \lambda_i \right| \\
&\leq \lambda \sum_{i=2}^{2n-1} |\langle \chi_S, x_i \rangle \langle \chi_T, x_i \rangle| \\
&\leq \lambda \left(\sum_{i=2}^{2n-1} \langle \chi_S, x_i \rangle^2 \right)^{1/2} \left(\sum_{i=2}^{2n-1} \langle \chi_T, x_i \rangle^2 \right)^{1/2}.
\end{aligned}$$

Where the last inequality is by Cauchy-Schwarz. Finally by the Pythagorean Theorem,

$$\sum_{i=2}^{2n-1} \langle \chi_S, x_i \rangle^2 = |S| - \frac{2|S|^2}{2n} < |S|$$

and

$$\sum_{i=2}^{2n-1} \langle \chi_T, x_i \rangle^2 = |T| - \frac{2|T|^2}{2n} < |T|.$$

□

Combining Lemmas 6.2.2 and 6.2.3 gives the next lemma.

Lemma 6.2.4. *For any $S \subset \mathcal{P}$ and $T \subset \mathcal{L}$,*

$$\left| e(S,T) - \frac{(q+1)|S||T|}{q^2+q+1} \right| \leq q^{1/2}\sqrt{|S||T|}$$

where $e(S,T)$ is the number of edges in $\mathcal{G}(\Pi)$ with one endpoint in S and the other in T.

We now state precisely what we mean by a line in Q^2.

Definition 6.2.5. *Given $a, b \in Q$, a line in Q^2 is a set of the form*

$$\{(x,y) \in Q^2 : y = b \cdot x + a\} \quad or \quad \{(a,y) : y \in Q\}.$$

When multiplication is commutative, $b \cdot x + a = x \cdot b + a$. In general, the binary operation $\cdot$ need not be commutative and so we write our lines with the slope on the left.

The next lemma is due to Elekes [30] (see also [82], page 315). In working in a (left) quasifield, which is not required to satisfy the right distributive law, some care must be taken with algebraic manipulations.

Lemma 6.2.6. *Let $A \subset Q^*$. There is a set P of $|A+A||A \cdot A|$ points and a set L of $|A|^2$ lines in Q^2 such that there are at least $|A|^3$ incidences between P and L.*

Proof. Let $P = (A+A) \times (A \cdot A)$ and

$$l(a,b) = \{(x,y) \in Q^2 : y = b \cdot x - b \cdot a\}.$$

Let $L = \{l(a,b) : a, b \in A\}$. The statement that $|P| = |A+A||A \cdot A|$ is clear from the definition of P. Suppose $l(a,b)$ and $l(c,d)$ are elements of L and $l(a,b) = l(c,d)$. We claim that $(a,b) = (c,d)$. In a quasifield, one has $x \cdot 0 = 0$ for every x, and

$x \cdot (-y) = -(x \cdot y)$ for every x and y ([52], Lemma 7.1). The line $l(a, b)$ contains the points $(0, -b \cdot a)$ and $(1, b - b \cdot a)$. Furthermore, these are the unique points in $l(a, b)$ with first coordinate 0 and 1, respectively. Similarly, the line $l(c, d)$ contains the points $(0, -d \cdot c)$ and $(1, d - d \cdot c)$. Since $l(a, b) = l(c, d)$, we must have that $-b \cdot a = -d \cdot c$ and $b - b \cdot a = d - d \cdot c$. Thus, $b = d$ and so $b \cdot a = b \cdot c$. We can rewrite this equation as $b \cdot a - b \cdot c = 0$. Since $-x \cdot y = x \cdot (-y)$ and Q satisfies the left distributive law, we have $b \cdot (a - c) = 0$. If $a = c$, then $(a, b) = (c, d)$ and we are done. Assume that $a \neq c$ so that $a - c \neq 0$. Then we must have $b = 0$ for if $b \neq 0$, then the product $b \cdot (a - c)$ would be contained in Q^* as multiplication is a binary operation on Q^*. Since $A \subset Q^*$, we have $b \neq 0$. It must be the case that $a = c$. We conclude that each pair $(a, b) \in A^2$ determines a unique line in L and so $|L| = |A|^2$.

Consider a triple $(a, b, c) \in A^3$. The point $(a + c, b \cdot c)$ belongs to P and is incident to $l(a, b) \in L$ since

$$b \cdot (a + c) - b \cdot a = b \cdot a + b \cdot c - b \cdot a = b \cdot c.$$

Each triple in A^3 generates an incidence and so there are at least $|A|^3$ incidences between P and L. □

6.3 Proof of Theorem 6.1.4, 6.1.6, and 6.1.9

Throughout this section, Q is a finite quasifield with q elements, $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ is the the projective plane coordinatized by Q as in Section 6.2. The graph $\mathcal{G}(\Pi)$ is the bipartite graph defined before Lemma 6.2.2 in Section 6.2.

Proof of Theorem 6.1.6. Let $P \subset Q^2$ be a set of points and view P as a subset of $\mathcal{P}$. Let $r(a, b) = \{(x, y) \in Q^2 : y = b \cdot x + a\}$, $R \subset Q^2$, and let

$$L = \{r(a, b) : (a, b) \in R\}$$

be a collection of lines in Q^2. The point $p = (p_1, p_2)$ in P is incident to the line $r(a, b)$ in L if and only if $p_2 = b \cdot p_1 + a$. This however is equivalent to

$(p_1, -p_2)\mathcal{I}[b, -a]$ in Π. If $S = \{(p_1, -p_2) : (p_1, p_2) \in P\}$ and $T = \{[b, -a] : (a, b) \in R\}$, then

$$|\{(p, l) \in P \times L : p \in l\}| = e(S, T)$$

where $e(S, T)$ is the number of edges in $\mathcal{G}(\Pi)$ with one endpoint in S and the other in T. By Lemma 6.2.4,

$$|\{(p, l) \in P \times L : p \in l\}| \leq \frac{|S||T|}{q} + q^{1/2}\sqrt{|S||T|}$$

which proves Theorem 6.1.6. □

Proof of Theorem 6.1.4 and Corollary 6.1.5. Let $A \subset Q^*$. Let $S = (A + A) \times (A \cdot A)$. We view S as a subset of $\mathcal{P}$. Let $s(a, b) = \{(x, y) \in Q^2 : y = b \cdot x - b \cdot a\}$ and

$$L = \{s(a, b) : a, b \in A\}.$$

By Lemma 6.2.6, $|L| = |A|^2$ and there are at least $|A|^3$ incidences between S and L. Let $T = \{[-b, -b \cdot a] : a, b \in A\}$ so T is a subset of $\mathcal{L}$. By Lemma 6.2.4,

$$e(S, T) \leq \frac{|S||T|}{q} + q^{1/2}\sqrt{|S||T|}.$$

We have $|L| = |T| = |A|^2$. If $m = |A + A|$ and $n = |A \cdot A|$, then

$$e(S, T) \leq \frac{mn|A|^2}{q} + q^{1/2}|A|\sqrt{mn}.$$

Next we find a lower bound on $e(S, T)$. By construction, an incidence between S and L corresponds to an edge between S and T in $\mathcal{G}(\Pi)$. To see this, note that $(x, y) \in S$ is incident to $s(a, b) \in L$ if and only if $y = b \cdot x - b \cdot a$. This is equivalent to the equation $-b \cdot x + y = -b \cdot a$ which holds if and only if (x, y) is adjacent to $[-b, -b \cdot a]$ in $\mathcal{G}(\Pi)$. Thus,

$$|A|^3 \leq e(S, T) \leq \frac{mn|A|^2}{q} + q^{1/2}|A|\sqrt{mn}. \tag{6.6}$$

To prove Corollary 6.1.5, observe that from (6.6), we have

$$|A + A||A \cdot A| \geq \min\left\{cq|A|, \frac{c|A|^4}{q}\right\}$$

where c is any real number with $c + c^{1/2} < 1$. If $x = \max\{|A + A|, |A \cdot A|\}$, then $x \geq \min\{(cq|A|)^{1/2}, \frac{c^{1/2}|A|^2}{q^{1/2}}\}$ and Corollary 6.1.5 follows from this inequality. □

Proof of Corollary 6.1.7. Let $A \subset Q$, $P = A \times (A \cdot (A + A))$,

$$l(b, c) = \{(x, y) \in Q^2 : y = b \cdot (x + c)\},$$

and $L = \{l(b, c) : b, c \in A\}$. Then $|P| = |A||A \cdot (A + A)|$, $|L| = |A|^2$, and L is a set of lines in Q^2. Let $z = |A \cdot (A + A)|$. Observe that each $l(b, c) \in L$ contains at least $|A|$ points from P. By Theorem 6.1.6,

$$|A|^3 \leq \frac{|P||L|}{q} + q^{1/2}\sqrt{|P||L|} = \frac{|A|^3 z}{q} + q^{1/2}|A|^{3/2}z^{1/2}.$$

This implies that $q|A|^{3/2} \leq |A|^{3/2}z + q^{3/2}\sqrt{z}$. Therefore,

$$\sqrt{z} \geq \frac{-q^{3/2} + \sqrt{q^3 + 4|A|^3 q}}{2|A|^{3/2}} = \frac{4|A|^3 q}{2|A|^{3/2}(q^{3/2} + \sqrt{q^3 + 4|A|^3 q})},$$

which implies that

$$|A \cdot (A + A)| \geq c \min\left\{q, \frac{|A|^3}{q}\right\}.$$

We note that if $|A| \gg q^{2/3}$ then we can take $c = 1 + o(1)$. □

Proof of Theorem 6.1.9 and Corollary 6.1.10. Let $A, B, C, D \subset Q$. Consider the sets $P = \{(d, -a) : d \in D, a \in A\}$ and $L = \{[c, b + \gamma] : c \in C, b \in B\}$. An edge between P and L in $\mathcal{G}(\Pi)$ corresponds to a solution to $c \cdot d + (-a) = b + \gamma$ with $c \in C$, $d \in D$, $a \in A$, and $b \in B$. Therefore, $e(P, L)$ is precisely the number of solutions to $a + b + \gamma = c \cdot d$ with $(a, b, c, d) \in A \times B \times C \times D$. Observe that $|P| = |D||A|$ and $|L| = |C||B|$. By Lemma 6.2.4,

$$\left|N_\gamma(A, B, C, D) - \frac{(q + 1)|A||B||C||D|}{q^2 + q + 1}\right| \leq q^{1/2}\sqrt{|A||B||C||D|}.$$

To obtain Corollary 6.1.10, apply Theorem 6.1.9 with A, B, C, and $-D$. For any $-\gamma \in Q$, the number of $(a, b, c, -d) \in A \times B \times C \times (-D)$ with $a + b - \gamma = c \cdot (-d)$ is at least

$$\frac{(q + 1)|A||B||C|| - D|}{q^2 + q + 1} - q^{1/2}\sqrt{|A||B||C|| - D|}. \tag{6.7}$$

When $|A||B||C||D| > q^3$, (6.7) is positive and so we have a solution to $a + b - \gamma = c \cdot (-d)$. Since this equation is equivalent to $a + b + c \cdot d = \gamma$ and γ was arbitrary, we get

$$Q = A + B + C \cdot D.$$

□

6.4 Proof of Theorems 6.1.8, 6.1.11, 6.1.13, and 6.1.15

Let Q be a finite quasifield with q elements and let K be the kernel of Q. Let $d \geq 1$ be an integer and $\gamma \in Q$. The *product graph*, denoted $\mathcal{DP}_Q(d, \gamma)$, is the bipartite graph with parts X and Y where X and Y are disjoint copies of Q^{d+1}. The vertex $(x_1, \ldots, x_{d+1})_X \in X$ is adjacent to $(y_1, \ldots, y_{d+1})_Y \in Y$ if and only if

$$x_{d+1} + \gamma = x_1 \cdot y_1 + x_2 \cdot y_2 + \cdots + x_d \cdot y_d + y_{d+1}. \tag{6.8}$$

Lemma 6.4.1. *The graph $\mathcal{DP}_Q(d, \gamma)$ is q^d-regular.*

Proof. Fix a vertex $(x_1, \ldots, x_{d+1})_X \in X$. We can choose $y_1, \ldots, y_d$ arbitrarily and then (6.8) gives a unique solution for y_{d+1}. Therefore, $(x_1, \ldots, x_{d+1})_X$ has degree q^d. A similar argument shows that every vertex in Y has degree q^d. □

Lemma 6.4.2. *If $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$ are the eigenvalues of $\mathcal{DP}_Q(d, \gamma)$, then $|\lambda| \leq q^{d/2}$ where $\lambda = \max_{i \neq 1,n} |\lambda_i|$.*

Proof. Let M be the adjacency matrix of $\mathcal{DP}_Q(d, \gamma)$. Assume that the first q^{d+1} rows/columns of M correspond to the vertices of X. We can write

$$M = \begin{pmatrix} 0 & N \\ N^T & 0 \end{pmatrix}$$

where N is the $q^{d+1} \times q^{d+1}$ matrix whose $(x_1, \ldots, x_{d+1})_X \times (y_1, \ldots, y_{d+1})_Y$-entry is 1 if (6.8) holds, and is 0 otherwise. Let J be the $q^{d+1} \times q^{d+1}$ matrix of all 1's and let

$$P = \begin{pmatrix} 0 & J \\ J & 0 \end{pmatrix}.$$

We claim that

$$M^3 = q^d M + q^d(q^{d-1} - 1)P. \tag{6.9}$$

The (x, y)-entry of M^3 is the number of walks of length 3 from $x = (x_1, \ldots, x_{d+1})_X$ to $y = (y_1, \ldots, y_{d+1})_Y$. Suppose that $xy'x'y$ is such a walk where

$$y' = (y'_1, \ldots, y'_{d+1})_Y \quad \text{and} \quad x' = (x'_1, \ldots, x'_{d+1})_X.$$

By Lemma 6.4.1, there are q^d vertices $x' \in X$ such that x' is adjacent to y. In order for $xy'x'y$ to be a walk of length 3, y' must be adjacent to both x and x' so we need

$$x_{d+1} = x_1 \cdot y'_1 + \cdots + x_d \cdot y'_d + y'_{d+1} \tag{6.10}$$

and

$$x'_{d+1} = x'_1 \cdot y'_1 + \cdots + x'_d \cdot y'_d + y'_{d+1}. \tag{6.11}$$

We want to count the number of y' that satisfy both (6.10) and (6.11). We consider two cases.

Case 1: x is not adjacent to y.

If $x_i = x'_i$ for $1 \leq i \leq d$, then (6.10) and (6.11) imply that $x_{d+1} = x'_{d+1}$. This implies $x = x'$ and so x is adjacent to y but this contradicts our assumption that x is not adjacent to y. Therefore, $x_i \neq x'_i$ for some $1 \leq i \leq d$. Without loss of generality, assume that $x_1 \neq x'_1$. Subtracting (6.11) from (6.10) gives

$$x_{d+1} - x'_{d+1} = x_1 \cdot y'_1 + \cdots + x_d \cdot y'_d - x'_1 \cdot y'_1 - \cdots - x'_d \cdot y'_d. \tag{6.12}$$

Choose $y'_2, \ldots, y'_d \in Q$. Since Q is a quasifield and $x_1 - x'_1 \neq 0$, there is a unique solution for y'_1 in (6.12). Equation (6.10) then gives a unique solution for y'_{d+1} and so there are q^{d-1} choices for $y' = (y'_1, \ldots, y'_{d+1})_Y$ for which both (6.10) and (6.11) hold. In this case, the number of walks of length 3 from x to y is $(q^d - 1)q^{d-1}$ since x' may be chosen in $q^d - 1$ ways as we require $(x'_1, x'_2, \ldots, x'_d) \neq (x_1, x_2, \ldots, x_d)$ otherwise $x = x'$.

Case 2: x is adjacent to y.

The same counting as in Case 1 shows that there are $(q^d - 1)q^{d-1}$ paths $xy'x'y$ with $x \neq x'$. By Lemma 6.4.1, there are q^d paths of the form $xy'xy$ since the degree of x is q^d.

From the two cases, we deduce that

$$M^3 = q^d M + q^{d-1}(q^d - 1)P.$$

Let λ_j be an eigenvalue of M with $j \neq 1$ and $j \neq n$. Let v_j be an eigenvector for λ_j. Since v_j is orthogonal to $\chi_X + \chi_Y$ and $\chi_X - \chi_Y$, we have $Pv_j = 0$ and so

$$M^3 v_j = q^d M v_j.$$

This gives $\lambda_j^3 = q^d \lambda_j$ so $|\lambda_j| \leq q^{d/2}$. □

Proof of Theorem 6.1.8. Let $A, B, C \subset Q$ where Q is a finite quasifield with q elements. Given $\gamma \in Q$, let

$$Z_\gamma = \{(a, b, c) \in A \times B \times C : a + b \cdot c = \gamma\}.$$

We have $\sum_\gamma |Z_\gamma| = |A||B||C|$ so by the Cauchy-Schwarz inequality,

$$|A|^2|B|^2|C|^2 = \left(\sum_\gamma |Z_\gamma|\right)^2 \leq |A + B \cdot C| \sum_{\gamma \in Q} |Z_\gamma|^2. \tag{6.13}$$

Let $x = \sum_\gamma |Z_\gamma|^2$. By (6.13),

$$|A + B \cdot C| \geq \frac{|A|^2|B|^2|C|^2}{x}. \tag{6.14}$$

The integer x is the number of ordered triples (a, b, c), (a', b', c') in $A \times B \times C$ such that $a + b \cdot c = a' + b' \cdot c'$. This equation can be rewritten as

$$a = b \cdot (-c) + b' \cdot c' + a'.$$

This is equivalent to the statement that $(b, b', a)_X$ is adjacent to $(-c, c', a')_Y$ in the graph $\mathcal{DP}_Q(2, 0)$. Thus, x is the number of edges between the sets

$$S = \{(b, b', a)_X : a \in A, b, b' \in B\}$$

and

$$T = \{(-c, c', a')_Y : a' \in A, c, c' \in C\}$$

in $\mathcal{DP}_Q(2, 0)$. By Lemma 6.2.4 and Lemma 6.4.2,

$$x = e(S, T) \leq \frac{|S||T|}{q} + q^{1/2}\sqrt{|S||T|}.$$

This inequality together with (6.14) gives

$$\frac{|A|^2|B|^2|C|^2}{|A + B \cdot C|} \leq x \leq \frac{|A|^2|B|^2|C|^2}{q} + q|A||B||C|$$

from which we deduce

$$|A + B \cdot C| \geq q - \frac{q^3}{|A||B||C| + q^2}$$

□

Proof of Theorem 6.1.11. Let $A \subset Q$, $S = A \times \cdots \times A \times (-A) \subset Q^{d+1}$, and $T = A \times \cdots \times A \times A \subset Q^{d+1}$. View S as a subset X and T as a subset of Y in the graph $\mathcal{DP}_Q(\gamma, d)$. By Lemmas 6.2.4 and 6.4.2,

$$\left| e(S,T) - \frac{q^d |S||T|}{q^{d+1}} \right| \leq 2q^{d/2}\sqrt{|S||T|}.$$

An edge between S and T corresponds to a solution to

$$-a_{d+1} + \gamma = a_1 \cdot a_1' + \cdots + a_d \cdot a_d' + a_{d+1}'$$

with $a_i, a_i' \in A$. If $|A| > q^{\frac{d+2}{2d+2}}$, then $e(S,T) > 0$. Since γ is an arbitrary element of Q, we get

$$Q = A + A + \underbrace{A \cdot A + \cdots + A \cdot A}_{d \text{ terms}}$$

which completes the proof of Theorem 6.1.11. □

Proof of Theorem 6.1.13. We will work in the graph $\mathcal{DP}_Q(2,0)$. Let $\gamma \in Q^*$ and $A, B, C, D \subset Q$. For each pair $(b,d) \in B \times D$, define

$$L_\gamma(b,d) = \{(b \cdot \lambda, d \cdot \lambda, -\gamma \cdot \lambda)_Y : \lambda \in K^*\}.$$

Claim 1: If $(a,c) \in A \times C$ and $a \cdot b + c \cdot d = \gamma$, then $(a,c,0)_X$ is adjacent to every vertex in $L_\gamma(b,d)$.

Proof. Assume $(a,c) \in A \times C$ satisfies $a \cdot b + c \cdot d = \gamma$. If $\lambda \in K^*$, then

$$a \cdot (b \cdot \lambda) + c \cdot (d \cdot \lambda) = (a \cdot b) \cdot \lambda + (c \cdot d) \cdot \lambda = (a \cdot b + c \cdot d) \cdot \lambda = \gamma \cdot \lambda.$$

Therefore, $0 = a \cdot (b \cdot \lambda) + c \cdot (d \cdot \lambda) - \gamma \cdot \lambda$ which shows that $(a,c,0)_X$ is adjacent to $(b \cdot \lambda, d \cdot \lambda, -\gamma \cdot \lambda)_Y$.

Claim 2: If $(b_1, d_1) \neq (b_2, d_2)$, then $L_\gamma(b_1, d_1) \cap L_\gamma(b_2, d_2) = \emptyset$.

Proof. Suppose that $L_\gamma(b_1, d_1) \cap L_\gamma(b_2, d_2) \neq \emptyset$. There are elements $\lambda, \beta \in K^*$ such that

$$(b_1 \cdot \lambda, d_1 \cdot \lambda, -\gamma \cdot \lambda)_Y = (b_2 \cdot \beta, d_2 \cdot \beta, -\gamma \cdot \beta)_Y.$$

This implies

$$b_1 \cdot \lambda = b_2 \cdot \beta, \quad d_1 \cdot \lambda = d_2 \cdot \beta, \quad \text{and} \quad \gamma \cdot \lambda = \gamma \cdot \beta.$$

Since $\gamma \cdot \lambda = \gamma \cdot \beta$, we have $\gamma \cdot (\lambda - \beta) = 0$. As $\gamma \neq 0$, we must have $\lambda = \beta$ so $b_1 \cdot \lambda = b_2 \cdot \beta = b_2 \cdot \lambda$. Using Lemma 6.2.1,

$$0 = b_1 \cdot \lambda - (b_2 \cdot \lambda) = b_1 \cdot \lambda + (-b_2) \cdot \lambda = (b_1 - b_2) \cdot \lambda.$$

Since $\lambda \neq 0$, we have $b_1 = b_2$. A similar argument shows that $d_1 = d_2$.

Let $S = \{(a, c, 0)_X : a \in A, c \in C\}$ and

$$T = \bigcup_{(b,d) \in B \times D} L_\gamma(b, d).$$

The number of edges between S and T in $\mathcal{DP}_Q(2, 0)$ is $N_\gamma(|K| - 1)$ where N_γ is the number of 4-tuples $(a, b, c, d) \in A \times B \times C \times D$ such that $a \cdot b + c \cdot d = \gamma$. Furthermore $|S| = |A||C|$ and $|T| = |B||D|(|K|-1)$ by Claim 2. By Lemmas 6.2.4 and 6.4.2,

$$\left| N_\gamma(|K| - 1) - \frac{|S||T|}{q} \right| \leq q\sqrt{|S||T|}. \tag{6.15}$$

This equation is equivalent to

$$\left| N_\gamma - \frac{|A||B||C||D|}{q} \right| \leq q \left(\frac{|A||B||C||D|}{|K| - 1} \right)^{1/2}$$

which completes the proof of Theorem 6.1.13. □

The proof of Theorem 6.1.15 is similar to the proof of Theorem 6.1.13. Instead of working with the graph $\mathcal{DP}_Q(2, 0)$, one works with the graph $\mathcal{DP}_Q(d, 0)$. One counts edges between the sets

$$S = \{(a'_1, \ldots, a'_d, 0)_X : a'_i \in A\}$$

and

$$T = \bigcup_{(a_1, \ldots, a_d) \in A^d} L_\gamma(a_1, \ldots, a_d)$$

where $L_\gamma(a_1, \ldots, a_d) = \{(a_1 \cdot \lambda, \ldots, a_d \cdot \lambda, -\gamma \cdot \lambda)_Y : \lambda \in K^*\}$. The remaining details are left to the reader.

Chapter 6 is a version of the material in "A Szemerédi-Trotter type theorem, sum-product estimates in finite quasifields, and related results", co-authored with Thang Pham, Craig Timmons, and Le Anh Vinh, which has been submitted for publication. The author was one of the primary investigators and authors of this paper.

7

Fano Subplanes of Projective Planes

"The survival of finite geometry as an active field of study depends on someone finding a finite projective plane of a non-prime-power order."

– Gary Ebert

7.1 Introduction

A fundamental question in incidence geometry is about the subplane structure of projective planes. There are relatively few results concerning when a projective plane of order k is a subplane of a projective plane of order n. Neumann [67] found Fano subplanes in certain Hall planes, which led to the conjecture that every finite non-Desargesian plane contains $PG(2,2)$ as a subplane (this conjecture is widely attributed to Neumann, though it does not appear in her work).

Johnson [53] and Fisher and Johnson [36] showed the existence of Fano subplanes in many translation planes. Petrak [71] showed that Figueroa planes contain $PG(2,2)$ and Caliskan and Petrak [17] showed that Figueroa planes of odd order contain $PG(2,3)$. Caliskan and Moorhouse [16] showed that all Hughes planes contain $PG(2,2)$ and that the Hughes plane of order q^2 contains $PG(2,3)$ if $q \equiv 5 \pmod 6$. We prove the following.

Theorem 7.1.1. *Let* Π *be a finite projective plane of even order which admits an orthogonal polarity. Then* Π *contains a Fano subplane.*

Ganley [40] showed that a finite semifield plane admits an orthogonal polarity if and only if it can be coordinatized by a commutative semifield. A result of Kantor [54] implies that the number of nonisomorphic planes of order n a power of 2 that can be coordinatized by a commutative semifield is not bounded above by any polynomial in n. Thus, Theorem 7.1.1 applies to many projective planes.

7.2 Proof of Theorem 7.1.1

We collect some definitions and results first. Let $\Pi = (\mathcal{P}, \mathcal{L}, \mathcal{I})$ be a projective plane of order n. We write $p \in l$ or say p is on l if $(p, l) \in \mathcal{I}$. Let π be a polarity of Π. That is, π maps points to lines and lines to points, π^2 is the identity function, and π respects incidence. Then one may construct the polarity graph G_π^o as follows. $V(G_\pi^o) = \mathcal{P}$ and $p \sim q$ if and only if $p \in \pi(q)$. That is, the neighborhood of a vertex p is the line $\pi(p)$ that p gets mapped to under the polarity. If $p \in \pi(p)$, then p is an *absolute point* and the vertex p will have a loop on it. A polarity is *orthogonal* if exactly $n + 1$ points are absolute. We note that as neighborhoods in the graph represent lines in the geometry, each vertex in G_π^o has exactly $n + 1$ neighbors (if v is an absolute point, it has exactly n neighbors other than itself). We provide proofs of the following preliminary observations for completeness.

Lemma 7.2.1. *Let* Π *be a projective plane with polarity* π*, and* G_π^o *be the associated polarity graph.*

(a) For all $u, v \in V(G_\pi^o)$*,* u *and* v *have exactly* 1 *common neighbor.*

(b) G_π^o *is* C_4 *free.*

(c) If u *and* v *are two absolute points of* G_π^o*, then* $u \not\sim v$*.*

(d) If $v \in V(G_\pi^o)$*, then the neighborhood of* v *induces a graph of maximum degree at most* 1*.*

(e) Let $e = uv$ be an edge of G_π^o such that neither u nor v is an absolute point. Then e lies in a unique triangle in G_π^o.

Proof. To prove (a), let u and v be an arbitrary pair of vertices in $V(G_\pi^o)$. Because Π is a projective plane, $\pi(u)$ and $\pi(v)$ meet in a unique point. This point is the unique vertex in the intersection of the neighborhood of u and the neighborhood of v. (b) and (c) follow from (a).

To prove (d), if there is a vertex of degree at least 2 in the graph induced by the neighborhood of v, then G_π^o contains a 4-cycle, a contradiction by (b).

Finally, let $u \sim v$ and neither u nor v an absolute point. Then by (a) there is a unique vertex w adjacent to both u and v. Now uvw is the purported triangle, proving (e). □

Proof of Theorem 7.1.1. We will now assume Π is a projective plane of even order n, that π is an orthogonal polarity, and that G_π^o is the corresponding polarity graph (including loops). Since n is even and π is orthogonal, a classical theorem of Baer ([9], see also Theorem 12.6 in [52]) says that the $n+1$ absolute points under π all lie on one line. Let $a_1, \ldots, a_{n+1}$ be the set of absolute points and let l be the line containing them. Then there is some $p \in \mathcal{P}$ such that $\pi(l) = p$. This means that in G_π^o, the neighborhood of p is exactly the set of points $\{a_1, \ldots, a_{n+1}\}$. For $1 \leq i \leq n+1$, let N_i be the neighborhood of a_i (note that $a_i \in N_i$). Then by Lemma 7.2.1.b, $N_i \cap N_j = \{p\}$ if $i \neq j$. Further, counting gives that

$$V(G_\pi^o) = \bigcup_{i=1}^{n+1} N_i. \tag{7.1}$$

Let ER_2^o be the graph on 7 points which is the polarity graph (with loops) of $PG(2,2)$ under the orthogonal polarity (Figure 7.2).

Lemma 7.2.2. *If ER_2^o is a subgraph of G_π^o, then Π contains a Fano subplane.*

Proof. Let $v_1, \ldots, v_7$ be the vertices of a subgraph ER_2^o of G_π^o. Let $l_i = \pi(v_i)$ for $1 \leq i \leq 7$. Then the lines $l_1, \ldots, l_7$ in Π restricted to the points $v_1, \ldots, v_7$ form

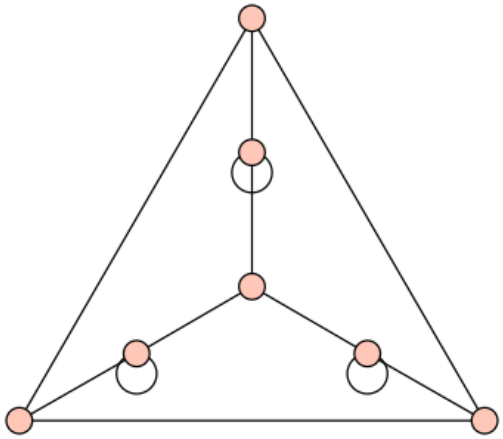

Figure 7.1: ER_2^o

a point-line incidence structure, and one can check directly that it satisfies the axioms of a projective plane. □

Thus, it suffices to find ER_2^o in G_π^o. To find ER_2^o it suffices to find distinct i, j, k such that there are $v_i \in N_i$, $v_j \in N_j$, and $v_k \in N_k$ where $v_i v_j v_k$ forms a triangle in G_π^o, for then the points $p, a_i, a_j, a_k, v_i, v_j, v_k$ yield the subgraph ER_2^o. Now note that for all i, and for $v \in N_i$, v has exactly n neighbors that are not absolute points. There are $n+1$ choices for i and $n-1$ choices for $v \in N_i$. As each edge is counted twice, this yields

$$\frac{n(n-1)(n+1)}{2}$$

edges with neither end an absolute point. By Lemma 7.2.1.e, there are at least

$$\frac{n^3-n}{6}$$

triangles in G_π^o. By Lemma 7.2.1.c, there are no triangles incident with p, by Lemma 7.2.1.b, there are no triangles that have more than one vertex in N_i for any i, and by Lemma 7.2.1.d there are at most $\lfloor \frac{n-1}{2} \rfloor = \frac{n}{2} - 1$ triangles incident with a_i for each i. Therefore, by (7.1), there are at least

$$\frac{n^3-n}{6} - (n+1)\left(\frac{n}{2}-1\right)$$

copies of ER_2^o in G_π^o. This expression is positive for all even natural numbers n. □

7.3 Concluding Remarks

First, we note that the proof of Theorem 7.1.1 actually implies that there are $\Omega(n^3)$ copies of $PG(2,2)$ in any plane satisfying the hypotheses, and echoing Petrak [71], perhaps one could find subplanes of order 4 for n large enough. We also note that it is crucial in both proofs that the absolute points form a line. When n is odd, the proof fails (as it must, since the proofs do not detect if Π is Desargesian or not).

Finally, Bill Kantor [55] communicated to the author that Theorem 7.1.1 can be proved in an even shorter way by using the language of finite incidence geometry and a theorem of Ostrom (Theorem 5.1 in [68]). Using this theorem, it suffices to find a self-polar triangle in the projective plane (equivalent to finding the triangle $v_i v_j v_k$ in our proof). An advantage of our proof is that we get an explicit lower bound on the number of Fano subplanes in the projective plane, whereas an advantage of Kantor's proof is that one does not even require the projective plane to be finite.

Bibliography

[1] Marien Abreu, Camino Balbuena, and Domenico Labbate. Adjacency matrices of polarity graphs and of other c 4-free graphs of large size. *Designs, Codes and Cryptography*, 55(2-3):221–233, 2010.

[2] Peter Allen, Peter Keevash, Benny Sudakov, and Jacques Verstraëte. Turán numbers of bipartite graphs plus an odd cycle. *Journal of Combinatorial Theory, Series B*, 106:134–162, 2014.

[3] Noga Alon and Fan RK Chung. Explicit construction of linear sized tolerant networks. *Annals of Discrete Mathematics*, 38:15–19, 1988.

[4] Noga Alon and Paul Erdős. An application of graph theory to additive number theory. *European Journal of Combinatorics*, 6(3):201–203, 1985.

[5] Noga Alon, Michael Krivelevich, and Benny Sudakov. Coloring graphs with sparse neighborhoods. *Journal of Combinatorial Theory, Series B*, 77(1):73–82, 1999.

[6] Noga Alon and Vojtěch Rödl. Sharp bounds for some multicolor ramsey numbers. *Combinatorica*, 25(2):125–141, 2005.

[7] Noga Alon and Joel H Spencer. *The probabilistic method*. John Wiley & Sons, 2000.

[8] Martin Bachratỳ and Jozef Širáň. Polarity graphs revisited. *Ars Mathematica Contemporanea*, 8(1), 2014.

[9] Reinhold Baer. Projectivities with fixed points on every line of the plane. *Bulletin of the American Mathematical Society*, 52(4):273–286, 1946.

[10] Béla Bollobás and Oleg Pikhurko. Integer sets with prescribed pairwise differences being distinct. *European Journal of Combinatorics*, 26(5):607–616, 2005.

[11] Anthony Bonato and Andrea Burgess. Cops and robbers on graphs based on designs. *Journal of Combinatorial Designs*, 21(9):404–418, 2013.

[12] Raj C Bose. An affine analogue of singer's theorem. *Journal of the Indian Mathematical Society*, 6(1-15):15, 1942.

[13] Jean Bourgain, Nets Katz, and Terence Tao. A sum-product estimate in finite fields, and applications. *Geometric & Functional Analysis*, 14(1):27–57, 2004.

[14] Andries E Brouwer, Arjeh M Cohen, and Arnold Neumaier. *Distance-Regular Graphs*. Springer Verlag, Berlin, Heidelberg, 1989.

[15] William G Brown. On graphs that do not contain a thomsen graph. *Canadian Mathematical Bulletin*, 9(2):1–2, 1966.

[16] Cafer Caliskan and G Eric Moorhouse. Subplanes of order 3 in hughes planes. *The Electronic Journal of Combinatorics*, 18(P2):1, 2011.

[17] Cafer Caliskan and Bryan Petrak. Subplanes of order 3 in figueroa planes. *Finite Fields and Their Applications*, 20:24–29, 2013.

[18] Ajai Choudhry. On equal sums of cubes. *Rocky Mountain Journal of Mathematics*, 28(4), 1998.

[19] Sarvadaman Chowla. Solution of a problem of erdos and turán in additive-number theory. *Proceedings of the National Academy of Sciences, India Section A*, 14(1-2):5–4, 1944.

[20] Fan RK Chung. *Spectral graph theory*, volume 92. American Mathematical Society, 1997.

[21] Fan RK Chung and Ronald L Graham. On multicolor ramsey numbers for complete bipartite graphs. *Journal of Combinatorial Theory, Series B*, 18(2):164–169, 1975.

[22] Fan RK Chung and Ronald L Graham. Quasi-random set systems. *Journal of the American Mathematical Society*, 4(1):151–196, 1991.

[23] Javier Cilleruelo. B_2-sequences whose terms are squares. *Acta Arithmetica*, 55(3):261–265, 1990.

[24] Javier Cilleruelo. Combinatorial problems in finite fields and sidon sets. *Combinatorica*, 32(5):497–511, 2012.

[25] Robert S Coulter and Rex W Matthews. Planar functions and planes of lenz-barlotti class ii. *Designs, Codes and Cryptography*, 10(2):167–184, 1997.

[26] Etienne de Klerk, Mike W Newman, Dmitrii V Pasechnik, and Renata Sotirov. On the lovász ϑ-number of almost regular graphs with application to Erdős–Rényi graphs. *European Journal of Combinatorics*, 30(4):879–888, 2009.

[27] Stefaan De Winter, Jeroen Schillewaert, and Jacques Verstraete. Large incidence-free sets in geometries. *The Electronic Journal of Combinatorics*, 19(4):P24, 2012.

[28] Peter Dembowski. *Finite Geometries*. Springer-Verlag, Berlin, 1968.

[29] Peter Dembowski and Theodore G Ostrom. Planes of order n with collineation groups of order n^2. *Mathematische Zeitschrift*, 103(3):239–258, 1968.

[30] György Elekes. On the number of sums and products. *Acta Arithmetica*, 81:365–367, 1997.

[31] Paul Erdős. On sequences of integers no one of which divides the product of two others and on some related problems. *Isvestia Nauchno-Issl. Inst. Mat. i Meh. Tomsk*, 2:74–82, 1938.

[32] Paul Erdős, Alfréd Rényi, and Vera T Sós. On a problem of graph theory. *Studia Scientiarum Mathematicarum Hungarica*, 1:215–235, 1966.

[33] Paul Erdős and Endre Szemerédi. On sums and products of integers. In *Studies in pure mathematics*, pages 213–218. Springer, 1983.

[34] Paul Erdős and Pál Turán. On a problem of sidon in additive number theory, and on some related problems. *Journal of the London Mathematical Society*, 1(4):212–215, 1941.

[35] Frank A Firke, Peter M Kosek, Evan D Nash, and Jason Williford. Extremal graphs without 4-cycles. *Journal of Combinatorial Theory, Series B*, 103(3):327–336, 2013.

[36] J Chris Fisher and Norman L Johnson. Fano configurations in subregular planes. *Note di Matematica*, 28(2):69–98, 2010.

[37] Zoltán Füredi. Quadrilateral-free graphs with maximum number of edges. *Proceedings of the Japan Workshop on Graph Theory and Combinatorics, Keio University, Yokohama, Japan*, pages 13–22, 1994.

[38] Zoltán Füredi. On the number of edges of quadrilateral-free graphs. *Journal of Combinatorial Theory, Series B*, 68(1):1–6, 1996.

[39] Zoltán Füredi and Miklós Simonovits. The history of degenerate (bipartite) extremal graph problems. In *Erdős Centennial*, pages 169–264. Springer, 2013.

[40] Michael J Ganley. Polarities in translation planes. *Geometriae Dedicata*, 1(1):103–116, 1972.

[41] Moubariz Z Garaev. The sum-product estimate for large subsets of prime fields. *Proceedings of the American Mathematical Society*, 136(8):2735–2739, 2008.

[42] Chris D Godsil and Mike W Newman. Eigenvalue bounds for independent sets. *Journal of Combinatorial Theory, Series B*, 98(4):721–734, 2008.

[43] Ben Green. The number of squares and $B_h[g]$ sets. *Acta Arithmetica*, 100:365–390, 2001.

[44] Katalin Gyarmati and András Sárközy. Equations in finite fields with restricted solution sets. ii (algebraic equations). *Acta Mathematica Hungarica*, 119(3):259–280, 2008.

[45] Godfrey H Hardy and Srinivasa Ramanujan. The normal number of prime factors of a number n. *Quarterly Journal of Mathematics*, 48:76–92, 1917.

[46] Godfrey H Hardy and Edward M Wright. *An introduction to the theory of numbers*. Oxford University Press, 1979.

[47] Derrick Hart and Alex Iosevich. Sums and products in finite fields: an integral geometric viewpoint. *Contemporary Mathematics*, 464, 2008.

[48] Derrick Hart, Alex Iosevich, and Jozsef Solymosi. Sum-product estimates in finite fields via kloosterman sums. *International Mathematics Research Notices*, 2007(7):rnm007, 2007.

[49] Sylvia A Hobart and Jason Williford. The independence number for polarity graphs of even order planes. *Journal of Algebraic Combinatorics*, 38(1):57–64, 2013.

[50] AJ Hoffman. On eigenvalues and colorings of graphs. 1970 Graph Theory and its Applications (Proc. Advanced Sem., Math. Research Center, Univ. of Wisconsin, Madison, Wis., 1969). *New York*.

[51] Christopher Hooley. On the representations of a number as the sum of two cubes. *Mathematische Zeitschrift*, 82(3):259–266, 1963.

[52] Daniel R Hughes and Frederick Charles Piper. *Projective planes*, volume 6. Springer, 1973.

[53] Norman L Johnson. Fano configurations in translation planes of large dimension. *Note di Matematica*, 27(1):21–38, 2009.

[54] William M Kantor. Commutative semifields and symplectic spreads. *Journal of Algebra*, 270(1):96–114, 2003.

[55] William M Kantor. Personal communication, 2015.

[56] Peter Keevash. Hypergraph Turán problems. *Surveys in combinatorics*, 392:83–140, 2011.

[57] Tamás Kővári, Vera Sós, and Pál Turán. On a problem of K. Zarankiewicz. In *Colloquium Mathematicae*, volume 1, pages 50–57, 1954.

[58] Alexandr Kostochka, Pavel Pudlák, and Vojtech Rödl. Some constructive bounds on ramsey numbers. *Journal of Combinatorial Theory, Series B*, 100(5):439–445, 2010.

[59] Manfred Kühleitner and Werner Nowak. The average number of solutions of the diophantine equation $u^2 + v^2 = w^3$ and related arithmetic functions. *Acta Mathematica Hungarica*, 104(3):225–240, 2004.

[60] Felix Lazebnik and Jacques Verstraëte. On hypergraphs of girth five. *The Electronic Journal of Combinatorics*, 10(R25):1, 2003.

[61] Rudolf Lidl and Harald Niederreiter. *Finite fields*, volume 20. Cambridge university press, 1997.

[62] Bernt Lindström. An inequality for B_2-sequences. *Journal of Combinatorial Theory*, 6(2):211–212, 1969.

[63] Bernt Lindström. Well distribution of sidon sets in residue classes. *Journal of Number Theory*, 69(2):197–200, 1998.

[64] Keith E Mellinger. Ldpc codes from triangle-free line sets. *Designs, Codes and Cryptography*, 32(1-3):341–350, 2004.

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

[66] Melvyn B Nathanson. N-graphs, modular sidon and sum-free sets, and partition identities. *The Ramanujan Journal*, 4(1):59–67, 2000.

[67] Hanna Neumann. On some finite non-desarguesian planes. *Archiv der Mathematik*, 6(1):36–40, 1954.

[68] Theodore G Ostrom. Ovals, dualities, and desargues's theorem. *Canadian Journal of Mathematics*, 7:417–431, 1955.

[69] Torrence D Parsons. Graphs from projective planes. *Aequationes Mathematicae*, 14(1):167–189, 1976.

[70] Xing Peng, Michael Tait, and Craig Timmons. On the chromatic number of the Erdős-Rényi orthogonal polarity graph. *The Electronic Journal of Combinatorics*, 22(2):P2–21, 2015.

[71] Bryan Petrak. Fano subplanes in finite Figueroa planes. *Journal of Geometry*, 99(1-2):101–106, 2010.

[72] Imre Z Ruzsa. Solving a linear equation in a set of integers i. *Acta Arithmetica*, 65(3):259–282, 1993.

[73] András Sárközy. On sums and products of residues modulo p. *Acta Arithmetica*, 118:403–409, 2005.

[74] András Sárközy. On products and shifted products of residues modulo p. *Integers*, 8(2), 2008.

[75] Simon Sidon. Ein satz über trigonometrische polynome und seine anwendung in der theorie der fourier-reihen. *Mathematische Annalen*, 106(1):536–539, 1932.

[76] Alexander Sidorenko. What we know and what we do not know about Turán numbers. *Graphs and Combinatorics*, 11(2):179–199, 1995.

[77] James Singer. A theorem in finite projective geometry and some applications to number theory. *Transactions of the American Mathematical Society*, 43(3):377–385, 1938.

[78] József Solymosi. Bounding multiplicative energy by the sumset. *Advances in mathematics*, 222(2):402–408, 2009.

[79] Douglas R Stinson. Nonincident points and blocks in designs. *Discrete Mathematics*, 313(4):447–452, 2013.

[80] Michael Tait and Craig Timmons. Sidon sets and graphs without 4-cycles. *Journal of Combinatorics*, 5(2), 2014.

[81] Terence Tao. The sum-product phenomenon in arbitrary rings. *Contributions to Discrete Mathematics*, 4(2), 2009.

[82] Terence Tao and Van H Vu. *Additive combinatorics*, volume 105. Cambridge University Press, 2006.

[83] Gérald Tenenbaum. *Introduction to analytic and probabilistic number theory*, volume 46. Cambridge university press, 1995.

[84] Edwin R Van Dam and Willem H Haemers. Which graphs are determined by their spectrum? *Linear Algebra and its applications*, 373:241–272, 2003.

[85] Le Anh Vinh. On the solvability of systems of sum-product equations in finite fields. *Glasgow Mathematical Journal*, 53(03):427–435, 2011.

[86] Le Anh Vinh. The Szemerédi–Trotter type theorem and the sum-product estimate in finite fields. *European Journal of Combinatorics*, 32(8):1177–1181, 2011.

[87] Le Anh Vinh. Graphs generated by sidon sets and algebraic equations over finite fields. *Journal of Combinatorial Theory Series B*, 103(6):651–657, 2013.

[88] Le Anh Vinh. On three-variable expanders over finite fields. *International Journal of Number Theory*, 10(03):689–703, 2014.

[89] Van H Vu. Sum-product estimates via directed expanders. *Mathematical Research Letters*, 15(2):375–388, 2008.

[90] Jason Williford. *Constructions in finite geometry with applications to graphs*. PhD thesis, University of Delaware, 2004.