Spring 2022

Dot Product Bounds in Galois Rings

David Lee Crosby
Missouri State University, Crosby24@live.missouristate.edu

DOT PRODUCT BOUNDS IN GALOIS RINGS

A Master's Thesis

Presented to

The Graduate College of

Missouri State University

In Partial Fulfillment

Of the Requirements for the Degree

Master of Science, Mathematics

By

David Lee Crosby

May 2022

DOT PRODUCT BOUNDS IN GALOIS RINGS

Mathematics

Missouri State University, May 2022

Master of Science

David Lee Crosby

ABSTRACT

We consider the Erdős Distance Conjecture in the context of dot products in Galois rings and prove results for single dot products and pairs of dot products.

KEYWORDS: Dot Product, Erdős Distance Conjecture, Galois Rings

DOT PRODUCT BOUNDS IN GALOIS RINGS

By

David Lee Crosby

A Master's Thesis
Submitted to the Graduate College
Of Missouri State University
In Partial Fulfillment of the Requirements
Master of Science, Mathematics

May 2022

Approved:

Steven Senger, Ph.D., Thesis Committee Chair

Cameron Wickham, Ph.D., Committee Member

Les Reid, Ph.D., Committee Member

Mark Rogers, Ph.D., Committee Member

Julie Masterson, Ph.D., Dean of the Graduate College

ACKNOWLEDGEMENTS

I would like to thank all my professors at Missouri State University. Especially Steven Senger, Xingping Sun, Mark Rogers, Cameron Wickham, and William Bray for helping me become the mathematician I am today. I would like to thank Cameron Wickham for suggesting the context of Galois rings and suggesting references for Galois rings. I would like to thank the thesis committee for their suggestions and comments. I would like to thank the folks at Ekklesia for being almost a second family and helping me through these years. Lastly, I would like to thank my brother for taking care of me during my stay at Missouri State University.

TABLE OF CONTENTS

LIST OF FIGURES

1 INTRODUCTION

In 1946, Paul Erdős posed the following question: how often can a single distance occur in a large finite set of points in the plane? While there has been much activity on this and related problems (using other functionals besides distance, and looking at different ambient settings), the best known upper and lower bounds for quantity of the original question are still quite far apart. The pursuit of this question has led to many surprising connections between seemingly disparate fields of mathematics and has deepened our understanding of these fields. To gain a deeper understanding of what lies at the core of this question, there have been a number of variants explored in algebraic settings such as vector spaces over finite fields and modules over various finite rings.

Finite fields have been studied as they play a close role to coding theory, which has many applications for compression and transmission of data. Another reason is that finite fields provide an easier environment to study problems in analysis without having to worry about convergence. Thus, understanding the unit distance and dot product problem in finite fields may help us understand coding theory and analysis problems. A few reasons to study the distinct dot product problem instead of the unit distance distance problem is that dot products are analogous to lines and have deep connections with the so called sum-product conjecture, which we discuss later. In this thesis, we focus on the following variant: how often can a particular dot product occur in a subset of a module over a Galois ring?

In Chapter 1, we introduce the man behind the Erdős distance problem. Then we explore the developments made on the problem and its variants, and then the applications these have for mathematics and industry. Next we introduce terms and results needed for the rest of the thesis. In Chapter 2, we address the unit distance problem in the context of single dot products over Galois rings. For Chapter 3, we extend our single dot product result to pairs of dot products determined by triples of points (called a hinge).

1.1 Background on the Erdős Distance Problem

How often can a single distance occur in a large finite set of points in the plane? In this chapter, we will give background on the man who posed this problem, its history, and its applications. To better understand this problem, we give the example below:

Example 1. Consider how many times a single distance may occur with three points in the plane. One way to view this problem is to place unit circles and find the maximal incidences between centers of circles and edges of circles. This is as each center and intersection with its corresponding edge gives us a unit distance. Thus, for three points, we may place three unit circles whose centers form an equilateral triangle. This gives us the maximum number of a single distance for three points is three (see Figure 1.1). If we were to add another point, then anywhere we place it, it must introduce at least one new distance.

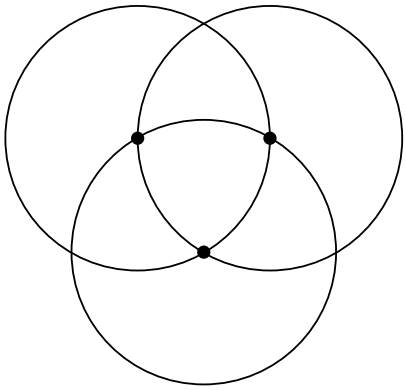

Figure 1.1: Three unit circles forming an equilateral triangle.

1.1.1 Erdős. Paul Erdős was one of the most prolific mathematicians of the 20th century (see [16]). He was born in 1913 in Hungary to two mathematics teachers. At the age of 20 he proved Chebyshev's theorem, an important result in number theory. When he was 21, he was awarded his doctorate at the university of Budapest. Before the Holocaust he relocated to the United States of America and became a traveling mathematician, living out of a suitcase. During his life, he proposed problems in discrete mathematics,

graph theory, number theory, mathematical analysis, approximation theory, set theory, and probability theory. One of his peers said, "A mathematician is a machine for turning coffee into theorems, and Erdős drank copious quantities." For many of his conjectures, their proofs and exploration would deepen and tie together many fields of mathematics. Erdős would often also offer cash prize money for whoever solved one of his conjectures.

In 1946, Paul Erdős published a paper called, "On sets of distances of n points" in the American Mathematical Monthly (see [9]). There he posed the following question: How often can a single distance occur in a large finite set of points in the plane? The cash prize for the Erdős distance problem was \$500 in 1946. In today's (2022) money, this is over \$7,000. Proving the Erdős distance conjecture would also give one a check with Erdős's signature.

In his paper (see [9, Theorem 2]), Erdős found that for n points, the number of times a distance r may occur in the plane, call $g(n;r)$, has $n^{1+c/\log(\log(n))} < g(n;r) < n^{3/2}$. We give an adaptation of his proof below.

Proof. By using similar reasoning as we did in Example 1, Erdős found $g(n;r) < n^{3/2}$. Let $a = [n^{1/2}]$. For a lower bound, we consider the set of points $(x, y),\ 0 \leq x \leq a,\ 0 \leq y \leq a$. This is the $a \times a$ grid of integers. Thus, we are after the number of solutions $x^2 + y^2 = r^2$. In another paper (see [10, §1]), Erdős shows that the number of solutions of the equation $m = p^2 + q^2$ is greater than $n^{c/\log(\log(n))}$ for some $0 < c < 1$, and hence

$$g(n;r) > n^{1+c/\log(\log(n))}$$

which completes the proof.

□

At the end of his proof, Erdős writes, "It seems likely that $g(n) < n^{1+\epsilon}$," $(\forall \epsilon > 0)$.

1.1.2 History. In this section, we give an overview of the developments toward bounding the Erdős distance problem and the variants that arose. We will use the notation $f(n) = \Omega(h(n))$ to mean that for n large enough, there exists constant C such that $f(n) > Ch(n)$. We will use $f(n) = O(h(n))$ to mean that for n large enough, there exists constant C such that $f(n) < Ch(n)$. We will use $f(n) = \Theta(h(n))$ for $f(n) = \Omega(h(n))$ and $f(n) = O(h(n))$. The single distance problem is often called the unit distance problem. This is as we may turn any single distance into the unit distance by scaling. The best known upper bound to the original unit distance problem is $O(n^{4/3})$ and was shown by Spencer, Szemerédi, and Trotter in 1984 (see [27, Corollary 2]) where they consider the number of incidences between points and circles.

After years of work on the unit distance problem with little progress, mathematicians turned their gaze to a related problem. The related problem is the distinct distance problem: For n points, how few different distances may be obtained? Let $g(n)$ be the minimal number of distinct distances for n points. So, for instance, $g(3) = 1$ by using an equilateral triangle. For $g(4)$, we see that no matter where we place a fourth point in Figure 1.1, we will introduce at least one new distance. Ergo, $g(4) = 2$.

In that same paper where Erdős posed the unit distance problem [9, Theorem 1], he also posed the distinct distance problem and conjectured that $f(n) = \Omega(n/(\log n)^{1/2})$, where $f(n)$ is the minimum number of distance determined by n points in the plane. He conjectured that in d dimensions, this problem is $\Theta(n^{2/d})$. In 2004 Katz and Tardos showed that the lower bound on the number of distinct distances is $\Omega(n^{0.8641})$ for n points in the plane (see [20]). This problem was practically solved in 2010 by Guth and Katz [14, Theorem 1.1], where the bound was found to be $\Omega(n/\log(n))$. Higher dimensional settings were studied by Solymosi and Vu in [26, Theorem 1.1], where they showed the number of distinct distances in R^d is $\Omega\left(n^{\frac{2}{d}-\frac{2}{d(d+2)}}\right)$, as opposed to the conjectured $\Omega(n^{2/d})$. In 2008 Iosevich and Rudnev studied this problem in the instance of vector spaces over finite fields [18]. This may have inspired Burgain, Katz, and Tao to study the sum-product estimate in

finite fields [4]. The distinct distance problem was further extended to the integers modulo a prime power in 2011 by Covert, Iosevich, and Pakianathan [5], where they also considered the distinct dot product as well as the distinct distance problem. This idea of studying dot products as well as vector spaces over rings is where most of this thesis will spend it's time.

Since the distinct distance problem was practically solved, many turned their gaze back to studying the unit distance problem, but this time they studied variants of the problem. The variant we focus on is the single dot product problem. This is in a set with n points, how many pairs of points have a specified dot product? The single dot product problem has been studied in the case of finite fields and integers modulo a prime power in [15], [1], [6], and more, where different bounds and configurations are studied.

So far, in the single dot product problem, we have been looking at how many pairs of points have the specified dot product. An extension to this idea is to ask how subsets of points have a specified configuration of dot products.

In [1], Barker and Senger obtain upper bounds on the number triples with a specified pair of dot products. This is, for a given $(\alpha, \beta) \in \mathbf{R}^2$, how large is the set $\{(a, b, c) \in P^3 : a \cdot b = \alpha,\ b \cdot c = \beta\}$ where $P \subset \mathbf{R}^2$? Such configurations are sometimes called hinges. In [6], Covert and Senger extend the concept of hinges to finite fields and the integers modulo a prime power. Kilmer, Marshall, and Senger, in [21], broaden the concept of hinges over the reals to k-chains over the reals, where $k + 1$ points determine k dot products.

1.1.3 Applications. This unit distance problem and variants has far-reaching applications. We see its ideas being used in multiple industries, such as in mobile robot swarms, big data, pattern recognition, and more.

A mathematical reason to study the unit dot product problem is that, if we fix (u, v) and r, then $(u, v) \cdot (x, y) = r$ is the same as $ux + vy = r$, the standard form of a line in $\mathbf{R}^2$. Thus, studying the unit dot product problem helps us understand key facts about

lines. Another reason to study dot products is that the set $A \cdot A + A \cdot A = \{a_1a_2 + a_3a_4 : a_i \in A\}$ is equivalent to the set of dot products of A^2 with itself. This set has connections with the sum-product conjecture that $\max(|A+A|, |A \cdot A|) \geq |A|^{2-o(1)}$ where $A \subset \mathbf{R}$. This was conjectured by Erdős and Szemerédi in 1983 in [11] over the integers and is figured to be true for the reals. In [31], Terence Tao studies the sum-product conjecture over many types of rings. Hart, Iosevich, Koh, and Rudnev [15], prove, using the Erdős distance conjecture, results relating to the set $A \cdot A + \cdots + A \cdot A$ where A is a subset of a finite field.

Finite rings have started to be used in every day life through coding theory. This is the theory of strings over a set and how to compress, transmit, encrypt, etc. these strings. We are seeing codes over $\mathbf{Z}_{p^n}$ being used as they have a better way of defining distance than other rings (see, [2, §8.1.1]). One of the common types of codes, cyclic, can be described in terms of polynomials, so in [2, §8.1.3], we see Galois rings and coding theory coming together.

Another reason to study finite rings is that they provide a test bed for complicated analysis problems as integrals are always convergent. The prototypical example of this is Zeev Dvir's paper "On the size of Kakeya sets in finite fields" [8, Theorem 2], where he proved the Kakeya Conjecture (relates to subsets of $\mathbf{F}_{p^l}$ that contain a line in every direction) via simple means.

1.2 Ring Theory Background

We will assume that the reader has an undergraduate knowledge of groups and rings. For further background information, see [7].

Throughout this thesis, we will assume that p is a given prime number. We will use $\mathbf{Z}_{p^l}$ to be the integers modulo p^l for some $l > 0$. We will use $\mathbf{F}_{p^l}$ to denote the finite field of order p^l, this is also called a Galois field.

1.2.1 Construction of Galois Rings. We focus on Galois rings as they are the building blocks of finite local rings which are in turn the building blocks of finite commutative rings. Any finite local ring is isomorphic to a quotient of a polynomial ring over a Galois ring. This is if L is a local ring, then $L \cong R_{e,k}[x_1, x_2, \cdots, x_n]/I$ for some prime p, natural numbers e, k and ideal $I \subset R_{e,k}[x_1, x_2, \cdots, x_n]$. In particular, $\mathbf{Z}_{p^e} \cong R_{e,1} \cong Z_{p^l}[x]/(x+1)$ and $\mathbf{F}_{p^k} \cong \mathbf{Z}_p[x]/(f(x)) \cong R_{1,k}$ (where f is a monic irreducible polynomial of degree k). In turn, local rings are the building blocks for any finite commutative ring with unity (see [2, Chapter 3, Theorem 3.1.4]). We will first build up some definitions to be able to understand what a Galois ring is. Our presentation follows elements from [2], [17], and [24]

We will use the notation $\mathbf{Z}_{p^l}$ to mean $\mathbf{Z}/(p^l)$ where (p^l) is the ideal generated by p^l.

Definition 2 (Basic monic irreducible polynomial)**.** Let the map $\rho : \mathbf{Z}_{p^l} \to \mathbf{Z}_p$ be the map $\rho(x) = r$ where r is remainder of x divided by p. Let the map $\mu : \mathbf{Z}_{p^l}[x] \to \mathbf{Z}_p[x]$ be $\mu(\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} \rho(a_i) x_i$, which will apply mod p to the coefficients. Recall that a monic polynomial is a polynomial with leading coefficient 1. A basic monic irreducible polynomial is a polynomial f in $\mathbf{Z}_{p^l}[x]$ such that $\mu(f)$ is a monic irreducible polynomial in $\mathbf{Z}_p[x]$.

We know monic irreducible polynomials of a given degree exist (see [32, §2.3]). As μ is surjective, we may take a preimage of a monic irreducible in $\mathbf{Z}_p[x]$ as our basic irreducible polynomial in $\mathbf{Z}_p^{\ell}[x]$. Further, at least one of these preimages is monic as $\rho(1) = 1$.

Definition 3 (Galois Ring)**.** Let p be a given prime. The construction of the Galois ring, $R_{e,k}$, is $R_{e,k} = Z_{p^e}[x]/(f(x))$, where f is a basic monic irreducible polynomial in $Z_{p^e}[x]$ of degree k.

In particular, $\mathbf{Z}_{p^l}$ and $\mathbf{F}_{p^n}$ are both Galois rings. For $\mathbf{Z}_{p^l}$, we may construct as $\mathbf{Z}_{p^l}[x]/(x+1) = R_{l,1}$ and for $\mathbf{F}_{p^n}$ we may construct as $\mathbf{Z}_p[x]/(f(x)) = R_{1,n}$ where $f(x)$ is a basic monic irreducible polynomial of degree n. Thus, $\mathbf{Z}_{p^l} = R_{l,1}$ and $\mathbf{F}_{p^n} = R_{1,n}$

Example 4. We will construct $R_{2,2}$ when $p = 2$. We see that $x^2 + x + 1 \in \mathbf{Z}_2[x]$ is monic irreducible as 0 and 1 are not roots of this degree 2 polynomial. Thus, $x^2 + x + 1 \in \mathbf{Z}_{2^2}[x]$ is a basic monic irreducible polynomial. Thus, $R_{2,2} = \mathbf{Z}_4[x]/(x^2 + x + 1)$.

In this thesis, we will study dot products over $(R_{e,k})^d$. This type of structure is called a module.

Definition 5 (Module)**.** Suppose that R is a commutative ring with identity, 1. Then a module, M, over R is a structure much like a vector space with the properties that for all $r, s \in R$ and $x, y \in M$,

$$r \cdot (x + y) = r \cdot x + r \cdot y$$

$$(r + s) \cdot x = r \cdot x + s \cdot x$$

$$(rs) \cdot x = r \cdot (s \cdot x)$$

$$1 \cdot x = x$$

1.2.2 Properties of Galois Rings. We will now show many of the properties of Galois Rings. One important property of Galois rings is that they are finite local rings. To understand what a local ring is, we must first define a maximal ideal.

Definition 6. Let R be a given ring. A maximal ideal $M \subsetneq R$ is a proper ideal, that is an ideal not equal to R, of R such that if J is an ideal and $M \subset J \subset R$, then $J = M$ or $J = R$.

A local ring is a ring with one unique maximal ideal. Notice that a field is a local ring as (0) is the unique maximal ideal. We now prove some results about local rings. Recall that a unit is an element with a multiplicative inverse. We will use $R^\times$ to denote the set of units of the ring R.

Proposition 7. Any element of a local ring is either a unit or an element of the maximal ideal.

Proof. Let R be a local ring with maximal ideal M. Let $r \in R$. In the case that r is a unit, we are done. In the case that r is not a unit, then $(r) \subsetneq R$ and hence (r) is a proper ideal. As every proper ideal is a subset of a maximal ideal, and M is the unique maximal ideal, $(r) \subset M$. Thus, $r \in M$. □

Proposition 8. Any element $r \in R$ where R is a local ring has either r as a unit or $1 - r$ as a unit.

Proof. Let M be the maximal ideal of R. Suppose that r is not in M, then since (r) is an ideal, it must be contained in a maximal ideal of R or $(r) = R$ and hence $r \in R^\times$. As $r \notin M$, it must be that $(r) = R$.

Suppose that $x \in M$ and that $1 - x$ is not a unit. As $1 - x$ is not a unit, then $1 - x \in M$. This means $1 - x = m$ for some $m \in M$ and so $1 = x + m$. As ideals are closed under addition, $1 \in M$, and hence $M = R$. This is a contradiction. Hence, $1 - x$ must be a unit. □

We will now build up to showing that Galois rings are local rings.

Definition 9. Let R be a given ring. A nilpotent element $a \in R$ is an element such that there exists some $n > 0$ such that $a^n = 0$.

Proposition 10. The set of nilpotent elements lie in the intersection of all prime ideals.

Proof. Let R be a given ring. Let $\pi : R \to D$ where D is an integral domain. Let $a \in R$ be nilpotent. Then there exists $n > 0$ such that $aa^n = 0$. Then $\pi(aa^n) = 0 = \pi(a)\pi(a^n)$, hence $\pi(a)$ is a zero divisor. As D is an integral domain, $\pi(a)$ must then be 0. Thus, a must be in any given prime ideal as $R/(p)$ is an integral domain when p is a prime ideal. □

We will call a set nilpotent if all elements of the set are nilpotent.

Proposition 11. If a ring R has a maximal ideal M with all nilpotent elements, then M is the unique maximal ideal of R.

Proof. Suppose that M' is a maximal ideal of R. Then by 10, $M \subset M'$. By maximality of M, $M = M'$. □

Lemma 12. A Galois ring is local.

Proof. Let $R_{e,k}$ be a given Galois ring. If $a \in (p)$, then $a = pr$ for some $r \in R_{e,k}$, and so $a^e = (pr)^e = 0$ and so (p) is nilpotent. Note

$$R_{e,k}/(p) \cong \frac{\mathbf{Z}[x]}{(p^e, p, f)} \cong \mathbf{Z}_p[x]/(f),$$

and so as $\mathbf{Z}_p[x]/(f)$ is a field, (p) is a maximal ideal. Thus by 11, (p) is the unique maximal ideal of $R_{e,k}$. Ergo, $R_{e,k}$ is a local ring. □

Lemma 13. The units of a Galois ring $R_{e,k}$ has

$$R_{e,k}^{\times} \cong (R_{e,k}/(p))^{\times} \times (1 + (p)).$$

Proof. As $R_{e,k}$ is local, the set $1 + (p)$ is a subgroup of the units under multiplication. As (p) is a maximal ideal, $R_{e,k}/(p)$ if a field and hence every non zero element of $R_{e,k}/(p)$ is a unit. Let S' be a set of representatives of $R_{e,k}/(p)$ in $R_{e,k}$. That is the canonical surjective homomorphism $\pi : R_{e,k} \to R_{e,k}/(p)$ is bijective when restricted to S'. Let $S = S' \setminus \{0\}$. Then $S \subset R_{e,k}^{\times}$. Also note, $|S \cap (1 + (p))| = 1$. This implies that $S(1 + (p)) = \{st : s \in S, t \in (1 + (p))\} \cong S \times (1 + (p))$. As $|R_{e,k}^{\times}| = |R_{e,k} \setminus (p)| = p^{ek} - p^{(e-1)k}$ and $|S| = p^k - 1$ and $|(1 + (p))| = |(p)| = p^{(e-1)k}$, we see that $|S \times (1 + (p))| = p^{ek} - p^{(e-1)k}$. Thus, $R_{e,k}^{\times} \cong (R_{e,k}/(p))^{\times} \times (1 + (p))$. □

It is also known that the units $R_{e,k}^{\times}$ has structure $R_{e,k}^{\times} \cong \mathbf{Z}_{p^k-1} \times (\mathbf{Z}_{p^{e-1}})^k$ when p is odd or when p and e are both 2. We have $R_{e,k}^{\times} \cong \mathbf{Z}_{2^k-1} \times \mathbf{Z}_2 \times \mathbf{Z}_{2^{e-2}} \times (\mathbf{Z}_{2^{e-1}})^{k-1}$ when $p = 2$ and $e \geq 3$. The proof for this is given in [2, Proposition 6.2.5]. This gives rise to the p-adic representation for an element of $R_{e,k}$.

Example 14. When $p = 2$, $R_{2,2}^{\times} \cong \mathbf{Z}_{2^2-1} \times (\mathbf{Z}_{2^{2-1}})^2 \cong \mathbf{Z}_3 \times \mathbf{Z}_2 \times \mathbf{Z}_2$.

Lemma 15. For any $0 \leq i \leq e$, $R_{e,k}/(p^i) \cong R_{i,k}$.

Proof. Note that (p^i) is the kernel of the map $g : R_{e,k} \to R_{e,k}$ with $g(r) = p^{e-i}r$. Recall

$$R_{e,k} \cong \frac{\mathbf{Z}_{p^e}[x]}{(f)}$$

by definition of $R_{e,k}$ where f is a basic monic irreducible polynomial of degree k. Further, we restrict f to having coefficients in the range 0–$(p^i - 1)$. Also, we will view $R_{e,k}$ as polynomials with coefficients in the range 0–$(p^e - 1)$. This will allow us to view an element in $R_{i,k}$ as being also an element in $R_{e,k}$. Set $g(z) = p^{e-i}z$, then g has kernel (p^i) and so by the first isomorphism theorem,

$$\frac{R_{e,k}}{(p^i)} \cong g(R_{e,k}).$$

Notice,

$$g(a_0+a_1x+\cdots a_{k-1}x^{k-1}) = p^{e-i}(a_0+a_1x+\cdots a_{k-1}x^{k-1}) = p^{e-i}a_o+p^{e-i}a_1x+\cdots p^{e-i}a_{k-1}x^{k-1},$$

and so, it is equivalent to the map $h : \mathbf{Z}_{p^e} \to \mathbf{Z}_{p^e}$ with $h(r) = p^{e-i}r$ lifted to $\mathbf{Z}_{p^e}[x]/(f)$ (that is applying the map to the coefficients). Notice that $(p^i) \subset \mathbf{Z}_{p^e}$ is the kernel of h. Thus, by the first isomorphism theorem, $h(\mathbf{Z}_{p^e}) \cong \mathbf{Z}_{p^e}/(p^i) \cong \mathbf{Z}_{p^i}$. Hence g is the lifting of h, so

$$g(R_{e,k}) \cong \frac{h(\mathbf{Z}_{p^e})[x]}{(f)}$$

. By the first isomorphism theorem and definition of $R_{i,k}$, we have

$$\frac{h(\mathbf{Z}_{p^e})[x]}{(f)} \cong \frac{\mathbf{Z}_{p^i}[x]}{(f)} \cong R_{i,k}.$$

Thus, $\frac{R_{e,k}}{(p^i)} \cong R_{i,k}$. □

Theorem 1.1. Let β be a generator of the subgroup of $R_{e,k}^{\times}$ isomorphic to $\mathbf{Z}_{p^k-1}$ (recall $\mathbf{Z}_{p^k-1} \cong (R_{e,k}/(p))^{\times}$). Let $T_{e,k} = \{0, 1, \beta, \cdots \beta^{p^k-2}\}$. Every $z \in R$ has a unique p-adic representation

$$z = z_0 + pz_1 + \cdots + p^{e-1}z_{e-1}, \quad z_i \in T_{e,k}.$$

Proof. We proceed by induction. It is clear that the theorem holds for $R_{1,k} \cong \mathbf{F}_{p^k}$. Suppose that the theorem holds for all $1 \leq i < e$. Let $R = R_{e,k}$ and $K = R/pR$. Let π be the natural surjective quotient map from R to K with kernel (p). Let $h(x) = px$. Recall that $(p) = \{px : x \in R\}$, which is $\mathrm{Im}(h)$. By the first isomorphism theorem, $\mathrm{Im}(h) \cong R/\ker(h)$. As R has characteristic p^e (recall a ring has characteristic κ if $\kappa 1 = 0$ and κ is the minimal such number), $\ker h = (p^{e-1})$. Thus by Lemma 15, $\mathrm{Im}(h) \cong R/(p^{e-1})$. Ergo,

$$\mathrm{Im}(h) \cong R/(p^{e-1}) \cong R_{e-1,k}.$$

Thus, elements of $(p) = \mathrm{Im}\, h$ have p-adic representation. As R is split into cosets by (p), every $x \in R$ has unique representation $x = k + pr$ where $k \in \ker h \cong (p^{e-1})$ and $pr \in (p)$. As $|R| = |\mathrm{Im}\, h||\ker h|$ and $|\mathrm{Im}\, h| = |R_{e-1,k}| = p^{(e-1)k}$, it must be $|\ker h| = p^k$. As $\ker h = (p^{e-1})$, hence a cyclic subgroup of R of order p^{e-1}, $\ker h \cong \mathbf{F}_{p^k}$. Thus, $x = k + pr$ has that $k \in T_{e,k}$. Also, $(p) \cong R_{e-1,k}$, so we have r has p-adic representation. Therefore, x has p-adic representation. □

Theorem 1.2 (Uniqueness)**.** For any given e, k, the Galois ring $R_{e,k}$ is unique up to isomorphism.

Proof. Let e, k be given and g, f be basic monic irreducible polynomials of degree k. Let $R_1 = \mathbf{Z}_{p^e}[x]/(f)$ and $R_2 = \mathbf{Z}_{p^e}[x]/(g)$. Let $\mathrm{mod}_p(r) = r + (p)$. As f, g are both basic monic irreducible polynomials of degree k, $\mathrm{mod}_p(R_1) \cong \mathbf{F}_{p^k} \cong \mathrm{mod}_p(R_2)$. Let β_1 and β_2 be generators for $R_1^{\times}, R_2^{\times}$ isomorphic to $\mathbf{Z}_{p^k-1}$ respectively and T_1, T_2 be the corresponding $T_{e,k}$ for each from Theorem 1.1. By Theorem 1.1, we may form an isomorphism,

ϕ, between R_1 and R_2 by sending β_1 to β_2 and extending by p-adic expansion. That is, $\phi(z_0 + pz_1 + \ldots + p^{e-1}z_{e-1}) = z'_0 + pz'_1 + \ldots + p^{e-1}z'_{e-1}$ where $z_i \in T_1$ and $z'_i \in T_2$. □

For an alternative proof of the uniqueness of Galois rings (see [17, Theorem 20]).

Definition 16. We will use $[p^i]$ to mean $(p^i) \setminus (p^{i+1})$.

Any $r \in [p^i]$ has p-adic representation, $r = p^i z_i + p^{i+1}z_{i+1} + \cdots + p^{e-1}z_{e-1}$ where $z_i \in T_{e,k} \setminus \{0\}$ and $z_j \in T_{e,k}$ for $j > i$. Note that $\bigcup_{i=0}^{e}[p^i] = R$ and that $[p^i] \cap [p^j] = \emptyset$ when $i \neq j$.

Lemma 17. Any $s \in [p^i]$ has the form $s = p^i u$ where u is the uniquely determined unit of the form $u_1 + pu_2 + \cdots + p^{e-i-1}u_{e-i-1}$ where $u_i \in T_{e,k}$.

Proof. Let $s \in [p^i]$. That means that $s \in (p^i)$ and $s \notin (p^{i+1})$. As $s \in (p^i)$, $s = p^i u$ for some $u \in R$. Suppose that u is not a unit, then $(u) \neq R$ and so $(u) \subsetneq R$. As R is a local ring, $(u) \in (p)$ and hence $u = pr$ for some $r \in R$. This means that $s = p^i pr = p^{i+1}r$, and so $s \in (p^{i+1})$. This is a contradiction. Thus, u is a unit. □

Lemma 18. Any ideal of $R_{e,k}$ has the form (p^i) for $0 \leq i \leq e$.

Proof. Let I be an ideal of $R_{e,k}$. As $R_{e,k} = \bigcup_{i=0}^{e}[p^i]$, and I is non-empty, all $a \in I$ are in some $[p^i]$. Let $b \in I$ be such that $b \in [p^j]$ and j is minimal. By Lemma 17, $b = p^j u$ for some unit u. Thus, $(b) = (p^j)$. As j is minimal and all other elements of I have form $a = p^i u$ for $i \geq j$, we have $I = (p^j)$. □

1.2.3 Characters of Galois Rings and Their Properties. The proofs of the main theorems rely heavily on characters, which are maps from a ring to the complex numbers. Thus, here we give some background theorems and lemmas on characters over Galois Rings. When the context is clear, we will write R for $R_{e,k}$. We will use $\bar{0}$ to denote the element with all zero entries in the module R^d.

Example 19. We will examine $R_{2,2} = \mathbf{Z}_4[x]/(x^2 + x + 1)$ with $p = 2$. We will use notation from Theorem 1.1. For finding $T_{2,2}$, we must first find β. Since β must be isomorphic to

$\mathbf{Z}_{p^2-1}$, we will take $\beta = x$ and show $\text{ord}(x) = 3$. As $x^2 = 3x+3$ and $x(3x+3) = 3x^2+3x = 3(3x+3)+3x = x+3x+1 = 1$, we have $\text{ord}(x) = 3$. So, $T_{2,2} = \{0, 1, x, 3x+3\}$. We will use this choice of p, β, and $T_{2,2}$ for our examples with $R_{2,2}$.

Definition 20 (Trace map)**.** Let $\text{Tr}_{e,k} : R_{e,k} \to \mathbf{Z}_{p^e}$ be the trace map with

$$\text{Tr}_{e,k}(z) = z + \tau(z) + \tau^2(z) + \cdots + \tau^{k-1}(z)$$

(here $\tau^n = \tau \circ \tau^{n-1}$) where z has p-adic expansion $z_0 + z_1 p + \cdots + z_{e-1}p^{e-1}$ and

$$\tau(z) = z_0^p + pz_1^p + \cdots + p^{e-1}z_{e-1}^p.$$

Lemma 21. For $n \in \mathbf{N}$, $\tau^n(z) = z_0^{p^n} + pz_1^{p^n} + \cdots + p^{e-1}z_{e-1}^{p^n}$ where $z = z_0 + pz_1 + \cdots + p^{e-1}z_{e-1}$ by p-adic expansion.

Proof. We proceed by induction. By definition, this is true for $\tau^1(z)$. Suppose that for all $i < n$, the theorem holds. Then

$$\tau^{n-1}(z_0 + pz_1 + \cdots + p^{e-1}z_{e-1}) = z_0^{p^{n-1}} + pz_1^{p^{n-1}} + \cdots + p^{e-1}z_{e-1}^{p^{n-1}}.$$

Thus,

$$\begin{aligned}
\tau(\tau^{n-1}(z)) &= \tau^n(z) \\
&= (z_0^{p^{n-1}})^p + p(z_1^{p^{n-1}})^p + \cdots + p^{e-1}(z_{e-1}^{p^{n-1}})^p \\
&= z_0^{p^n} + pz_1^{p^n} + \cdots + p^{e-1}z_{e-1}^{p^n}.
\end{aligned}$$

□

Example 22. We compute the trace of $2x + 3 \in R_{2,2}$. First we see that the p-adic expan-

sion of $2x+3$ is $1+2(3x+3)$, so we have

$$\begin{aligned}\mathrm{Tr}_{2,2}(1+2(3x+3)) &= (1+2(3x+3)) + \tau(1+2(3x+3)) \\ &= (1+2(3x+3)) + (1^2+2(3x+3)^2) \\ &= 1+1+2(3x+3)+2x \\ &= 2(1+3+3x+x) \\ &= 0.\end{aligned}$$

Definition 23 ($\chi_{e,k}$)**.** The canonical additive character $\chi_{e,k} : R_{e,k} \to \mathbf{C}^\times$ is defined as

$$\chi_{e,k}(z) = e^{2\pi i \,\mathrm{Tr}_{e,k}(z)/p^e}$$

Example 24. We compute $\chi_{2,2}(3x+2)$. By definition,

$$\chi_{2,2}(3x+2) = e^{2\pi i \,\mathrm{Tr}_{2,2}(3x+2)/2^2}$$

where

$$\begin{aligned}\mathrm{Tr}_{2,2}(3x+2) &= \mathrm{Tr}_{2,2}(x+2(3x+3)) \\ &= x+2(3x+3)+(x^2+2(3x+3)^2) \\ &= x+2(3x+3)+(3x+3)+2x \\ &= x+2x+2+3x+3+2x \\ &= 1.\end{aligned}$$

So,

$$\begin{aligned}\chi_{2,2}(3x+2) &= e^{2\pi i(1)/4} \\ &= e^{\pi i/2} \\ &= 0 + i.\end{aligned}$$

Lemma 25. The canonical additive character χ is non-trivial.

Proof. From [19, §2.2] we see that $\mathrm{Tr}_{1,k} \circ \mu = \rho \circ \mathrm{Tr}_{e,k}$, where μ, ρ are from Definition 2. Note $\mathrm{Tr}_{1,k}$ is also the usual trace from $\mathbf{F}_{p^k}$ to $\mathbf{F}_p$. Notice that from Definition 20 that $\mathrm{Tr}_{1,k}(z_0) = z_0 + z_0^p + \cdots + z_0^{(k-1)p}$. That is $\mathrm{Tr}_{1,k}$ has degree p^{k-1} when viewed as a polynomial over $R_{1,k}$. We know that $|R_{1,k}| = p^k$. Thus, there must exist $a \in R_{1,k}$ such that $\mathrm{Tr}_{1,k}(a) \neq 0$. So in particular, $\mathrm{Tr}_{1,k}(\mu(\iota(a))) \neq 0$ where $\iota : R_{1,k} \to R_{e,k}$ is the standard inclusion map so that $\mu \circ \iota = id$. Thus, $\rho(\mathrm{Tr}_{e,k}(\iota(a))) \neq 0$. As $\rho(0) = 0$, $\mathrm{Tr}_{e,k}(\iota(a)) \neq 0$. Hence $2\pi i \,\mathrm{Tr}_{e,k}(\iota(a))/p^e \neq 0$ and hence $\chi_{e,k}(\iota(a)) \neq 1$. Ergo, $\chi_{e,k}$ is non-trivial. □

Definition 26. Let $\rho_i : R_{e,k} \to R_{e-i,k}$ by $\rho_i(b_0 + pb_1 + \cdots p^{e-1}b_{e-1}) = b_0 + pb_1 + \cdots + p^{e-i-1}b_{e-i-1}$ where $b_0 + pb_1 + \cdots + p^{e-1}b_{e-1}$ is the p-adic expansion of the argument (Definition 1.1).

Lemma 27. If $0 \leq i \leq e$, then ρ_i is a homomorphism.

Proof. Notice that $\rho_i(1) = 1$, and that for any $a, b \in R_{e,k}$,

$$a + b = (a_0 + b_0) + p(a_1 + b_1) + \ldots + p^{e-1}(a_{e-1} + b_{e-1})$$

by the distributive property and p-adic expansion, so

$$\begin{aligned}\rho_i(a+b) &= (a_0+b_0)+p(a_1+b_1)+\ldots+p^{e-i-1}(a_{e-i-1}+b_{e-i-1}) \\ &= (a_0+pa_1+\ldots+p^{e-i-1}a_{e-i-1})+(b_0+pb_1+\ldots+p^{e-i}b_{e-i-1}) \\ &= \rho_i(a)+\rho_i(b).\end{aligned}$$

Also, $ab = \sum_{i=0}^{e}\sum_{j=0}^{i} p^i a_j b_{i-j}$. So

$$\begin{aligned}\rho_i(ab) &= \sum_{i=0}^{e-i-1}\sum_{j=0}^{i} p^i a_j b_{i-j} \\ &= \sum_{i=0}^{e-i-1} p^i a_i \sum_{j=0}^{e-i} p^j b_j \\ &= \rho_i(a)\rho_i(b).\end{aligned}$$

Hence, ρ_i is a homomorphism.

□

Also, ρ_i is equivalent to the natural projection to the quotient ring $R_{e,k}/(p^{e-i}) \cong R_{e-i,k}$.

Example 28. For $R_{2,2}$, we see ρ_1 has codomain $R_{1,2} \cong \mathbf{Z}_{2^1}[x]/(x^2+x+1)$.

Example 29. We compute $\rho_1(x+2)$:

$$\begin{aligned}\rho_1(x+2) &= \rho_1(x+2(1)) \\ &= x\end{aligned}$$

Lemma 30. For every $a \in R_{e,k}$, we have $\chi_{e,k}(p^i a) = \chi_{e-i,k}(\rho_i(a))$, where $\chi_{e,k}$ is the canonical additive character for $R_{e,k}$.

Proof. If $a \in R_{e,k}$, then $p^i a$ has p-adic expansion $p^i a_0 + \cdots + p^{e-1+i} a_{e-1}$ with $a_i \in T_{e,k}$. Note

$$\chi_{e,k}(p^i a) = \exp(2\pi i \operatorname{Tr}_{e,k,1}(p^i a)/p^e)$$

which by definition of Trace (Definition 20) gives

$$\chi_{e,k}(p^i a) = \exp(2\pi i[p^i a + (p^i a_0^p + \cdots + p^{e-1+i} a_{e-1}^p) + \cdots + (p^i a_0^{p^k} + \cdots + p^{e-1+i} a_{e-1}^{p^k})]/p^e).$$

As $R_{e,k}$ has characteristic p^e, the a_{e-i} through a_{e-1} terms become zero. Hence,

$$\begin{aligned}
\chi_{e,k}(p^i a) &= \exp(2\pi i[p^i a + (p^i a_0^p + \cdots + p^{e-1} a_{e-1-i}^p) + \cdots + (p^i a_0^{p^k} + \cdots + p^{e-1} a_{e-1-i}^{p^k})]/p^e) \\
&= \exp(2\pi i[a + (a_0^p + \cdots + p^{e-1-i} a_{e-1-i}^p) + \cdots + (a_0^{p^k} + \cdots + p^{e-1-i} a_{e-1-i}^{p^k})]/p^{e-i}) \\
&= \chi_{e-i,k}(\rho_i(a)).
\end{aligned}$$

□

This gives the following corollary.

Corollary 31. If $a \in R_{e,k}$ is given, then

$$\sum_{z \in p^i R_{e,k}} \chi_{e,k}(az) = \sum_{w \in R_{e-i,k}} \chi_{e-i,k}(\rho_i(a)w).$$

Proof. We use the p-adic expansion of z to obtain

$$\begin{aligned}\sum_{z\in p^i R_{e,k}} \chi_{e,k}(az) &= \sum_{z\in p^i R_{e,k}} \chi_{e,k}(a(p^i z_i + p^{i+1} z_{i+1} + \cdots + p^{e-1} z_{e-1})) \\ &= \sum_{z\in p^i R_{e,k}} \chi_{e,k}(p^i a(z_i + p^1 z_{i+1} + \cdots + p^{e-i-1} z_{e-1})) \\ &= \sum_{w\in R_{e-i,k}} \chi_{e,k}(p^i a\iota(w_0 + p^1 w_1 + \cdots + p^{e-i-1} w_{e-i-1}))\end{aligned}$$

where ι is the inclusion map $\iota : R_{e-i,k} \to R_{e,k}$. By Lemma 30, this is

$$\begin{aligned}\sum_{z\in p^i R_{e,k}} \chi_{e,k}(az) &= \sum_{w\in R_{e-i,k}} \chi_{e-i,k}(\rho_i(a\iota(w))) \\ &= \sum_{w\in R_{e-i,k}} \chi_{e-i,k}(\rho_i(a)w)).\end{aligned}$$

concluding the proof. □

Lemma 32 (Orthogonality)**.** Let e, k be given. For any $a \in R$,

$$\sum_{z\in R} \chi(az) = \begin{cases} |R|, & a = 0 \\ 0, & a \neq 0 \end{cases}$$

Proof. When $a = 0$, then $\chi(az) = \chi(0z) = 1$. So

$$\sum_{z\in R} \chi(az) = \sum_{z\in R} 1 = |R|.$$

When $a \neq 0$, then $a = p^i u$ for some $i < e$ and unit u (Lemma 17). Then we have

$$\begin{aligned}\sum_{z \in R} \chi(az) &= \sum_{z \in R} \chi(p^i u) \\ &= \sum_{z \in R} \chi_{e-i,k}(\rho_i(uz)).\end{aligned}$$

As ρ_i is a homomorphism, we may break R into cosets of $\ker(\rho_i)$. Let S be a set of representatives of $R/\ker(\rho_i)$. This gives,

$$\sum_{z \in R} \chi(az) = \sum_{x \in \ker(\rho_i)} \sum_{y \in S} \chi_{e-i,k}(\rho_i(u(x+y)))$$

As $R/\ker(\rho_i) \cong R/(p^{e-i}) \cong R_{e-i,k}$ by Lemma 15,

$$\sum_{z \in R} \chi(az) = |\ker(\rho_i)| \sum_{y \in R_{e-i,k}} \chi_{e-i,k}(\rho_i(uy)).$$

As u is a unit, $y \mapsto uy$ is an automorphism. So, summing uy is the same as summing over y. Hence,

$$|\ker(\rho_i)| \sum_{y \in R_{e-i,k}} \chi_{e-i,k}(\rho_i(uy)) = p^{ik} \sum_{y \in R_{e-i,k}} \chi_{e-i,k}(\rho_i(y)).$$

Since $y \in R_{e-i,k}$ and ρ_i removes the upper p^{e-i} through p^{e-1} terms, $\rho_i(y) = y$. Hence,

$$|\ker(\rho_i)| \sum_{y \in R_{e-i,k}} \chi_{e-i,k}(\rho_i(uy)) = p^{ik} \sum_{y \in R_{e-i,k}} \chi_{e-i,k}(y).$$

Since $\chi_{e-i,k}$ is a non-trivial character (Lemma 25), there exists $b \in R_{e-i,k}$ such that $\chi_{e-i,k}(b) \neq$

1. Thus,

$$\chi_{e-i,k}(b)\sum_{y\in R_{e-i,k}}\chi_{e-i,k}(y)=\sum_{y\in R_{e-i,k}}\chi_{e-i,k}(b+y)$$

Which as addition forms a group, summing over $y-b$ is the same as summing over y as we are summing over all of $R_{e-i,k}$. Thus,

$$\chi_{e-i,k}(b)\sum_{y\in R_{e-i,k}}\chi_{e-i,k}(y)=\sum_{y-b\in R_{e-i,k}}\chi_{e-i,k}(y)$$

As $R_{e-i,k}$ is a group under addition, this is

$$\chi_{e-i,k}(b)\sum_{y\in R_{e-i,k}}\chi_{e-i,k}(y)=\sum_{y\in R_{e-i,k}}\chi_{e-i,k}(y).$$

Thus, $\chi_{e-i,k}(b)\sum_{y\in R_{e-i,k}}\chi_{e-i,k}(y)=\sum_{y\in R_{e-i,k}}\chi_{e-i,k}(y)$. Since $\chi_{e-i,k}(b)\neq 1$, it must be that $\sum_{y\in R_{e-i,k}}\chi_{e-i,k}(y)=0$. Therefore, $\sum_{z\in R}\chi(az)=0$.

□

Lemma 33. If $0<n<e$ is a given natural number, then

$$\sum_{z\in R^\times}\chi(p^n z)\leq 0$$

when $n<e$.

Proof. Note that

$$\begin{aligned}\sum_{z\in R^\times}\chi(p^n z)&=\sum_{z\in R}\chi(p^n z)-\sum_{z\in(p)}\chi(p^n z)\\&=I+II.\end{aligned}$$

By orthogonality (Lemma 32), $I = 0$. So $\sum_{z \in R^\times} \chi(p^n z) = -\sum_{z \in (p)} \chi(p^n z)$. Thus, when $n+1 = e$, $\sum_{z \in R^\times} \chi(p^n z) = -|(p)| = -|pR_{e,k}|$. In the case that $n+1 \neq e$, by applying Corollary 31,

$$\begin{aligned} -\sum_{z \in R^\times} \chi(p^n z) &= \sum_{pz \in pR_{e,k}} \chi(p^{n+1} z) \\ &= \sum_{w \in R_{e-1,k}} \chi_{e-1,k}(p^n w). \end{aligned}$$

By orthogonality in z, this is 0 (as $n \neq e-1$). Thus, $\sum_{z \in R^\times} \chi(p^n z) \leq 0$ when $n < e$. Further,

$$\sum_{z \in R^\times} \chi(p^n z) = \begin{cases} -|pR_{e,k}| & , \ n+1 = e \\ 0 & , \ n+1 < e \end{cases}$$

□

For more properties of character sums, see [25].

We now state the Cauchy-Schwarz inequality.

Lemma 34 (Cauchy-Schwarz)**.** If $\{a_k\}$ and $\{b_k\}$ are sequences of complex numbers, then

$$\left| \sum_{k=1}^{n} a_k \bar{b}_k \right|^2 \leq \left(\sum_{k=1}^{n} a_k \bar{a}_k \right) \left(\sum_{k=1}^{n} b_k \bar{b}_k \right)$$

where $\bar{z}$ represents the conjugate of complex number z.

2 SINGLE DOT PRODUCTS

We will follow the proof by Covert, Iosevich, and Pakianathan [5, Theorem 1.3.2]. There they study the Erdős distance problem over the integers modulo an odd prime to a power. They study the finite cyclic rings $\mathbf{Z}_{p^l}$ as such results give insights for questions about the rationals and the integers. Their dot product result is as follows:

Theorem 2.1. Let $E \subset (\mathbf{Z}_{p^l})^d$. If $|E| > lp^{l\left(\frac{(2l-1)d}{2l}+\frac{1}{2l}\right)}$, then $\Pi(E) \supset \mathbf{Z}_{p^l}^{\times}$ where $\Pi(E) = \{x \cdot y : x, y \in E\}$.

Their general method of proof is to estimate a counting function $\nu(t)$ (which counts the number of pairs of points with dot products t). They first transform $\nu(t)$ into a character sum, then use the p-adic expansion of elements of $\mathbf{Z}_{p^l}$, then they apply Cauchy-Schwarz, and then they extend their main sum to over all of $\mathbf{Z}_{p^l}$, then they simplify the sum using orthogonality of characters and properties of $\mathbf{Z}_{p^l}$. They get that $\nu(t) = |E|^2/p^l + R(t)$, where $|R(t)| < l|E|p^{l(\frac{d-1}{2}(2-1/l))}$ whenever $|E| > lp^{ld-d/2+1/2}$. We now formally define $\nu(t)$ for the Galois ring setting.

Definition 35. Let e, k be given natural numbers greater than 0. Let $E \subset R_{e,k}^d$. We define $\nu(t) = |\{(x, y) \in E \times E : x \cdot y = t\}|$.

The following is the key estimate for our main result.

Lemma 36. Let p, e, k, d be given natural numbers with p prime, $e \geq 5$, $d \geq 2$, and $k \geq 1$. Then

$$\nu(t) \leq 2|E|/p^{ek}$$

for any $t \in R_{e,k}$ whenever $|E| \geq \sqrt{6+3e}p^{dek-dk/2+ek/2+k/2}$.

Lemma 36 is an application of the more technical result whose proof we delay until later.

Theorem 2.2. Let e, k be given natural numbers greater than 0. Let $E \subset R_{e,k}^d$. Let

$\nu(t) = |\{(x, y) \in E \times E : x \cdot y = t\}|$. For any $t \in R$,

$$\nu(t) < |E|^2/p^{ek} + D(t).$$

Further, the discrepancy $D(t)$, has $D(t) < |E|^2/p^{ek}$ whenever

$$|E| \geq p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\,(2p^{-ik-k} + 1 + p^{-ek})}$$

We now prove Lemma 36.

Proof. Label

$$F = p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\,(2p^{-ik-k} + 1 + p^{-ek})}.$$

By Theorem 2.2, we know that

$$|E| \geq F.$$

Examining F, we see

$$\begin{aligned} F &= p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\,(2p^{-ik-k} + 1 + p^{-ek})} \\ &= p^{ek+dek/2} \sum_{i=0}^{e-1} \sqrt{p^{dik-ik}\,(2p^{-ik-k} + 1 + p^{-ek})} \end{aligned}$$

So,

$$\frac{F}{p^{ek}p^{dek/2}} \leq \sum_{i=0}^{e-1} p^{dik/2-ik/2} \sqrt{2p^{-ik-k} + 1 + p^{-ek}}.$$

For getting a cleaner bound for Theorem 2.2, we now apply Cauchy–Schwarz, which loosens our bound to

$$\begin{aligned}\frac{F}{p^{ek}p^{dek/2}} &\leq \sqrt{\sum_{i=0}^{e-1}(p^{dik/2-ik/2})^2 \sum_{i=0}^{e-1}\sqrt{2p^{-ik-k}+1+p^{-ek}}^2} \\ &\leq \sqrt{\sum_{i=0}^{e-1} p^{dik-ik}\sum_{i=0}^{e-1} 2p^{-ik-k}+1+p^{-ek}}.\end{aligned}$$

This is a sum of geometric series or constants. Thus,

$$\frac{F}{p^{ek}p^{dek/2}} = \sqrt{\frac{1-p^{dek-ek}}{1-p^{dk-k}}\left(2p^{-k}\frac{1-p^{-ek}}{1-p^{-k}}+e+ep^{-ek}\right)}.$$

The above quantity in parenthesis is maximized when e grows large, $k = 1$ and $p = 2$, giving $\frac{1-p^{-ek}}{1-p^{-k}} \leq 2$. This quantity is smaller for all other choices of e, k, and p. Ergo,

$$\begin{aligned}\frac{F}{p^{ek}p^{dek/2}} &\leq \sqrt{\frac{1-p^{dek-ek}}{1-p^{dk-k}}(2p^{-k}+e+ep^{-ek})} \\ &\leq \sqrt{\left(\frac{1}{1-p^{dk-k}}-\frac{p^{dek-ek}}{1-p^{dk-k}}\right)(2p^{-k}+e+ep^{-ek})}.\end{aligned}$$

Let $C = 1/(1-p^{dk-k})$. We may bound $-\frac{p^{dek-ek}}{1-p^{dk-k}}$ by $2p^{dek-ek-dk+k}$ as $\frac{-1}{1-B} \leq \frac{2}{B}$ for any $B \geq 2$. This gives,

$$\frac{F}{p^{ek}p^{dek/2}} \leq \sqrt{(C+2p^{dek-ek-dk+k})\,(2p^{-k}+e+ep^{-ek})}.$$

Since $e \geq 5$, $k \geq 1$, and $p \geq 2$, we have $2p^{-k}+e+ep^{-ek} \leq 2+e$. So,

$$\frac{F}{p^{ek}p^{dek/2}} \leq \sqrt{(C+2p^{dek-ek-dk+k})\,(2+e)}.$$

As $C = 1/(1-p^{dk-k})$, $p^{dk-k} \geq 2$, $|C| \leq 1$, and $C + 2p^{dek-ek-dk+k} \leq (|C|+2)p^{dek-ek-dk+k}$ we have,

$$\begin{aligned}
\frac{F}{p^{ek}p^{dek/2}} &\leq \sqrt{(1+2)p^{dek-ek-dk+k}\,(2+e)} \\
&\leq \sqrt{3(2+e)p^{dek-dk-ek-dk+k}} \\
&\leq \sqrt{6+3e}p^{dek/2-dk/2-ek/2+k/2}
\end{aligned}$$

Thus $F \leq \sqrt{6+3e}p^{dek-dk/2+ek/2+k/2}$ and so $\nu(t) \leq 2|E|/p^{ek}$ whenever

$$|E| > \sqrt{6+3e}p^{dek-dk/2+ek/2+k/2}.$$

□

We now go on to show when Lemma 36 is nontrivial. As $|E| \leq |R^d| = p^{dek}$, this result is non-trivial when

$$p^{dek} \geq \sqrt{6+3e}p^{dek-dk/2+ek/2+k/2},$$

which simplifies to

$$\begin{aligned}
p^{dk/2} &\geq \sqrt{6+3e}p^{ek/2+k/2} \\
p^{dk} &\geq (6+3e)p^{ek+k} \\
dk &\geq ek + k + \log_p(6+3e).
\end{aligned}$$

So, whenever $d \geq e + 1 + \frac{\log_p(6+3e)}{k}$, then we may take a proper subset of $|R^d|$ for Lemma 36.

We now get to the heart of the thesis; the technical result for the number of pairs in Galois rings with specified dot product. We now prove Theorem 2.2.

Proof. Recall that by Lemma 32, $\sum_{r\in R}\chi(ra) = 0$ if $a \neq 0$ and p^{ek} if $a = 0$. Since we are after $x \cdot y = t$, we examine $\sum_{s\in R}\sum_{x,y\in E}\chi(s(x \cdot y - t))$. This sum gives out a p^{ek} precisely when $x \cdot y = t$ and 0 when $x \cdot y \neq t$. Thus, by multiplying this sum by p^{-ek} we get the number of $x, y \in E$ such that $x \cdot y = t$. Thus, we write $\nu(t)$ as below and split $\nu(t)$ into the following parts

$$\begin{aligned}\nu(t) &= p^{-ek}\sum_{s\in R}\sum_{x,y\in E}\chi(s(x \cdot y - t)) \\ &= p^{-ek}\sum_{s\in R}\sum_{x,y\in E}\chi(s(x \cdot y))\chi(-st) \\ &= \nu_0(t) + \cdots + \nu_e(t),\end{aligned}$$

where

$$\nu_i(t) = p^{-ek}\sum_{s\in[p^i]}\sum_{x,y\in E}\chi(s(x \cdot y))\chi(-st).$$

For $\nu_e(t)$, we have

$$\nu_e(t) = p^{-ek}\sum_{x,y\in E}\chi(0(x \cdot y))\chi(-0t) = |E|^2/p^{ek}.$$

This is what gives us the $|E|^2/p^{ek}$ term for $\nu(t)$. Thus the discrepancy is

$$D(t) = \sum_{i=0}^{e-1}\nu_i(t) = p^{-ek}\sum_{s\in R\setminus\{0\}}\sum_{x,y\in E}\chi(s(x \cdot y - t)). \tag{2.1}$$

We now examine $\nu_i(t)$ for some $i \neq e$. Recall,

$$\nu_i(t) = p^{-ek} \sum_{s\in[p^i]} \sum_{x,y\in E} \chi(s(x\cdot y))\chi(-st).$$

We will prepare to use Cauchy-Schwarz 34 by recognizing that

$$\begin{aligned}\nu_i(t) &= p^{-ek}\left(\sum_{x\in E}(1)\sum_{y\in E}\sum_{s\in[p^i]}\chi(s(x\cdot y))\chi(-st)\right)\\ &= \left(\sum_{x\in E}(1)\sum_{y\in E}p^{-ek}\sum_{s\in[p^i]}\chi(s(x\cdot y))\chi(-st)\right).\end{aligned}$$

By applying Cauchy-Schwarz with $a_x = 1$ and $b_x = \sum_{y\in E} p^{-ek}\sum_{s\in[p^i]}\chi(s(x\cdot y))\chi(-st)$,

$$|\nu_i(t)|^2 \le p^{-2ek}\left(\sum_{x\in E}1\bar{1}\right)\left(\sum_{x\in E}\sum_{y\in E}\sum_{s\in[p^i]}\chi(s(x\cdot y))\chi(-st)\overline{\sum_{y'\in E}\sum_{s'\in[p^i]}\chi(s'(x\cdot y'))\chi(-s't)}\right).$$

Because $z\bar{z} \ge 0$ for any $z \in \mathbf{C}$, we may dominate the second sum of $x \in E$ by $x \in R^d$, obtaining,

$$|\nu_i(t)|^2 \le p^{-2ek}|E|\sum_{x\in R^d}\sum_{y,y'}\sum_{s,s'\in[p^i]}\chi(s(x\cdot y - t))\chi(-s'(x\cdot y' - t)).$$

We make use of Lemma 17, which gives that $s \in [p^i]$ has the form $s = p^i u$ in which u is a uniquely determined unit of the form $u_1 + pu_2 + \cdots + p^{e-i-1}u_{e-i-1}$ where $u_i \in T_{e,k}$. Thus as $s, s' \in [p^i]$, we let $s = p^i u$ and $s' = p^i v$. This gives,

$$|\nu_i(t)|^2 \le p^{-2ek}|E|\sum_{x\in R^d}\sum_{y,y'}\sum_{p^iu,p^iv\in[p^i]}\chi(p^i(uy - vy')\cdot x)\chi(p^it(u-v)) \tag{2.2}$$

$$= p^{-2ek}|E| \sum_{y,y'} \sum_{p^i u, p^i v \in [p^i]} \sum_{x \in R^d} \chi(p^i(uy - vy') \cdot x)\chi(p^i t(u-v))$$

$$= p^{-2ek}|E| \sum_{y \in E} \left(\sum_{\substack{y' \in E,\ p^i u, p^i v \in [p^i] \\ p^i(uy - vy') = \bar{0}}} \sum_{x \in R^d} \chi(p^i(uy - vy') \cdot x)\chi(p^i t(u-v)) \right.$$

$$\left. + \sum_{\substack{y' \in E,\ p^i u, p^i v \in [p^i] \\ p^i(uy - vy') \neq \bar{0}}} \sum_{x \in R^d} \chi(p^i(uy - vy') \cdot x)\chi(p^i t(u-v)) \right).$$

By orthogonality in x, when ever $p^i(uy - vy') = \bar{0}$ we get a factor of p^{ek} for each component of x, so a factor of p^{dek}. When $p^i(uy - vy') \neq 0$, we get a factor of zero. Thus,

$$|\nu_i(t)|^2 \leq |E| p^{dek - 2ek} \sum_{\substack{y,y' \in E \\ p^i(uy - vy') = \bar{0} \\ p^i u, p^i v \in [p^i]}} \chi(p^i t(v-u)).$$

We now split this sum into,

$$|\nu_i(t)|^2 \leq I + II,$$

where I has $u = v$ and II has $u \neq v$.

Lemma 37. For I, we have

$$|I| \leq |E|^2 p^{dek + ikd - ek - ik}.$$

Proof. For I, we have

$$I = |E| p^{dek - 2ek} \sum_{\substack{y,y' \in E \\ p^i(uy - vy') = \bar{0} \\ p^i u = p^i v \in [p^i]}} \chi(p^i t(v-u)),$$

which as $u = v$,

$$I = |E|p^{dek-2ek} \sum_{\substack{y,y' \in E \\ p^i u(y-y') = \overline{0} \\ p^i u \in [p^i]}} \chi(p^i t(0)).$$

Let $E(y) = 1$ when $y \in E$ and $E(y) = 0$ when $y \notin E$. As u is a unit, $p^i u(y - y') = \overline{0}$ is the same as $p^i(y - y') = \overline{0}$. As $\chi(p^i t0) = 1$ does not depend on u, we have

$$\begin{aligned} I &= |E|p^{dek-2ek}|[p^i]| \sum_{\substack{y,y' \in R^d \\ p^i(y-y') = \overline{0}}} E(y)E(y') \\ &= |E|p^{dek-2ek}(p^{(e-i)k} - p^{(e-i-1)k}) \sum_{\substack{y,y' \in R^d \\ p^i(y-y') = \overline{0}}} E(y)E(y'). \end{aligned}$$

Note

$$\sum_{\substack{y,y' \in R^d \\ p^i(y-y') = \overline{0}}} E(y)E(y')$$

is count of $(y, y') \in E^2$ such that $y - y' \in (p^{e-i})^d$. This we may bound above by taking an arbitrary $y \in E$ and seeing that there are, at most, $|p^{e-i}R| = p^{ik}$ many choices for each component of y'. This gives

$$\sum_{\substack{y,y' \in R^d \\ p^i(y-y') = \overline{0}}} E(y)E(y') \leq \sum_{y \in E} \sum_{\substack{y' \in R^d \\ p^i(y-y') = \overline{0}}} 1 \leq |E|p^{ikd}.$$

Thus,

$$|I| \leq |E|p^{dek-2ek}(p^{(e-i)k} - p^{(e-i-1)k})|E|p^{ikd} \leq |E|^2 p^{dek+ikd-ek-ik}.$$

□

For II we have $v \neq u$. So,

$$II = |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ p^i u, p^i v \in [p^i] \\ p^i(uy - vy') = \overline{0} \\ u \neq v}} \chi(p^i t(v-u)).$$

Let $v = b$ and $a = u/v$. This gives us,

$$\begin{aligned} II &= |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ p^i u, p^i v \in [p^i] \\ p^i b(ay - y') = \overline{0} \\ u \neq v}} \chi(p^i tb(1-a)) \\ &= II_u + II_n, \end{aligned}$$

where II_u has $1-a$ being a unit and II_n has $1-a$ being a non-unit.

Lemma 38. For II_u we have,

$$|II_u| \leq |E|^2 p^{dek+dik-2ik-k}| + |E|^2 p^{dek+dik-ik}.$$

Proof. For II_u, we have that as $1-a$ is a unit,

$$II_u = |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ p^i u, p^i v \in [p^i] \\ p^i b(ay - y') = \overline{0} \\ u \neq v \\ 1-a \in R^{\times}_{e-i,k}}} \chi(p^i tb(1-a)).$$

As $b = v$ and $p^i v \in [p^i]$, b has the form $b = u_1 + pu_2 + \ldots + p^{e-i-1}u_{e-i-1}$ where $u_i \in T_{e,k}$ by Lemma 17. So, summing over $p^i b \in [p^i]$ is the same as summing over $b \in R^\times_{e-i,k}$. As $a = u/v$ and $1 - a \neq 0$, it must be that $u \neq v$ (allowing us to drop it from the restriction on the summation). This gives,

$$|II_u| \leq |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ b \in R^\times_{e-i,k} \\ p^i b(ay-y') = \bar{0} \\ 1-a \in R^\times_{e-i,k}}} \chi_{e-i,k}(tb(1-a)).$$

Since $p^i b(ay - y') = \bar{0}$, and b is a unit, we must have $ay - y' \in (p^{e-i})^d$, so

$$|II_u| \leq |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ b \in R^\times_{e-i,k} \\ ay-y' \in (p^{e-i})^d \\ 1-a \in R^\times_{e-i,k}}} \chi_{e-i,k}(tb(1-a)).$$

As a is a unit, and $ay - y' \in (p^{e-i})^d$, it must be that for each choice of y, that y' is in a coset of $(p^{e-i})^d$. Being the case that $\chi_{e-i,k}(tb(1-a))$ does not depend on y nor y', we can bound $ay - y' \in (p^{e-i})^d$ by summing $y \in E$, and summing $y' \in -ay + (p^{e-i})^d$, giving $|(p^{e-i})^d| = p^{idk}$ many choices for y'. Pulling out this factor of p^{idk}, we get

$$|II_u| \leq |E| p^{dek-2ek+idk} \sum_{y \in E} \sum_{1-a \in R^\times_{e-i,k}} \sum_{b \in R^\times_{e-i,k}} \chi_{e-i,k}(tb(1-a)).$$

As b sums over $R^\times_{e-i,k}$, by Lemma 33, we have that $II_u = 0$ when $t \notin (p^{e-i-1})$.

When $t \in [p^{e-i-1}]$, we have, by Lemma 33,

$$|II_u| \leq \left| |E| p^{dek-2ek+idk} \sum_{y \in E} \sum_{1-a \in R^{\times}_{e-i,k}} -|pR_{e-i,k}| \right|,$$

which then simplifies as follows:

$$\begin{aligned} |II_u| &\leq \left| -|E| p^{dek-2ek+idk} |E| |R^{\times}_{e-i,k}| |pR_{e-i,k}| \right| \\ &\leq \left| -|E|^2 p^{dek-2ek+idk} p^{(e-i)k} p^{(e-i-1)k} \right| \\ &\leq \left| -|E|^2 p^{dek+dik-2ik-k} \right|. \end{aligned}$$

In the final case that $t \in (p^{e-i})$, we have $\chi(tb(1-a)) = 1$, and so

$$|II_u| \leq |E| p^{dek-2ek+idk} \sum_{y \in E} \sum_{1-a \in R^{\times}_{e-i,k}} |R^{\times}_{e-i,k}|.$$

Which then simplifies as follows:

$$\begin{aligned} |II_u| &\leq |E| p^{dek-2ek+idk} |E| |R^{\times}_{e-i,k}| |R^{\times}_{e-i,k}| \\ &\leq |E| p^{dek-2ek+idk} |E| p^{2(e-i)k} \\ &\leq |E|^2 p^{dek+dik-ik}. \end{aligned}$$

Thus,

$$|II_u| \leq \left| -|E|^2 p^{dek+dik-2ik-k} \right| + |E|^2 p^{dek+dik-ik}$$

□

Lemma 39. For II_n, we have

$$|II_n| \leq |E|^2 p^{dek+dik-2ik-k}.$$

Proof. Recall $v = b$ and $a = u/v$. For II_n, we have $1-a$ being a non-unit, hence $p^i(1-a) \in (p^{i+1})$. Also this requirement already makes satified $u \neq v$. Thus,

$$II_n = |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ p^i v, p^i u \in [p^i] \\ p^i b(ay-y') = \overline{0} \\ p^i(1-a) \in (p^{i+1})}} \chi(p^i tb(1-a)).$$

As summing over $p^i u \in [p^i]$ is the same as summing over $p^i u/v \in [p^i]$, we have,

$$II_n = |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ p^i b, p^i a \in [p^i] \\ p^i b(ay-y') = \overline{0} \\ p^i(1-a) \in (p^{i+1})}} \chi(p^i tb(1-a)).$$

Recall $p^i a \in [p^i]$ means that $a = u_0 + pz_1 + \ldots + p^{e-i-1} z_{e-i-1}$ for some unit u_0 and $z_j \in T_{e,k}$ by Lemma 17. As $1-a$ is not a unit, $a = 1 + pr$ for some $r \in R_{e,k}$. This means that the restriction $p^i(1-a) \in (p^{i+1})$ restricts $p^i a \in [p^i]$ to the subset $p^i a \in p^i + (p^{i+1})$. Thus,

$$II_n = |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ p^i b \in [p^i],\ p^i a \in p^i + (p^{i+1}) \\ p^i b(ay-y') = \overline{0}}} \chi(p^i tb(1-a)).$$

By letting $c = p^i(1-a)$, we have

$$II_n = |E| p^{dek-2ek} \sum_{y \in E} \sum_{\substack{y' \in E,\ p^i b \in [p^i],\ c \in (p^{i+1}) \\ p^i b(ay-y') = \overline{0}}} \chi(tbc).$$

As $p^i b(ay - y') = \overline{0}$ means $y' \in ay + (p^{e-i})^d$ and we no where else depend on y', we may bound this sum by summing $y' \in (p^{e-i})^d$. This gives,

$$|II_n| \leq |E| p^{dek-2ek} \sum_{y \in E} \sum_{y' \in (p^{e-i})^d,\ p^i b \in [p^i],\ c \in (p^{i+1})} \chi(tbc).$$

Which, by Corollary 31 (supressing ρ_i) and pulling out $y' \in (p^{e-i})^d$ is

$$|II_n| \leq |E| p^{dek-2ek} \left|(p^{e-i})^d\right| \sum_{y \in E} \sum_{p^i b \in [p^i]} \sum_{c \in R_{e-i-1,k}} \chi(tbc).$$

By Lemma 32, orthogonality in c, we have $II_n = 0$ when $t \notin (p^{e-i-1})$. Otherwise,

$$\begin{aligned} |II_n| &\leq |E| p^{dek-2ek} \left|(p^{e-i})^d\right| \sum_{y \in E} \sum_{p^i b \in [p^i]} \sum_{c \in R_{e-i-1,k}} 1 \\ &= |E| p^{dek-2ek} \left|(p^{e-i})^d\right| \sum_{y \in E} \sum_{p^i b \in [p^i]} \left|R_{e-i-1,k}\right|. \end{aligned}$$

We now bound II_n by the size of each index of summation's domain. Thus,

$$|II_n| \leq |E| p^{dek-2ek} \left|(p^{e-i})^d\right| |E| \left|[p^i]\right| \left|R_{e-i-1,k}\right|.$$

As $|R_{e-i-1,k}| = p^{(e-i-1)k}$, $|[p^i]| = |(p^i)| - |(p^{i+1})| \leq |(p^i)|$, and $|(p^i)| = p^{(e-i)k}$,

$$|II_n| \leq |E|^2 p^{(e-i)k} p^{dek+dik-2ek+(e-i-1)k}.$$

We simplify this to

$$|II_n| \leq |E|^2 p^{dek+dik-2ik-k}.$$

□

Recall,

$$|II| \leq |II_u| + |II_n|,$$

which by Lemmas 38 and 39 give,

$$\begin{aligned} |II| &\leq \left||E|^2 p^{dek+dik-2ik-k}\right| + |E|^2 p^{dek+dik-ik}\Big| + |E|^2 p^{dek+dik-2ik-k} \\ &\leq 2|E|^2 p^{dek+dik-2ik-k} + |E|^2 p^{dek+dik-ik}. \end{aligned}$$

As $|\nu_i(t)|^2 \leq |I| + |II|$ and by our bounds on II and I (Lemma 37),

$$|\nu_i(t)|^2 \leq 2|E|^2 p^{dek+dik-2ik-k} + |E|^2 p^{dek+dik-ik} + |E|^2 p^{dek+ikd-ek-ik}. \tag{2.3}$$

Thus the discrepancy, $D(t) = \left|\sum_{i=0}^{e-1} \nu_i(t)\right|$, has

$$\begin{aligned} D(t) &\leq \sum_{i=0}^{e-1} \sqrt{2|E|^2 p^{dek+dik-2ik-k} + |E|^2 p^{dek+dik-ik} + |E|^2 p^{dek+ikd-ek-ik}} \\ &\leq \sum_{i=0}^{e-1} \sqrt{|E|^2 p^{dek+dik-ik}\left(2p^{-ik-k} + 1 + p^{-ek}\right)}. \end{aligned}$$

Thus,

$$D(t) \leq |E| \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\left(2p^{-ik-k} + 1 + p^{-ek}\right)} \tag{2.4}$$

So as we want $\nu_e(t) \geq D(t)$, we must have

$$|E|^2/p^{ek} \geq |E| \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\left(2p^{-ik-k}+1+p^{-ek}\right)}$$
$$|E| \geq p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\left(2p^{-ik-k}+1+p^{-ek}\right)}$$

This concludes the proof of Theorem 2.2. □

We also have proved the following two corollaries.

Corollary 40. Let e, k be given. With $R = R_{e,k}$,

$$p^{-2ek}|E| \sum_{y,y' \in E} \sum_{p^i u, p^i v \in [p^i]} \sum_{x \in R^d} \chi(p^i(uy - vy') \cdot x)\chi(p^i t(u-v))$$
$$\leq 2|E|^2 p^{dek+dik-2ik-k} + |E|^2 p^{dek+dik-ik} + |E|^2 p^{dek+ikd-ek-ik}$$

whenever

$$|E| \geq p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\left(2p^{-ik-k}+1+p^{-ek}\right)}$$

Proof. By Equation 2.2 and Equation 2.3 this is immediate. □

Corollary 41. Let e, k be given. With $R = R_{e,k}$,

$$p^{-ek} \sum_{s \in R \setminus \{0\}} \sum_{x,y \in E} \chi(s(x \cdot y - t))$$
$$\leq |E| \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\left(2p^{-ik-k}+1+p^{-ek}\right)}$$

whenever

$$|E| \geq p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik} \left(2p^{-ik-k} + 1 + p^{-ek}\right)}$$

Proof. By the definition of $D(t)$ (Equation 2.1) and Equation 2.4 this is immediate. □

3 PAIRS OF DOT PRODUCTS

Now we extend the single dot product problem to subsets of points that have a specified configuration of dot products. The first such problem we study is for hinges of dot products, which asks for a given set of points and given (α, β), how many triplets of points (a, b, c) have $a \cdot b = \alpha$ and $b \cdot c = \beta$? Figure 3.1 shows a representation of a hinge.

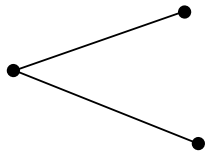

Figure 3.1: A hinge.

The argument for this section follows and extends the paper "Pairs of Dot Products in Finite Fields and Rings" by David Covert and Steven Senger [6], where they obtain bounds on the number triples of elements from subset of a given ring with specified dot products. The rings they consider are $\mathbf{F}_{p^l}$ and $\mathbf{Z}_{p^l}$, the finite field of order p^l and the integers modulo p^l.

Definition 42. Let $\Pi_{\alpha,\beta}(E) = \{(x, y, z) \in E^3 : x \cdot y = \alpha, x \cdot z = \beta\}$ where $E \subset R$ for a given ring R.

The bound that Covert and Senger get for $\Pi_{\alpha,\beta}(E)$ is for $\alpha, \beta \in R_{e,k}^{\times}$. They find when $E \subset (\mathbf{F}_{p^l})^d$ that,

$$|\Pi_{\alpha,\beta}(E)| = \frac{|E|^3}{p^{2l}}(1 + o(1))$$

whenever $|E| > cp^{l(\frac{d+1}{2})}$ for some constant c. In the case $E \subset (\mathbf{Z}_{p^l})^d$, they find,

$$|\Pi_{\alpha,\beta}(E)| = \frac{|E|^3}{p^{2l}}(1 + o(1))$$

whenever $|E| > cp^{dl-d/2+1}$ for some constant c.

Their method of proof is to convert $|\Pi_{\alpha,\beta}(E)|$ into a character sum. Then they split the sum into three terms, I, II, and III, based on if their two indices of summation for orthogonality are zero. When both of these are zero, we get the expected bound of $|E|^3/p^{2l}$. For case II where one and only one index is zero, it simplifies to the sum of two single dot product sums, for which bounds are known by [15]. For III, where both are non-zero, it reduces to a product of single dot product sums.

The reason that they studied hinges is that it relates to the sum-product problem. Their result extends the results of Hart et. al. [15] from a single dot product to a pair of dot products over $\mathbf{Z}_{p^e}$ and $\mathbf{F}_{p^k}$. Here we will further extend the field by considering $\mathbf{Z}_{p^k}$ and $\mathbf{F}_{p^k}$ simultaneously by having our ambient setting be the module $(R_{e,k})^d$.

Lemma 43. Let $d \geq 3, e \geq 5, k \geq 1$. Let $E \subset (R_{e,k})^d$ and suppose that $\alpha, \beta \in R_{e,k}$. We have the bound

$$|\Pi_{\alpha,\beta}(E)| \leq \frac{2|E^3|}{p^{2ek}}$$

whenever

$$|E| \geq \sqrt{35e/8}p^{dek-dk/2+ek/2+k/2}.$$

This lemma relies on the more technical Theorem 3.1 whose statement is below and whose proof is given later in this chapter.

Theorem 3.1. Let $d \geq 2$, $E \subset (R_{e,k})^d$ and suppose that $\alpha, \beta \in R_{e,k}$. We have the bound

$$|\Pi_{\alpha,\beta}(E)| = \frac{|E^3|}{p^{2ek}}(1 + o(1))$$

whenever

$$|E| \geq \max\left(p^{ek}\sum_{i=0}^{e-1}\sqrt{p^{dek+dik-ik}\left(2p^{-ik-k}+1+p^{-ek}\right)}, \sqrt{2G}\right)$$

where

$$G = p^{dek+2ek}e\left(2p^{-k}\frac{p^{dek-2ek}-1}{p^{dk-2k}-1} + (1+p^{-ek})\frac{p^{dek-ek}-1}{p^{dk-k}-1}\right)$$

We now begin the proof of Lemma 43.

Proof. By Theorem 3.1 we know that this is true whenever

$$|E| \geq \max\left(p^{ek}\sum_{i=0}^{e-1}\sqrt{p^{dek+dik-ik}\left(2p^{-ik-k}+1+p^{-ek}\right)}, \sqrt{2G}\right)$$

where

$$G = p^{dek+2ek}e\left(2p^{-k}\frac{p^{dek-2ek}-1}{p^{dk-2k}-1} + (1+p^{-ek})\frac{p^{dek-ek}-1}{p^{dk-k}-1}\right).$$

By Lemma 36, we know

$$p^{ek}\sum_{i=0}^{e-1}\sqrt{p^{dek+dik-ik}\left(2p^{-ik-k}+1+p^{-ek}\right)} \leq \sqrt{6+3e}p^{dek-dk/2+ek/2+k/2}$$

whenever $e \geq 5,\ d \geq 2$, and $k \geq 1$, which is given. We focus now on getting a nice upper bound on G. Recall

$$G = p^{dek+2ek}e\left(2p^{-k}\frac{p^{dek-2ek}-1}{p^{dk-2k}-1} + (1+p^{-ek})\frac{p^{dek-ek}-1}{p^{dk-k}-1}\right).$$

As $1/(B-1) \leq 2/B$ for any $B \geq 2$,

$$\begin{aligned}
G &\leq 2p^{dek+2ek}e\left(2p^{-k}\frac{p^{dek-2ek}-1}{p^{dk-2k}} + (1+p^{-ek})\frac{p^{dek-ek}-1}{p^{dk-k}}\right) \\
&\leq 2p^{dek+2ek}e\left(2p^{-k}\frac{p^{dek-2ek}}{p^{dk-2k}} + (1+p^{-ek})\frac{p^{dek-ek}}{p^{dk-k}}\right) \\
&\leq 2p^{dek+2ek}e\left(2p^{-k+dek-2ek-dk+2k} + (1+p^{-ek})p^{dek-ek-dk+k}\right) \\
&\leq 2p^{2dek+ek-dk+k}e\left(2p^{-ek} + (1+p^{-ek})\right) \\
&\leq 2p^{2dek+ek-dk+k}e\left(3p^{-ek}+1\right)
\end{aligned}$$

Recall, $e \geq 5, p \geq 2, k \geq 1$, so the part in parentheses is maximized when $e = 5,\ p = 2$, and $k = 1$. Thus,

$$\begin{aligned}
G &\leq 2p^{2dek+ek-dk+k}e\left(3(2^{-5})+1\right) \\
&\leq 2p^{2dek+ek-dk+k}e(35/32) \\
&\leq p^{2dek+ek-dk+k}e(35/16).
\end{aligned}$$

Thus, we have that this lemma is true whenever

$$|E| \geq \max\left(\sqrt{6+3e}p^{dek-dk/2+ek/2+k/2}, \sqrt{2(35/16)ep^{2dek+ek-dk+k}}\right).$$

As $\sqrt{35e/8}p^{dek-dk/2+ek/2+k/2} \geq \sqrt{6+3e}p^{dek+ek/2-dk/2+k/2}$ since $e \geq 5$, we have that

$$|E| \geq \sqrt{35e/8}p^{dek-dk/2+ek/2+k/2}.$$

□

This is non-trivial when $|E| < p^{dek}$, giving

$$\begin{aligned} p^{dek} &\geq \sqrt{35e/8}p^{dek-dk/2+ek/2+k/2} \\ p^{dk/2} &\geq \sqrt{35e/8}p^{ek/2+k/2} \\ p^{dk} &\geq 35e/8p^{ek+k} \\ dk &\geq ek + k + \log_p(35e/8) \end{aligned}$$

Thus, this resut is non-trivial when $d \geq e + 1 + \log_p(35e/8)/k$.

We now begin the proof of Theorem 3.1.

Proof. For the sake of brevity, we will use R to stand for $R_{e,k}$. Let χ denote the canonical additive character of R (Definition 23). Recall that,

$$|\Pi_{\alpha,\beta}(E)| = |\{(x, y, z) \in E \times E \times E : x \cdot y = \alpha, x \cdot z = \beta\}|.$$

As we want $x \cdot y = \alpha$ and $x \cdot z = \beta$, the character sum becomes

$$\begin{aligned} |\Pi_{\alpha,\beta}(E)| &= p^{-2ek} \sum_{s,t \in R} \sum_{x,y,z \in E} \chi(s(x \cdot y - \alpha))\chi(t(x \cdot z - \beta)) \\ &= p^{-2ek} \sum_{s,t \in R} \sum_{x,y,z \in E} \chi(-s\alpha)\chi(t\beta)\chi(x \cdot (sy - tz)) \\ &= I + II + III, \end{aligned}$$

where I has $s = t = 0$, II has s or t equal to zero but not both, and III has $s \neq 0$ and $t \neq 0$.

For I, we see

$$I = p^{-2ek} \sum_{s=t=0} \sum_{x,y,z \in E} \chi(-0\alpha)\chi(0\beta)\chi(x \cdot (0y - 0z)) = p^{-2ek}|E|^3. \tag{3.1}$$

For II and III, we will use Theorem 2.2 from Section 2, which requires that

$$|E| \geq p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik} \left(2p^{-ik-k} + 1 + p^{-ek}\right)}$$

which is given.

For II, as either $s = 0$ or $t = 0$ but not both, we may split the sum as two sums with either $s = 0$ or $t = 0$,

$$II = p^{-ek} \left(p^{-ek} \sum_{s \in R, t=0} \sum_{x,y,z \in E} \chi(s(x \cdot y - \alpha)) + p^{-ek} \sum_{t \in R, s=0} \sum_{x,y,z \in E} \chi(t(x \cdot z - \beta) \right). \quad (3.2)$$

Notice that this is the sum of two $\nu(t)$ from Theorem 2.2. Thus by Theorem 2.2, we have $II < 4|E|^2/p^{2ek}$.

For III, we have as $s, t \neq 0$,

$$|III| \leq \left| p^{-2ek} \sum_{s,t \in R_{e,k} \setminus \{0\}} \sum_{x,y,z \in E} \chi(s(x \cdot y - \alpha)) \chi(t(\beta - x \cdot z)) \right| \quad (3.3)$$

which we then prepare for Cauchy-Schwarz. So,

$$\begin{aligned} |III| &\leq \left| p^{-2ek} \sum_{x \in E} \sum_{y \in E} \sum_{s \neq 0} \chi(s(x \cdot y - \alpha)) \sum_{t \neq 0} \sum_{z \in E} \chi(t(\beta - x \cdot z)) \right| \\ &\leq p^{-2ek} \sum_{x \in R^d} \left| \sum_{y \in E} \sum_{s \neq 0} \chi(s(x \cdot y - \alpha)) \right| \left| \sum_{t \neq 0} \sum_{z \in E} \chi(t(\beta - x \cdot z)) \right|. \end{aligned}$$

By Cauchy-Schwarz,

$$|III| \leq p^{-2ek} \left(\sum_{x \in R^d} \left| \sum_{s \neq 0} \sum_{y \in E} \chi(s(x \cdot y - \alpha)) \right|^2 \right)^{1/2} \left(\sum_{x \in R^d} \left| \sum_{t \neq 0} \sum_{z \in E} \chi(t(x \cdot z - \beta)) \right|^2 \right)^{1/2}$$
$$\leq p^{-2ek} III_\alpha \cdot III_\beta.$$

Notice that III_α and III_β are similar, so we will examine III_α. With III_α we prepare to apply Cauchy-Schwarz a second time,

$$III_\alpha^2 = \sum_{x \in R^d} \left| \sum_{s \neq 0} \sum_{y \in E} \chi(s(x \cdot y - \alpha)) \right|^2.$$

So,

$$III_\alpha^2 = \sum_{x \in R^d} \left| \sum_{i=0}^{e-1} \left[(1) \left(\sum_{s \in [p^i]} \sum_{y \in E} \chi(s(x \cdot y - \alpha)) \right) \right] \right|^2. \tag{3.4}$$

Which by Cauchy-Schwarz is

$$III_\alpha^2 \leq \sum_{x \in R^d} \sum_{i=0}^{e-1} (1)^2 \sum_{i=0}^{e-1} \left| \sum_{s \in [p^i]} \sum_{y \in E} \chi(s(x \cdot y - \alpha)) \right|^2$$
$$\leq \sum_{x \in R^d} \sum_{i=0}^{e-1} (1)^2 \sum_{i=0}^{e-1} \left(\sum_{s \in [p^i]} \sum_{y \in E} \chi(s(x \cdot y - \alpha)) \right) \overline{\left(\sum_{s \in [p^i]} \sum_{y \in E} \chi(s(x \cdot y - \alpha)) \right)}$$
$$\leq e \sum_{x \in R^d} \sum_{i=0}^{e-1} \sum_{s,s' \in [p^i]} \sum_{y,y' \in E} \chi(s(x \cdot y - \alpha)) \overline{\chi(s'(x \cdot y' - \alpha))}.$$

Recall that by Lemma 17, $s \in [p^i]$ means $s = p^i u$ for some unit u. Likewise $s' = p^i v$ allowing us to relabel $s, s' \in [p^i]$ as $p^i u, p^i v \in [p^i]$. Since χ is an additive character, we may rearrange the terms in the innermost sum to the below:

$$III_\alpha^2 \leq e \sum_{x \in R^d} \sum_{i=0}^{e-1} \sum_{y,y' \in E} \sum_{p^i u, p^i v \in [p^i]} \chi(p^i(uy - vy') \cdot x) \chi(p^i \alpha(v-u)).$$

So,

$$III_\alpha^2 \leq e \sum_{x \in R^d} \sum_{i=0}^{e-1} \sum_{y,y' \in E} \sum_{p^i u, p^i v \in [p^i]} \chi(p^i(uy - vy') \cdot x) \chi(p^i \alpha(v-u)).$$

We introduce a factor of $|E|p^{-2ek}$ into the outer–most sum to prepare it for Corollary 40

$$III_\alpha^2 \leq (|E|p^{-2ek})^{-1} e \sum_{i=0}^{e-1} |E|p^{-2ek} \sum_{x \in R^d} \sum_{y,y' \in E} \sum_{p^i u, p^i v \in [p^i]} \chi(p^i(uy - vy') \cdot x) \chi(p^i \alpha(v-u)),$$

which by Corollary 40 is

$$\leq (|E|p^{-2ek})^{-1} e \sum_{i=0}^{e-1} \left(2|E|^2 p^{dek+dik-2ik-k} + |E|^2 p^{dek+dik-ik} + |E|^2 p^{dek+dik-ek-ik}\right).$$

Which then simplifies as follows

$$\begin{aligned} III_\alpha^2 &\leq |E|^{-1} p^{2ek} e \sum_{i=0}^{e-1} |E|^2 p^{dek+dik-ik} \left(2p^{-ik-k} + 1 + p^{-ek}\right). \\ &= |E| p^{dek+2ek} e \sum_{i=0}^{e-1} \left(2p^{-k} p^{dik-2ik} + p^{dik-ik} + p^{-ek} p^{dik-ik}\right). \end{aligned}$$

This is a sum of geometric series, so summing each term in i gives,

$$III_\alpha^2 \leq |E|p^{dek+2ek}e\left(2p^{-k}\frac{p^{dek-2ek}-1}{p^{dk-2k}-1}+(1+p^{-ek})\frac{p^{dek-ek}-1}{p^{dk-k}-1}\right).$$

Let

$$F = |E|p^{dek+2ek}e\left(2p^{-k}\frac{p^{dek-2ek}-1}{p^{dk-2k}-1}+(1+p^{-ek})\frac{p^{dek-ek}-1}{p^{dk-k}-1}\right).$$

By equation 3.4, we have $III_\alpha^2 \leq F$. Likewise $III_\beta^2 \leq F$. Ergo, $III_\alpha III_\beta \leq F$.

Thus as $|III| \leq p^{-2ek} III_\alpha III_\beta$,

$$|III| \leq p^{-2ek}F. \tag{3.5}$$

Putting $I,\ II,\ III$ together, we see that

$$I + II + III \leq |E|^3/p^{2ek} + 4|E|^2/p^{2ek} + p^{-2ek}F$$

As we want $I+II+III = |E^3|/p^{2ek}(1+o(1))$, we need show that $II+III = (|E|^3/p^{2ek})o(1)$ when $|E|$ is of sufficient size. Note that by definition of F, we have $e|E|p^{dek}/p^{2ek} \leq F/p^{2ek}$. As $4|E|^2/p^{2ek} < e|E|p^{dek}/p^{2ek}$ for any size of E (recall $E \subset R^d$ and $|R| = p^{ek}$), we need only have $2p^{-2ek}F \leq |E|^3 p^{-2ek}$.

Let $G = F/|E|$. This gives rise to the inequality,

$$|E|^3 p^{-2ek} \geq 2p^{-2ek}F$$

which simplifies to

$$|E|^2 \geq 2G$$

$$|E| \geq \sqrt{2G}$$

Thus, as we used Theorem 2.2 earlier in the proof and it requires

$$|E| \geq p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\,(2p^{-ik-k} + 1 + p^{-ek})},$$

we must have

$$|E| \geq \max\left(p^{ek} \sum_{i=0}^{e-1} \sqrt{p^{dek+dik-ik}\,(2p^{-ik-k} + 1 + p^{-ek})}, \sqrt{2G} \right).$$

□

4 CONCLUSION

We studied a variant the Erdős distance problem in the context of Galois rings. As $\mathbf{F}_{p^l}$ and $\mathbf{Z}_{p^l}$ are both a kind of Galois ring, we generalize bounds for those much-studied rings. For future works, we would like to extend the known results on Galois rings with dot products to arbitrary local rings, dot product configurations with cycles, improve bounds for small sets, and re-examine the known theory through the lens of spectral graph theory. Throughout this thesis, we only used fairly elementary character sum estimates for Galois rings. We conjecture it will be straightforward to find and use character sum estimates for other types of local rings as well so long as they have a p-adic representation.

The author is currently working on extending the results to tree configurations. This in turn leads to bounds for an inverse matrix multiplication problem. One of the applications of the trees result is a result for vector matrix multiplication. We expect to be able to use a similar result for matrix-matrix multiplication to give a result for dot product configurations with cycles.

It is possible that further improvements could be made to sharpen these bounds and we did not consider small sets. For studying the Erdős distance problem in finite rings, using character sum estimates and spectral graph theory are the common routes. To the author's knowledge, only character sum estimates have been used in the case of Galois rings and so better results may be obtainable with spectral graph theory.

This work helps tie together much of the current theory of the unit distance problem in the context of dot products over finite rings. This theory also has applications in additive combinatorics in bounding number of solutions to matrix equations. Just as Galois rings are the building blocks of finite local rings, we hope this thesis may be a building block for this area of mathematics.

REFERENCES

[1] D. Barker and S. Senger. Upper bounds on pairs of dot products. *Journal of Combinatorial Mathematics and Combinatorial Computing* 103:211–224, 2017.

[2] G. Bini and F. Flamini. *Finite commutative rings and their applications.* Springer, New York, 2002.

[3] V. Blevins, D. Crosby, E. Lynch and S. Senger. On the number of dot product chains in finite fields and rings. arXiv:2101.03277.

[4] J. Bourgain, N. H. Katz and T. Tao. A sum-product estimate in finite fields, and applications, *Geo. Funct. Anal. GAFA*, 14:27–57, 2003.

[5] D. Covert, A. Iosevich and J. Pakianathan. Geometric configurations in the ring of integers modulo p^ℓ. *Indiana University Mathematics Journal*, 61(5):1949-1969, 2012.

[6] D. Covert and S. Senger. Pairs of dot products in finite fields and rings. *Combinatorial and Additive Number Theory II*, 220:129-138, 2018.

[7] D. S. Dummit and R. M. Foote. *Abstract algebra*, (3rd ed.), Wiley, 2004.

[8] Z. Dvir. On the size of Kakeya sets in finite fields. *Journal of the American Mathematical Society*, 22:1093–1097, 2008.

[9] P. Erdős. On sets of distances of n points. *The American Mathematical Monthly*, 53:248–250, 1946.

[10] P. Erdős. On the sum and difference of squares of primes. *J. Lond. Math. Soc.*, 2:133-136, 1937.

[11] P. Erdős and E. Szemerédi. On sums and products of integers. In *Studies in Pure Mathematics*, pages 213-218. Springer, New York, 1983.

[12] J. Garibaldi, A. Iosevich and S. Senger. *The Erdős distance problem*. Student mathematical library, American Mathematical Society, Providence, R.I, 2011.

[13] D. J. Garling. The Cauchy-Schwarz master class: An introduction to the art of mathematical inequalities by J. Michael Steele. *Am. Math. Mon.*, 112:575–579, 2005.

[14] L. Guth and N. H. Katz. On the Erdős distinct distances problem in the plane. *Ann. of Math.*, 181:155–190, 2015.

[15] D. Hart, A. Iosevich, D. Koh and M. Rudnev. Averages over hyperplanes, sum-product theory in vector spaces over finite fields and the Erdős-Falconer distance conjecture. *Transactions of the American Mathematical Society*, 363:3255–3275, 2007.

[16] P. Hoffman. Paul erdős. *Britannica*, Accessed 2022.

[17] G. Holdman. Error-correcting codes over Galois rings. *Whitman College*, 2016.

[18] A. Iosevich and M. Rudnev. Erdős distance problem in vector spaces over finite fields. *Transactions of the American Mathematical Society*, 359:6127–6142, 2005.

[19] Y. Jang and S. P. Jun. The Gauss sums over Galois rings and its absolute values. *The Korean Journal of Mathematics*, 26:519–535, 2018.

[20] N. N. Katz and G. Tardos. A new entropy inequality for the Erdős distance problem. *Contemporary Mathematics* 342, 2004.

[21] S. C. Kilmer, C. Z. Marshall and S. Senger. Dot product chains. arXiv:2006.11467.

[22] P. Kumar, T. Helleseth and A. R. Calderbank. An upper bound for some exponential sums over Galois rings and applications. *Proceedings of 1994 IEEE International Symposium on Information Theory*, 41(2):456-468, 1995.

[23] P. Mattila. *Geometry of sets and measures in Euclidean spaces: fractals and rectifiability*. Cambridge studies in advanced mathematics, Cambridge University Press, Cambridge [England]; New York, 1995.

[24] B. R. McDonald. *Finite rings with identity*. New York : M. Dekker, 1974.

[25] F. Shuqin and H. Wenbao. Character sums over Galois rings and primitive polynomials over finite fields. *Finite Fields and Their Applications*, 10:36–52, 2004.

[26] J. Solymosi and V. H. Vu. Near optimal bounds for the Erdős distinct distances problem in high dimensions. *Combinatorica*, 28:113–125, 2008.

[27] J. H. Spencer, E. Szemerédi and W. T. Trotter. Unit distances in the euclidean plane. *Graph Theory and Combinatorics*, 293-300, 1984.

[28] E. M. Stein and T. S. Murphy. Harmonic analysis: Real-variable methods, orthogonality, and oscillatory integrals. Princeton University Press, 1993.

[29] E. Szemerédi and W. T. Trotter. Extremal problems in discrete geometry. *Combinatorica*, 3:381–392, 1983.

[30] E. Szemerédi and W. T. Trotter. A combinatorial distinction between the Euclidean and projective planes. *Eur. J. Comb.*, 4:385–390, 1983.

[31] T. Tao. The sum-product phenomenon in arbitrary rings. *Contributions Discret. Math.*, 4, 2009.

[32] G. Tzanakis. On the existence of irreducible polynomials with prescribed coefficients over finite fields. *Carleton University*, 2010.