2017

ON P-ADIC FIELDS AND P-GROUPS

Luis A. Sordo Vieira
University of Kentucky, l.sordovieira@gmail.com
Digital Object Identifier: https://doi.org/10.13023/ETD.2017.123

STUDENT AGREEMENT:

I represent that my thesis or dissertation and abstract are my original work. Proper attribution has been given to all outside sources. I understand that I am solely responsible for obtaining any needed copyright permissions. I have obtained needed written permission statement(s) from the owner(s) of each third-party copyrighted matter to be included in my work, allowing electronic distribution (if such use is not permitted by the fair use doctrine) which will be submitted to UKnowledge as Additional File.

I hereby grant to The University of Kentucky and its agents the irrevocable, non-exclusive, and royalty-free license to archive and make accessible my work in whole or in part in all forms of media, now or hereafter known. I agree that the document mentioned above may be made available immediately for worldwide access unless an embargo applies.

I retain all other ownership rights to the copyright of my work. I also retain the right to use in future works (such as articles or books) all or part of my work. I understand that I am free to register the copyright to my work.

REVIEW, APPROVAL AND ACCEPTANCE

The document mentioned above has been reviewed and accepted by the student's advisor, on behalf of the advisory committee, and by the Director of Graduate Studies (DGS), on behalf of the program; we verify that this is the final, approved version of the student's thesis including all changes required by the advisory committee. The undersigned agree to abide by the statements above.

Luis A. Sordo Vieira, Student

Dr. David B. Leep, Major Professor

Dr. Peter Hislop, Director of Graduate Studies

ON P-ADIC FIELDS AND P-GROUPS

DISSERTATION

A dissertation submitted in partial
fulfillment of the requirements for
the degree of Doctor of Philosophy
in the College of Arts and Sciences
at the University of Kentucky

By
Luis Sordo Vieira
Lexington, Kentucky

Director: Dr. David B. Leep, Professor of Mathematics
Lexington, Kentucky 2017

ABSTRACT OF DISSERTATION

ON P-ADIC FIELDS AND P-GROUPS

The dissertation is divided into two parts. The first part mainly treats a conjecture of Emil Artin from the 1930s. Namely, if $f = a_1x_1^d + a_2x_2^d + \cdots + a_{d^2+1}x_{d^2+1}^d$ where the coefficients a_i lie in a finite unramified extension of a rational p-adic field, where p is an odd prime, then f is isotropic. We also deal with systems of quadratic forms over finite fields and study the isotropicity of the system relative to the number of variables. We also study a variant of the classical Davenport constant of finite abelian groups and relate it to the isotropicity of diagonal forms. The second part deals with the theory of finite groups. We treat computations of Chermak-Delgado lattices of p-groups. We compute the Chermak-Delgado lattices for all p-groups of order p^3 and p^4 and give results on p-groups of order p^5.

KEYWORDS: p-adic fields, diagonal forms, unramified extensions, additive equations, number theory

Author's signature: Luis Sordo Vieira

Date: April 26, 2017

ON P-ADIC FIELDS AND P-GROUPS

By
Luis Sordo Vieira

Director of Dissertation: David B. Leep

Director of Graduate Studies: Peter Hislop

Date: April 26, 2017

ACKNOWLEDGMENTS

This material is based upon work supported by the National Science Foundation Graduate Research Fellowship under Grant No.1247392.

The author thanks Dr. David B. Leep for his patience and invaluable input, for late night emails correcting mistakes and providing ideas. He is a mentor few people are lucky enough to have. Without him, this work would be incomplete.

On the group theory part, the author is extremely thankful to Dr. Jack Schmidt. He provided many techniques and corrections to the author.

Many thanks are well deserved by the committee members, Drs. David Leep, Heide Gluessing-Luerssen, Uwe Nagel, Cidambi Srinivasan and Yuming Zhang.

Christine Levitt and Sheri Rhine deserve gratitude for much of their help dealing with scheduling, navigating administrative difficulties and making sure everything was done on time.

The author is very thankful to Dr. Daniel Isaksen and Dr. Frank Morgan, who pushed him to go to graduate school in mathematics. He is also very thankful to Dr. Edray Goins, Dr. Bert Guillou and Dr. Kate Ponto, whose personal advise during graduate school was beyond value.

The author is also very thankful to Dr. Hemar Godinho and Dr. Michael Knapp for referencing him to sources he was unaware of.

Many fruitful conversations happened with the author's fellow classmates Robert Cass, Jon Constable and Dustin Hedmark. The best way to learn mathematics is to share mathematics, and these people endured the sharing from the author many times.

The author is also deeply indebted to his parents, Luis F. Sordo and Nayarit Vieira, for supporting him throughout his life, in obviously more than monetary ways. He is also very thankful to his parents-in-law Dr. Bradley Orchard and Kathy Orchard, who told him to keep going when times were tough.

Without saying, the author is deeply thankful to his wife, Sarah Sordo Vieira, who provided support when the author needed it the most. To her, he owes more than words can describe.

The author also wants to thank all who helped him in his life, who he has not named. Without them he would not be where he is right now. It goes without saying that he loves them all.

TABLE OF CONTENTS

Part I

Number Theory

Chapter 1 Prelude

"It always seems impossible until it's done." Nelson Mandela.

1.1 Notation and basics

A finite field with $q = p^n$ elements, where p is a prime and $n \in \mathbb{N}$, will be denoted by $\mathbb{F}_q$. We recall that $\mathbb{F}_q$ is an n-dimensional vector space over $\mathbb{F}_p$. We recall that the multiplicative group $(\mathbb{F}_q - \{0\}, \times)$, usually denoted $\mathbb{F}_q^\times$, is a cyclic abelian group. That is, $\mathbb{F}_q^\times = \langle \zeta \rangle$ where $\zeta \in \mathbb{F}_q - \{0\}$ is a generator. Furthermore, the characteristic of $\mathbb{F}_q$, denoted $\mathrm{char}(\mathbb{F}_q)$, is equal to p.

We let $\mathbb{Z}$ denote the ring of rational integers. If $a, b \in \mathbb{Z}$, we write (a, b) for the greatest common divisor of a and b. We let $\lfloor a \rfloor$ and $\lceil a \rceil$ denote the usual floor and ceiling functions of a. Thus $\lfloor \frac{1}{2} \rfloor = 0$ and $\lceil \frac{1}{2} \rceil = 1$.

For any unital ring R, we let $R^\times$ denote the group of units of R. Thus for a field F, $F^\times$ denotes the nonzero elements of F.

Let $\mathbb{Q}$ denote the field of rational numbers. Let p be a rational prime number, let $v_p : \mathbb{Q} \to \mathbb{Z} \cup \{\infty\}$ denote the standard p-adic valuation, and let $|\ |_p : \mathbb{Q} \to \mathbb{R}$ denote the induced p-adic norm. Let $\mathbb{Q}_p$ denote the topological completion of $\mathbb{Q}$ with respect to this norm, and let $\mathbb{Z}_p = \{x \in \mathbb{Q}_p | |x|_p \leq 1\}$ denote the p-adic integers. We call $\mathbb{Q}_p$ the rational p-adic field. Let K be an extension of $\mathbb{Q}_p$ with $[K : \mathbb{Q}_p] = n < \infty$. K will be called a p-adic field. Let $\mathcal{O}_K$ denote the ring of integers of K, that is, the integral closure of $\mathbb{Z}_p$ in K. When no confusion shall arise, we shall denote $\mathcal{O}_K$ as simply $\mathcal{O}$. We have no desire nor hope of being complete with our treatment of p-adic fields. Thus we refer the reader to [24] for a gentle introduction. However, some facts are worth mentioning:

$\mathcal{O}_K$ is a discrete valuation ring with maximal ideal (π), where $\pi \in \mathcal{O}_K$ is a generator, usually called a uniformizer. Let e be the ramification index of K and $f = [\mathcal{O}_K/(\pi) : \mathbb{Z}_p/(p)]$ be the inertia degree of f. Then $(\pi^e) = (p)$. Recall that $ef = n = [K : \mathbb{Q}_p]$ and that $\mathcal{O}_K/(\pi) \cong \mathbb{F}_{p^f}$ where $\mathbb{F}_{p^f}$ denotes the finite field with p^f elements. It is called the residue field of K. The function $v_\pi : K \to \mathbb{R} \cup \{\infty\}$ will denote the extension of v_p from $\mathbb{Q}_p$ to K and $|\ |_\pi$ will denote the extension of $|\ |_p$ from $\mathbb{Q}_p$ to K. With respect to this norm, K becomes a complete non-archimedean field. In the special case $e = n = [K : \mathbb{Q}_p]$, K is said to be a totally ramified extension of $\mathbb{Q}_p$. At the other extreme, when $e = 1, f = [K : \mathbb{Q}_p]$, K is said to be unramified. The details can be found in [24, Chapter 5].

Now, let F be any field. By a form of degree $d \geq 1$, we mean an element of $F[x_1, \cdots, x_N]$ where each monomial has the same total degree. For an example, consider $\mathbb{Q}[x_1, x_2]$. Then $x_1 x_2^3 + x_1^4$ is a form of degree 4, whereas $x_1 + x_2^3 x_1$ is not a form of degree 4.

Let F be a field and consider a form f of degree d in $F[x_1, \cdots, x_N]$. Then f is a

diagonal form of degree d if

$$f = a_1x_1^d + a_2x_2^d + \cdots + a_Nx_N^d$$

where $a_i \in F$ for $i = 1, \cdots, N$ with at least one $a_i \neq 0$. That is, each monomial only has one variable appearing in it.

The set $V_F(f) := \{\mathbf{a} \in F^N | f(\mathbf{a}) = 0\}$ is called the (affine) F-variety of f. If $|V_F(f)| > 1$, we say f is F-isotropic. Otherwise, we say f is F-anisotropic.

More generally, let $S = \{f_1, f_2, \cdots, f_s\}$ be a system of forms in $F[x_1, \cdots, x_N]$ over a field F. Let $V_F(S) := \{\mathbf{a} \in F^N | f_i(\mathbf{a}) = 0 \text{ for } 1 \leq i \leq s\}$. If $|V_F(S)| > 1$, we say S is F-isotropic. Otherwise, we say S is F-anisotropic.

F is said to have the C_i property, or to be a C_i field, if any form $f \in F[x_1, \cdots, x_N]$ of degree d where $N > d^i$ is F-isotropic. The smallest i such that F satisfies the C_i property is called the *Diophantine dimension* of F. If no i exists, then F is said to have infinite Diophantine dimension.

1.2 A quick history of Artin's conjecture

Chevalley proved the following remarkable theorem for $\mathbb{F}_q$, the finite field with q elements:

Theorem 1.2.1. *(Chevalley) The number of zeroes in $\mathbb{F}_q$ of a homogeneous polynomial of degree d in $\mathbb{F}_q[x_1, x_2, \cdots, x_{d+1}]$ is a positive multiple of char$(\mathbb{F}_q)$.*

Emil Artin called a field F a quasi-algebraically closed field if F has the property that any homogeneous polynomial f with coefficients in F of degree d in $N > d$ variables is F-isotropic. An immediate corollary of Chevalley's Theorem is that any finite field is quasi-algebraically closed.

Artin's student, Serge Lang, generalized this concept in his dissertation [40] where he defined the C_i property of fields.

Definition 1.2.2. (Lang) A field F is said to have the C_i property, or to be a C_i field, if any homogeneous form $f \in F[x_1, \cdots, x_N]$ of degree d in $N > d^i$ variables is F-isotropic.

For a beautiful (arguably outdated) exposition to C_i fields, the reader should refer to [27].

An important example of a C_2 field is the field $\mathbb{F}_q((X))$, the field of meromorphic series over a finite field (see [41]). The local fields $\mathbb{F}_q((X))$ and $\mathbb{Q}_p$ are remarkably similar, albeit vastly distinct. One way to see that these two fields are not isomorphic is the fact that $\text{char}(\mathbb{F}_p((X))) = p$ and $\text{char}(\mathbb{Q}_p) = 0$. A conjecture usually attributed to Emil Artin states that any homogeneous polynomial of degree d in a finite extension F of $\mathbb{Q}_p$ in more than d^2 variables is F-isotropic (see the preface of [2]). In other words, the conjecture states that any finite extension of $\mathbb{Q}_p$ is a C_2 field. In 1966, the French mathematician Guy Terjanian disproved the conjecture by providing a $\mathbb{Q}_2$-anisotropic form of degree 4 in $18 > 4^2 + 1$ variables (see [57]). He later provided a stronger counterexample by providing a $\mathbb{Q}_2$-anistropic form of degree 4 in $20 > 4^2 + 1$

variables. On the positive side, using methods of model theory, Ax and Kochen proved the following beautiful theorem in [3]:

Given $d \in \mathbb{N}$, there exists a prime $p_0(d)$ such that if $p \geq p_0(d)$, any homogeneous form of degree d over $\mathbb{Q}_p$ in more than d^2 variables is $\mathbb{Q}_p$-isotropic. A classical theorem due to Hasse states that $p_0(2) = 2$. Demyanov [19] proved $p_0(3) \leq 5$ and Lewis proved in [46] that $p_0(3) = 2$.

For a short and expositional survey on recent work see [33].

A variation of Artin's conjecture is to consider *diagonal forms*

$$f = a_1 x_1^d + a_2 x_2^d + \cdots + a_N x_N^d$$

where the a_i lie in a finite extension K of $\mathbb{Q}_p$. Specializing to the case of diagonal forms has yielded some positive results and yet no counterexamples in terms of Artin's conjecture.

Conjecture 1.2.3. *Let K be a finite extension of $\mathbb{Q}_p$. Then any diagonal form*

$$f = a_1 x_1^d + a_2 x_2^d + \cdots + a_{d^2+1} x_{d^2+1}^d,$$

where $a_i \in K^\times$ for $1 \leq i \leq d^2 + 1$, is K-isotropic.

Davenport and Lewis proved the following remarkable theorem in [18]:

Theorem 1.2.4. [18] *Let p be a prime number.*

Let

$$f = a_1 x_1^d + \cdots + a_{d^2+1} x_{d^2+1}^d, \quad a_i \in \mathbb{Q}_p.$$

Then f is $\mathbb{Q}_p$-isotropic.

Let K be a p-adic field. Let $\Gamma_K(d)$ denote the smallest positive integer such that if the number of variables N is greater or equal to $\Gamma_K(d)$, then any diagonal form is K-isotropic. Some bounds do indeed exist for $\Gamma_K(d)$ for K a p-adic field, although the bounds are far from the conjectured $\Gamma_K(d) \leq d^2 + 1$.

It is remarkably difficult to extend the methods that Davenport and Lewis used to prove that $\Gamma_{\mathbb{Q}_p}(d) \leq d^2 + 1$ in [18] to an arbitrary finite extension of $\mathbb{Q}_p$. Among many difficulties is that the main lemma in [18], namely [18, Lemma 1], does not extend to nontrivial extensions of $\mathbb{F}_p$.

However, in the case that K is an unramified extension of $\mathbb{Q}_p$ with $p \geq 3$, Leep and Sordo Vieira have been able to prove many stronger results using the Weil bounds for diagonal forms over finite fields. In particular, Leep and Sordo Vieira proved (Theorem 3.1.2) Artin's conjecture holds for diagonal forms in the case that K is an unramified extension of $\mathbb{Q}_p$ with $p > 2$. This is the main topic of this dissertation.

Of remarkable interest is that many interesting and deep questions remain open. Namely, if K is a ramified extension of $\mathbb{Q}_p$, is it true that $\Gamma_K(d) \leq d^2 + 1$ for all d? If K is an unramified extension of $\mathbb{Q}_2$, is it still true that $\Gamma_K(d) \leq d^2 + 1$?

For completeness, we include some of the previously known results regarding (or related to) Artin's conjecture.

The following is a statement by Alemu for general finite extensions of $\mathbb{Q}_p$, where $n = [K : \mathbb{Q}_p]$. In particular, it is close to the desired bound of $d^2 + 1$ when n is small.

Theorem 1.2.5. [1, Theorem 1] *If $p \geq 3$, then*

$$\Gamma_K(d) \leq \max\{3nd^2 - nd + 1, 2d^3 - d^2\}.$$

If $p = 2$, then

$$\Gamma_K(d) \leq 4nd^2 - nd + 1.$$

Another interesting result is due to Birch in [9].

Theorem 1.2.6. [9] *Let K be a finite extension of $\mathbb{Q}_p$ with inertial degree f. Let $d = mp^\tau$ where $(m, p) = 1$. Then*

$$\Gamma_K(d) \leq (2\tau + 3)^d(\delta^2 d)^{d-1} + 1,$$

where $\delta = (d, p^f - 1)$.

In [56], Skinner stated that $\Gamma_K(d) \leq d((d+1)^{2\tau+1} - 1) + 1$. However, the proof of this result turned out to be flawed, applying Hensel's Lemma incorrectly near the end of the proof. In his subsequent article [55] acknowledging his mistake, Skinner proved the following:

Theorem 1.2.7. [55] *Let $K/\mathbb{Q}_p$ be a finite extension of $\mathbb{Q}_p$. Let $d = mp^\tau$ where $(m, p) = 1$. Then*

$$\Gamma_K(d) \leq d(p^{3\tau}m^2)^{2\tau+1} + 1.$$

The following is the optimal result for a general p-adic field K to the best of the author's knowledge.

Theorem 1.2.8. [14, Theorem 1] *Let $[K : \mathbb{Q}_p] = n < \infty$ and suppose $d = mp^\tau$ with $(m, p) = 1$. Then*

$$\Gamma_K(d) \leq d^{2\tau+5} + 1$$

and

$$\Gamma_K(d) \leq 4nd^2 + 1.$$

In the case of $\mathbb{Q}_p$, the following quantity is of interest:

Definition 1.2.9.

$$\Gamma^*(d) = \sup_{p \text{ prime}} \{\Gamma_{\mathbb{Q}_p}(d)\}.$$

Example. [18] If $d + 1 = p$ is prime, $\Gamma^*(d) = d^2 + 1$.

Proof.

$$\sum_{i=1}^{d} x_i^d + p\sum_{i=1}^{d} x_i^d + \cdots + p^{d-1}\sum_{i=1}^{d} x_i^d \equiv 0 \mod p^d$$

has no primitive solution. Combining this with Theorem 1.2.4 yields the result.

□

In a way, this means that the value conjectured by Artin is best possible. However one can do much better for other values. See, for example, [37] and its references.

Chapter 2 Diagonal equations over finite fields

2.1 On the Chevalley bound

The main goal of this dissertation is to prove Theorem 3.1.2, which proves a conjecture attributed to Emil Artin (see Conjecture 1.2.3) for diagonal forms in the case that K is an unramified extension of $\mathbb{Q}_p$ with $p > 2$.

In order to prove Theorem 3.1.2, we need some auxiliary results about diagonal forms over finite fields. Much effort has been devoted to the isotropicity of diagonal forms over finite fields. See for example the encyclopedic text [48]. In particular, [48, Chapter 6] provides many results and references dealing with the solvability of diagonal forms over finite fields.

Let p be a prime, $q = p^n$ where $n \in \mathbb{N}_{>0}$. Then $\mathbb{F}_q$ denotes the finite field with q elements.

The next theorem is a classical result of Chevalley proved in [15]:

Theorem 2.1.1 (Chevalley)**.** *Let $\{f_i\}_{i=1}^k$ be a set of homogeneous polynomials of degree d_i in $\mathbb{F}_q[x_1, ..., x_N]$ such that $N > \sum_{i=1}^k d_i$. Then the system $\{f_i\}_{i=1}^k$ is $\mathbb{F}_q$-isotropic.*

The following result due to André Weil is a special case of the Riemann Hypothesis for function fields over finite fields. See, for example, [54, Ch. 4, Corollary 6e].

Theorem 2.1.2 (Weil)**.** *Let $\mathbb{F}_q$ denote the finite field of cardinality q. Consider a diagonal form*

$$f = a_1 x_1^m + \cdots + a_N x_N^m$$

where $q \equiv 1 \mod m$ and $a_i \in \mathbb{F}_q^\times$ for $1 \leq i \leq N$. Then

$$\left| |V_{\mathbb{F}_q}(f)| - q^{N-1} \right| \leq \frac{(m-1)^N + (-1)^N (m-1)}{m} (q-1) q^{\frac{N}{2}-1}.$$

In particular, if $|V_{\mathbb{F}_q}(f)| \geq 2$, then f is $\mathbb{F}_q$-isotropic.

Lemma 2.1.3. *Let f be as in Theorem 2.1.2 with $N \geq 3$ and $m \geq 1$. If $m \leq q^{\frac{N-2}{2(N-1)}} + 1$, then f is $\mathbb{F}_q$-isotropic.*

Proof. If $m = 1$, the statement is clear. Suppose $m > 1$.

First, we estimate

$$\frac{(m-1)^N + (-1)^N (m-1)}{m}.$$

$$\begin{aligned} \frac{(m-1)^N + (-1)^N (m-1)}{m} &= \frac{(m-1)^{N-1} \left((m-1) + (-1)^N (m-1)^{-N+2} \right)}{m} \\ &\leq \frac{(m-1)^{N-1} \left((m-1) + 1 \right)}{m} = (m-1)^{N-1}. \end{aligned}$$

A homogeneous form always has a trivial zero, hence $|V_{\mathbb{F}_q}(f)| \geq 1$. Suppose $|V_{\mathbb{F}_q}(f)| = 1$. Then

$$q^{N-1} - 1 \leq \frac{(m-1)^N + (-1)^N(m-1)}{m}(q-1)q^{\frac{N-2}{2}} \leq (m-1)^{N-1}(q-1)q^{\frac{N-2}{2}}.$$

Since $N \geq 3$, this gives

$$q^{N-2} < \frac{q^{N-1}-1}{q-1} \leq (m-1)^{N-1}q^{\frac{N-2}{2}},$$

$$q^{\frac{N-2}{2}} < (m-1)^{N-1}.$$

By assumption, we have $m \leq q^{\frac{N-2}{2(N-1)}} + 1$. Then,

$$q^{\frac{N-2}{2(N-1)}} < m - 1 \leq q^{\frac{N-2}{2(N-1)}} + 1 - 1 = q^{\frac{N-2}{2(N-1)}},$$

a contradiction. □

Let $d = mp^\tau$ where $(m,p) = 1$ and $q = p^f$. Let $\delta = (d, q-1) = (m, q-1)$.

Lemma 2.1.4. $(\mathbb{F}_q^\times)^\delta = (\mathbb{F}_q^\times)^d$.

Proof. $kd + l(q-1) = \delta$ for some $k, l \in \mathbb{Z}$. Hence $a^\delta = (a^k)^d$ for all $a \in \mathbb{F}_q$. Let $d = t\delta$. Hence $a^d = (a^t)^\delta$ for all $a \in \mathbb{F}_q$. Thus $(\mathbb{F}_q^\times)^\delta = (\mathbb{F}_q^\times)^d$. □

Remark. It follows that the form $a_1x_1^d + \cdots + a_sx_s^d$ has a zero in $\mathbb{F}_q$ if and only if $a_1x_1^\delta + \cdots + a_sx_s^\delta$ has a zero in $\mathbb{F}_q$, where $\delta = (d, q-1)$.

The following invariants will be used several times in the dissertation. Thus we isolate them in a definition.

Definition 2.1.5. Let $l_{\mathbb{F}_q}(d)$ be the smallest integer i such that $x_1^d + \cdots + x_i^d = 0$ has a nontrivial zero in $\mathbb{F}_q$.

Let $s_{\mathbb{F}_q}(d)$ be the smallest integer i such that $a_1x_1^d + \cdots + a_ix_i^d = 0$ has a nontrivial zero in $\mathbb{F}_q$ for every choice of $a_1, \ldots, a_i \in \mathbb{F}_q^\times$.

It is straightforward that $2 \leq l_{\mathbb{F}_q}(d) \leq s_{\mathbb{F}_q}(d) \leq d+1$ by Theorem 2.1.1. Note that $l_{\mathbb{F}_q}(\delta) = l_{\mathbb{F}_q}(d)$ and $s_{\mathbb{F}_q}(\delta) = s_{\mathbb{F}_q}(d)$ by Lemma 2.1.4. If the finite field or d is clear from context, we will sometimes write $l(d)$ or l, and $s(d)$ or s.

Lemma 2.1.6.

1. $1 < l_{\mathbb{F}_q}(d) \leq p$.
2. *If $j \geq 2$, $j \mid q-1$, and δ is a divisor of $\frac{q-1}{j}$, then $l_{\mathbb{F}_q}(\delta) \leq j$.*

Proof. (1) We have $1 < l_{\mathbb{F}_q}(d) \leq p$ because $\mathrm{char}(\mathbb{F}_q) = p$.

(2) Suppose δ is a divisor of $\frac{q-1}{j}$. Let ζ be a generator of $\mathbb{F}_q^\times$. Suppose $u\delta = \frac{q-1}{j}$. Then $1 \neq \rho = (\zeta^u)^\delta \in (\mathbb{F}_q^\times)^\delta$ is a j^{th} root of unity and hence $1 + \rho + \cdots + \rho^{j-1} = 0$. Thus $l_{\mathbb{F}_q}(\delta) \leq j$. □

Lemma 2.1.7. *If $\delta \leq q^{\frac{N-2}{2(N-1)}} + 1$, then $s_{\mathbb{F}_q}(\delta) \leq N$.*

Proof. Since $\delta \mid q-1$, this follows from Lemma 2.1.3. □

Lemma 2.1.8. *Assume that q is odd. Then $l_{\mathbb{F}_q}(\delta) = 2$ if and only if $\delta \mid \frac{q-1}{2}$.*

Proof. Assume $l_{\mathbb{F}_q}(\delta) = 2$. Then $a^\delta + b^\delta = 0$, where $a, b \in \mathbb{F}_q^\times$. Hence, $-1 = \left(\frac{a}{b}\right)^\delta$. Then $(-1)^{\frac{q-1}{\delta}} = 1$. Since q is odd, we have $-1 \neq 1$ in $\mathbb{F}_q$, and so $2 \mid \frac{q-1}{\delta}$. Thus $\delta \mid \frac{q-1}{2}$.

If $\delta | \frac{q-1}{2}$, then $l_{\mathbb{F}_q}(\delta) \leq 2$ by Lemma 2.1.6, and thus $l_{\mathbb{F}_q}(\delta) = 2$. □

Theorem 2.1.9. [53] *For $\mathbb{F}_q$ with $q = p^n$ and with $n \geq 2$, if $\delta = 2^{v_2(p^n-1)}$, then $l(\delta) = 3$.*

Remark. The necessity of $n \geq 2$ in Theorem 2.1.9 is easily seen by the fact that

$$x_1^4 + x_2^4 + x_3^4 + x_4^4 = 0$$

has no nontrivial solution in $\mathbb{F}_5$. In fact, if p is a Fermat prime, then $l(\delta) = p$ for δ as in Theorem 2.1.9 for $\mathbb{F}_p$.

Remark. If $\delta = q - 1$, it is clear that $l(\delta) = p = \mathrm{char}(\mathbb{F}_q)$, since

$$x_1^\delta + \cdots + x_s^\delta$$

has no nontrivial solution for $s < p$. Thus $l_{\mathbb{F}_q}(q-1) = p$, where $p = \mathrm{char}(\mathbb{F}_q)$.

Theorem 2.1.10. *Let $\delta = 2^u \cdot 3^v$. Let $q = p^n$ where p is an odd prime and $n = 2^j \cdot 3^k \cdot t$ and $t \geq 5$ where t is odd and not divisble by 3. Then $l_{\mathbb{F}_q}(\delta) \leq 3$.*

Proof. The result is obvious for $p = 3$. Hence, assume $p > 3$. Write $\delta = 2^u 3^v$ and $n = 2^j 3^k t$ where $(t, 2) = (t, 3) = 1$ and $t \geq 5$. First assume that $j = 0$ and $p \equiv 2 \mod 3$. Then n is odd, and so 3 doesn't divide $p^n - 1$. This implies $v = 0$, and so $l_\delta \leq 3$ by Lemma 2.1.6 and Theorem 2.1.9. Now assume that either $j \geq 1$ or $p \equiv 1 \mod 3$. In each case, $p^{2^j 3^k} \equiv 1 \mod 6$, and so $(p^{2^j 3^k})^{t-1} + (p^{2^j 3^k})^{t-2} + \cdots + 1 \equiv t \mod 6$. This is not divisible by either 2 or 3, so it follows that δ divides $p^{2^j 3^k} - 1$ since δ divides $p^n - 1 = (p^{2^j 3^k} - 1)((p^{2^j 3^k})^{t-1} + (p^{2^j 3^k})^{t-2} + \cdots + 1)$. Then $\delta \leq p^{2^j 3^k} - 1 \leq p^{n/4} + 1$. Hence $l_\delta \leq 3$ by Lemma 2.1.7.

□

The following is due to Leep. Originally, the author of the dissertation proved special cases of the following result to prove Theorem 3.2.9 using SageMath. Leep provided the following result, using methods found in [53] and other methods, avoiding the necessity of using a computer and providing a more general statement.

Theorem 2.1.11. *Let p be a prime number with $p \neq 3$, and let $q = p^3$. Then $l_{\mathbb{F}_q}(3(p-1)) \leq 3$.*

Proof. Let $Tr_{\mathbb{F}_q/\mathbb{F}_p} : \mathbb{F}_q \to \mathbb{F}_p$ denote the trace map. We will show that there exists $\alpha \in \mathbb{F}_q^\times$ such that $Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha^3) = 0$. Suppose that this has been accomplished. Then $0 = Tr_{\mathbb{F}_q/\mathbb{F}_p}(\alpha^3) = \alpha^3 + (\alpha^3)^p + (\alpha^3)^{p^2}$. Since $\alpha \neq 0$, we have $1 + \alpha^{3(p-1)} + \alpha^{3(p^2-1)} = 0$. Thus $l_{\mathbb{F}_q}(3(p-1)) \leq 3$.

Let v_1, v_2, v_3 be a vector space basis of $\mathbb{F}_q$ over $\mathbb{F}_p$. Then

$$(xv_1 + yv_2 + zv_3)^3 = g_1(x,y,z)v_1 + g_2(x,y,z)v_2 + g_3(x,y,z)v_3,$$

where $g_1, g_2, g_3 \in \mathbb{F}_p[x,y,z]$ are homogeneous forms of degree 3. Then

$$\begin{aligned} h(x,y,z) :&= Tr_{\mathbb{F}_q/\mathbb{F}_p}\left((xv_1 + yv_2 + zv_3)^3\right) \\ &= \sum_{i=1}^{3} g_i(x,y,z) Tr_{\mathbb{F}_q/\mathbb{F}_p}(v_i) \in \mathbb{F}_p[x,y,z] \end{aligned}$$

is a homogeneous form of degree 3. We will show below that every nontrivial zero of h defined over $\mathbb{F}_p^{alg}$, the algebraic closure of $\mathbb{F}_p$, is nonsingular, and thus h is a nonsingular cubic form. Suppose that this has been accomplished. Then h defines a nonsingular cubic curve of genus 1. The Hasse-Weil estimate implies that h has a nontrivial zero (r,s,t) defined over $\mathbb{F}_p$. It follows that $Tr_{\mathbb{F}_q/\mathbb{F}_p}\left((rv_1 + sv_2 + tv_3)^3\right) = 0$ with $rv_1 + sv_2 + tv_3 \neq 0$, as desired.

For convenience, let $L = \mathbb{F}_p^{alg}$. We now show that every nontrivial zero of h defined over L is nonsingular. We have $\mathbb{F}_q \cong \mathbb{F}_p[x]/(f(x))$ for some irreducible polynomial $f \in \mathbb{F}_p[x]$ with $\deg(f) = 3$. We know that f has three distinct roots $a, b, c \in L$, because $\mathbb{F}_p$ is a perfect field. Thus

$$L[x]/(f(x)) \cong L[x]/(x-a) \times L[x]/(x-b) \times L[x]/(x-c) \cong L \times L \times L.$$

Let $V = \mathbb{F}_p[x]/(f(x))$. We have $Tr_{V/\mathbb{F}_p}\left((xv_1 + yv_2 + zv_3)^3\right) = h(x,y,z)$. It follows that $Tr_{(L\otimes V)/L}\left((xv_1 + yv_2 + zv_3)^3\right) = h(x,y,z)$. From above, we have $L \otimes V \cong L[x]/(f(x)) \cong L \times L \times L$. Let $w_1 = (1,0,0)$, $w_2 = (0,1,0)$, $w_3 = (0,0,1)$ be the L-basis of $(L \otimes V)/L$ corresponding to the decomposition $L \times L \times L$. Since $w_i w_j = 0$ in $L \otimes V$ for $i \neq j$, and $w_i^3 = w_i$ for $1 \leq i \leq 3$, we have

$$Tr_{(L\otimes V)/L}\left((xw_1 + yw_2 + zw_3)^3\right) = x^3 + y^3 + z^3.$$

Since $p \neq 3$, the zeros of $x^3 + y^3 + z^3$ over L are all nonsingular. Since the trace of an element does not depend on the basis chosen, it follows that the zeros of $h(x,y,z)$ over L are also all nonsingular. □

2.2 The Davenport constant of a finite abelian group and relations to diagonal forms over finite fields

In this section, we study the following invariant:

Definition 2.2.1. Let

$$\Delta_{\mathbb{F}_q}^r(d)$$

denote the smallest positive integer such that any system of equations of r diagonal forms over $\mathbb{F}_q$ of degree d in at least $\Delta_{\mathbb{F}_q}^r(d)$ variables is $\mathbb{F}_q$-isotropic.

We study this invariant in a group theoretic setting.

Let $(G, +)$ be a finite abelian group and let S be a multiset of elements of G. Let the Davenport constant of G, $D(G)$, be the smallest natural number such that for any multiset of elements S of G of cardinality $|S| = D(G)$, there exists a nonempty submultiset $S_1 \subset S$ such that $\sum_{g \in S_1} g = 0$, where 0 denotes the identity element of the group. We call a nonempty multiset S_1 such that $\sum_{g \in S_1} g = 0$ a zero-sum multiset.

The Davenport constant and some variants of it have important connections to the area of number theory. See, for example, [31].

Lemma 2.2.2. *Let G be a finite abelian group of order n. Then $D(G) \leq n$.*

Proof. Let S be a multiset $\{g_1, g_2, \cdots, g_n\}$ where $g_i \in G$ for $1 \leq i \leq n$. Of course, we may assume without loss of generality that $g_i \neq 0$ for $1 \leq i \leq n$.

Consider the elements

$h_1 = g_1$

$h_2 = g_1 + g_2$

$h_3 = g_1 + g_2 + g_3$

$h_4 = g_1 + g_2 + g_3 + g_4$

.

.

.

$h_n = \sum_{i=1}^{n} g_i$.

If $h_i = 0$ for $1 \leq i \leq n$, then $S_1 = \{g_1, g_2, \cdots, g_i\}$ is our desired submultiset.

Otherwise, by the Pigeonhole Theorem, $h_i = h_j$ for $i \neq j$. Without loss of generality, suppose $i > j$. Then if $S_1 = \{g_{j+1}, g_{j+2}, \cdots, g_i\}$, we have

$$\sum_{g \in S_1} g = 0.$$

Since S was arbitrarily chosen, we have $D(G) \leq n = |G|$.

□

Corollary 2.2.3. $D(C_m) = m$.

Proof. The multiset $S = \{1, \cdots, 1\}$ of cardinality $m-1$ has no zero-sum submultiset. This shows that $D(C_m) > m - 1$. By Lemma 2.2.2, we have $m - 1 < D(C_m) \leq m$ and thus $D(C_m) = m$. □

Let $D_{\pm}(G)$ be the smallest integer such thar for any sequence $(g_1, g_2, \cdots, g_{D_{\pm}(G)})$, there exists $a_i \in \{0, \pm 1\}$ for $1 \leq i \leq D_{\pm}(G)$ with at least one $a_i \neq 0$ such that $\sum_{i=1}^{D_{\pm}(G)} a_i g_i = 0$. We call $D_{\pm}(G)$ the plus-minus Davenport constant. The coefficients a_i are called *weights*. The sum $\sum_{i=1}^{D_{\pm}(G)} a_i g_i = 0$ is again called a zero-sum. For clarity, we sometimes refer to the sum as a sum with weights.

Consider the map $t_d : \mathbb{F}_p \to \mathbb{F}_p$ where $(d, p-1) | \frac{p-1}{2}$ defined by $t_d(a) = a^d$. Then $\{0, \pm 1\} \subseteq \mathrm{im}(t_d)$.

Let $d \in \mathbb{N}_{>0}$ such that $(d, p-1)|\frac{p-1}{2}$. Consider the system of diagonal forms

$$S = \left\{ f_i = \sum_{j=1}^{m} a_{ij} x_j^d \right\}$$

where $a_{ij} \in \mathbb{F}_p$, $1 \leq i \leq n$.

Consider the sequence of coefficients as elements of $\mathbb{F}_p^n \cong C_p^n$:

$$(a_{11}, a_{21}, \cdots, a_{n1}),$$

$$(a_{12}, a_{22}, \cdots, a_{n2}),$$

$$\vdots$$

$$(a_{1m}, \cdots, a_{nm}).$$

Then, if $D_{\pm(C_p^n)} \leq m$, it follows that the system is $\mathbb{F}_p$-isotropic. In particular, for d such that $(d, p-1)|\frac{p-1}{2}$, we have

$$\Delta_{\mathbb{F}_p}^n(d) \leq D_{\pm}(C_p^n).$$

We isolate this statement:

Proposition 2.2.4. *Let p be a prime and let $d \in \mathbb{N}$ be such that $(d, p-1)|\frac{p-1}{2}$. Let $n \in \mathbb{N}$. Then*

$$\Delta_{\mathbb{F}_p}^n(d) \leq D_{\pm}(C_p^n).$$

Furthermore, if d is such that $(d, p-1) = \frac{p-1}{2}$, we have

$$\Delta_{\mathbb{F}_p}^n(d) = D_{\pm}(C_p^n).$$

Proof. The first statement follows by the discussion above. The second statement follows by noticing that if d is such that $(d, p-1) = \frac{p-1}{2}$, then $\mathrm{im}(t_d) = \{0, \pm 1\}$. □

Corollary 2.2.5. $D_{\pm}(C_p^n) = \Delta_{\mathbb{F}_p}^n(\frac{p-1}{2}) \leq n \cdot \frac{p-1}{2} + 1$.

Proof. By Theorem 2.1.1. □

Proposition 2.2.6. *Let G be a finite abelian group of order n. Then*

$$D_{\pm}(G) \leq \min\{s \in \mathbb{N} \mid 2^s - 1 \geq n\}.$$

Proof. Let $t = \min\{s \in \mathbb{N} \mid 2^s - 1 \geq n\}$ and consider a sequence $g_1, \cdots, g_t$ where $g_i \in G - \{0\}$ where 0 denotes the identity element of G, and suppose it has no zero subsequence. Since we are allowed to invert, we may assume that $g_i \neq g_j$ for $i \neq j$. Furthermore, suppose $g_{i_1} + g_{i_2} + \cdots + g_{i_k} = g_{j_1} + \cdots + g_{j_l}$ and $(i_1, \cdots, i_k) \neq (j_{\sigma(1)}, \cdots, j_{\sigma(l)})$ for any $\sigma \in S_l$, where S_l is the permutation group on the l indices $j_1, \cdots, j_l$. We may cancel elements that appear on the left and right side simultaneously, so we may assume $i_a \neq j_b$ for $1 \leq a \leq k$, $1 \leq b \leq l$. But then $g_{i_1} + g_{i_2} + \cdots + g_{i_k} - (g_{j_1} + \cdots + g_{j_l}) = 0$ is a zero subsequence.

In particular, we may assume all distinct choices of i-tuples of elements of G (up to permutation), $1 \leq i \leq t$, give distinct elements of G. There are $\sum_{i=1}^{t} \binom{t}{i} = 2^t - 1 \geq n$ distinct possible choices for the i-tuples, but only n elements in the group, hence at least some choice of tuple yields zero.

□

For an abelian group G with $|G| = n$, let

$$[G] = \min\{s \in \mathbb{N} | 2^s - 1 \geq n\} = \lceil \log_2(|G| + 1) \rceil.$$

Lemma 2.2.7. *Let G_1, G_2 be two abelian groups. Then*

$$D_{\pm}(G_1) + D_{\pm}(G_2) - 1 \leq D_{\pm}(G_1 \oplus G_2) \leq [G_1] + [G_2].$$

Proof. Let

$$g_1, \cdots, g_{D_{\pm}(G_1)-1}$$

be a sequence of elements of G_1 with no zero subsum with weights ± 1. Similarly, let

$$h_1, \cdots, h_{D_{\pm}(G_2)-1}$$

be a sequence of elements of G_2 with no zero subsum with weights ± 1. Then the sequence

$$(g_1, 0), \cdots, (g_{D_{\pm}(G_1)-1}, 0), (0, h_1), \cdots, (0, h_{D_{\pm}(G_2)-1})$$

has no zero subsum with weights ± 1 and has length

$$D_{\pm}(G_1) - 1 + D_{\pm}(G_2) - 1 = D_{\pm}(G_1) + D_{\pm}(G_2) - 2.$$

Thus,

$$D_{\pm}(G_1 \oplus G_2) > D_{\pm}(G_1) + D_{\pm}(G_2) - 2.$$

For the second bound, by Proposition 2.2.6, it suffices to note that $2^{[G_1]+[G_2]} - 1 \geq (2^{[G_1]} - 1)(2^{[G_2]} - 1) \geq |G_1||G_2| = |G_1 \oplus G_2|$.

□

Proposition 2.2.8. $D_{\pm}(C_n) = \min\{s \in \mathbb{N} | 2^s - 1 \geq n\}$. *In particular, the bound given in Proposition 2.2.6 is sharp.*

Proof. By Proposition 2.2.6, $D_{\pm}(C_n) \leq \min\{s|2^s - 1 \geq n\}$. Let

$$m = \min\{s \in \mathbb{N}|2^s - 1 \geq n\}.$$

We claim the sequence

$$\sum_{i=0}^{m-2} a_i 2^i,$$

where the $a_i \in \{\pm 1\}$ for $0 \leq i \leq m$, has no zero subsum.

Using the standard notation of $|\cdot|_\infty$ denoting the standard absolute value on $\mathbb{Q}$, we see that since

$$\left|\sum_{i=0}^{m-2} a_i 2^i\right|_\infty \leq 2^{m-1} - 1 < n,$$

it suffices to notice that for any subsum

$$a_{i_1} 2^{i_1} + \cdots + a_{i_j} 2^{i_j},$$

we have

$$a_{i_1} 2^{i_1} + \cdots + a_{i_j} 2^{i_j} = 2^{\min\{i_1, \cdots i_j\}} \cdot u$$

where $u \not\equiv 0 \mod 2$ and is thus nonzero. Thus, $m - 1 < D_{\pm}(C_n) \leq m$ and hence $D_{\pm}(C_n) = m$.

□

Corollary 2.2.9.

$$[C_n] + [C_m] - 1 \leq D_{\pm}(C_n \oplus C_m) \leq [C_n] + [C_m].$$

Proof. By Lemma 2.2.7.

□

Corollary 2.2.10. $D_{\pm}(C_p^n) \leq \lceil n \log_2(p) + 1 \rceil$.

Proof.

$$2^{n \log_2(p)+1} = 2 \cdot p^n \geq p^n$$

and thus the result follows by Proposition 2.2.6.

□

Theorem 2.2.11. $D_{\pm}(C_{2^k}^n) = nk + 1$ *for* $k > 1$.

Proof. Since $k > 1$,

$$2^{nk+1} - 1 > 2^{nk} = |C_{2^k}^n|$$

and thus by Proposition 2.2.6, $D_{\pm}(C_{2^k}^n) \leq nk + 1$.

Since $D_{\pm}(C_{2^k}) = k + 1$, we may build a sequence of nk elements of $C_{2^k}^n$ with no zero subsum as in the proof of Lemma 2.2.7, and thus $D_{\pm}(C_{2^k}^n) > nk$.

Combining inequalities, we get $D_{\pm}(C_{2^k}^n) = nk + 1$.

□

Theorem 2.2.12. $D_{\pm}(C_3^n) = n + 1$.

Proof. By Corollary 2.2.5, $D_{\pm}(C_3^n) = \Delta^n_{\mathbb{F}_3}(1) = n + 1$.

□

Proposition 2.2.13. [49, Prop 4.1] *Let m_1, m_2 with $m_1 \geq 4$ and $m_2 \geq 3$. Then*

$$D_{\pm}(C_{m_1} \oplus C_{m_2}) \geq \lfloor \log_2(m_1/3) \rfloor + \lfloor \log_2(m_2/3) \rfloor + 4.$$

Theorem 2.2.14. [49, Theorem 4.3] *Let $n \geq 4$ be an integer with $\{\log_2 n\} \geq \{\log_2 3\}$ where $\{\cdot\}$ denotes the fractional part of a real number. If r is a positive integer such that*

$$\{\log_2 n\} < \frac{\lfloor r/2 \rfloor + 1}{r},$$

then $D_{\pm}(C_n^r) = \lfloor r \log_2 n \rfloor + 1$.

Theorem 2.2.15. $D_{\pm}(C_5^n) = 2n + 1$ *for all n.*

Proof. By Corollary 2.2.5,

$$D_{\pm}(C_5^n) \leq 2n + 1.$$

The sequence

$$(1, 0, \cdots, 0), (2, 0, \cdots, 0),$$
$$(0, 1, 0, \cdots, 0), (0, 2, 0, \cdots, 0),$$
$$, \cdots,$$
$$(0, \cdots, 1), (0, \cdots, 2)$$

is readily verified to have no nontrivial zero subsum with weights ± 1. Thus

$$D_{\pm}(C_5^n) > 2n.$$

Combining the inequalities, we get $D_{\pm}(C_5^n) = 2n + 1$.

□

Theorem 2.2.16. $D_{\pm}(C_7^2) = 6 = \Delta^2_{\mathbb{F}_7}(3)$.

Proof. By Proposition 2.2.6,

$$D_{\pm}(C_7^2) \leq 6.$$

The sequence of elements

$$(1, 0), (0, 1), (1, 5), (6, 5), (4, 5)$$

has no zero subsum with weights ± 1. Thus, $5 < D_{\pm}(C_7^2) \leq 6$. Thus,

$$D_{\pm}(C_7^2) = 6.$$

By Proposition 2.2.4, we have $D_{\pm}(C_7^2) = 6 = \Delta^2_{\mathbb{F}_7}(3)$. □

Theorem 2.2.17. *1.* $D_{\pm}(C_{11}) = 4 = \Delta^1_{\mathbb{F}_{11}}(5)$.

2. $D_{\pm}(C_{11}^2) = 7 = \Delta_{\mathbb{F}_{11}}^2(5)$.

Proof. 1. By Proposition 2.2.8.

2. By Corollary 2.2.9, $D_{\pm}(C_{11}^2) \geq 7$. Since $2^7 - 1 > 121$, by Proposition 2.2.6 we have $D_{\pm}(C_{11}^2) \leq 7$. Thus $D_{\pm}(C_{11}^2) = 7$.

□

Theorem 2.2.18. $D_{\pm}(C_{13}^2) = 8 = \Delta_{\mathbb{F}_{13}}^2(6)$.

Proof. Proposition 2.2.13 yields $D_{\pm}(C_{13}^2) \geq 8$. Since $2^8 - 1 > 169 = 13^2$, Proposition 2.2.6 yields $D_{\pm}(C_{13}^2) \leq 8$. Hence $D_{\pm}(C_{13}^2) = 8$. By Proposition 2.2.4, we have $D_{\pm}(C_{13}^2) = 8 = \Delta_{\mathbb{F}_{13}}^2(6)$. □

Theorem 2.2.19. $D_{\pm}(C_{13}^4) = 15 = \Delta_{\mathbb{F}_{13}}^4(6)$.

Proof. Let $\{\cdot\}$ denote the fractional part of a real number. Since $13 > 4$ and $\{\log_2(13)\} > \{\log_2(3)\}$ and $\{\log_2(13)\} < \frac{2+1}{4}$, we can apply Proposition 2.2.14. This yields $D_{\pm}(C_{13}^4) = \lfloor 4\log_2(13) \rfloor + 1 = 15$.

By Proposition 2.2.4, we have $D_{\pm}(C_{13}^4) = 15 = \Delta_{\mathbb{F}_{13}}^4(6)$.

□

Theorem 2.2.20. *For $r \leq 11$, $D_{\pm}(C_{17}^r) = 4r + 1 = \Delta_{\mathbb{F}_{17}}^r(8)$.*

Proof. Since $D_{\pm}(C_{17}) = 5$ by Proposition 2.2.8, $D_{\pm}(C_{17}^r) \geq 4r + 1$. If $r < 12$, $2^{4r+1} - 1 > 17^r$, and thus $D_{\pm}(C_{17}^r) \leq 4r + 1$ for $r \leq 11$ by Proposition 2.2.6. Thus $D_{\pm}(C_{17}^r) = 4r + 1$ for $r \leq 11$.

By Proposition 2.2.4, we have $D_{\pm}(C_{17}^r) = 4r + 1 = \Delta_{\mathbb{F}_{17}}^r(8)$ for $r \leq 11$.

□

Theorem 2.2.21. *Let $2^{2^n} + 1$ be a Fermat number. If $r \cdot \log_2 \dfrac{2^{2^n}+1}{2^{2^n}} \leq 1$, then $D_{\pm}(C_{2^{2^n}+1}^r) = 2^n r + 1$.*

Proof. By Proposition 2.2.8, $D_{\pm}(C_{2^{2^n}+1}) = 2^n + 1$, since $2^n + 1 = \min\{s \in \mathbb{N} | 2^s - 1 \geq 2^{2^n} + 1 = |C_{2^{2^n}+1}|\}$. Thus, $D_{\pm}(C_{2^{2^n}+1}^r) > 2^n r$ for all r.

If $r \cdot \log_2 \dfrac{2^{2^n}+1}{2^{2^n}} \leq 1$, then

$$2 \geq \left(\frac{2^{2^n}+1}{2^{2^n}}\right)^r.$$

Thus

$$2 \cdot 2^{2^n r} = 2^{2^n r + 1} \geq (2^{2^n} + 1)^r = |C_{2^{2^n}+1}^r|.$$

By Proposition 2.2.6, $D_{\pm}(C_{2^{2^n}+1}^r) \leq 2^n r + 1$.

Combining inequalities, we get $D_{\pm}(C_{2^{2^n}+1}^r) = 2^n r + 1$.

□

Theorem 2.2.22. *Let $\mathbb{F}_q$ be the finite field with q elements, where $q \equiv 1 \mod 2$. Let $d > 2$, and suppose $-1 \in \mathbb{F}_q^d$. Let $\delta = (q-1, d)$. Then, any form*

$$f = \sum_{i=1}^{d} a_i x_i^d$$

is $\mathbb{F}_q$-isotropic. In particular, the bound given by Theorem 2.1.1 is a weak bound for diagonal forms in the case -1 is a dth power.

Proof. By Lemma 2.1.4 and Theorem 2.1.1, we may assume $d = (d, q-1)$. By Proposition 2.2.6, since $-1 \in \mathbb{F}_q^d$, if $2^d - 1 \geq q$, then f has a nontrivial zero in $\mathbb{F}_q$. In particular, we may assume $q \geq 2^d$. By Lemma 2.1.3, if $d \leq 2^{d\frac{d-2}{2(d-1)}} + 1 \leq q^{\frac{d-2}{2(d-1)}} + 1$, then f has a nontrivial zero in $\mathbb{F}_q$. For $d \geq 6$, $d \leq 2^{d\frac{d-2}{2(d-1)}} + 1$, and thus f has a nontrivial zero in $\mathbb{F}_q$. This leaves the cases $d = 3, 4, 5$.

1. $d = 3$.

   Suppose in Theorem 2.1.2, $|V_{\mathbb{F}_q}(f)| = 1$. Then

   $$q^2 - 1 \leq \frac{2^3 - 2}{3}(q-1)q^{\frac{1}{2}}.$$

   This implies

   $$q + 1 \leq 2 \cdot q^{\frac{1}{2}},$$

   which is a contradiction.

2. $d = 4$.

   By Proposition 2.2.6 and Lemma 2.1.3, we may assume $17 \leq q < 27$. Notice $d = 4$ does not divide $q - 1$ for $q = 19, 23$. For $q = 25$, by Theorem 2.1.2, if $|V_{\mathbb{F}_q}(f)| = 1$, this would imply

   $$651 = q^2 + q + 1 \leq \frac{3^4 + 3}{4}q = 525,$$

   which is absurd.

   For $q = 17$, write

   $$f = a_1x_1^4 + a_2x_2^4 + a_3x_3^4 + a_4x_4^4$$

   where the $a_i \in (\mathbb{F}_{17})^\times$. Let $[\cdot]$ denote a residue class of $\mathbb{F}_{17}^\times/(\mathbb{F}_{17}^\times)^4$. Since $-1 \in (\mathbb{F}_{17}^\times)^4$, we may assume $[a_i] \neq [a_j]$ for $j \neq i$. Since $|\mathbb{F}_{17}^\times/(\mathbb{F}_{17}^\times)^4| = 4$ and the residue classes of $[1], [2], [3]$ are distinct in $\mathbb{F}_{17}^\times/(\mathbb{F}_{17}^\times)^4$, we may assume without loss of generality that $a_1 = 1$, $a_2 = 2$, and $a_3 = 3$. But then $a_1(1)^4 + a_2(1)^4 + a_3(2)^4 + a_4(0)^4 = 0$. Thus, f is isotropic.

3. $d = 5$.

   By Proposition 2.2.6, we may assume $32 \leq q$. Furthermore, by Lemma 2.1.3, since $5 < 41^{\frac{5-2}{2(4)}} + 1 = 41^{\frac{3}{8}} + 1$ we may assume $q < 41$. Since $d = 5|q-1$, $q \equiv 1 \mod 5$, but there is no such prime power between 32 and 41.

□

2.3 Systems of quadratic forms over finite fields

We now consider systems of quadratic forms over a finite field $\mathbb{F}_q$ with $q = p^n$ elements, where p is an odd prime.

We find nonsingular anisotropic varieties defined by a system of three quadratic forms in five variables over $\mathbb{F}_q$ for $5 \leq q \leq 47$ via a computer search using SageMath, although we have not checked by hand that these systems of three quadratic forms are actually anisotropic. We use a well known counting technique to count the cardinality of a $\mathbb{F}_q$-variety defined by a system of quadratic forms over $\mathbb{F}_q$. A lot of what follows can be generalized to the case where q is even, although we do not include this.

We restrict our attention to affine varieties, although sometimes it will be convenient to talk about the number of projective zeroes.

We say two quadratic forms $Q_1, Q_2 \in \mathbb{F}_q[x_1, \cdots, x_N]$ are equivalent if there exists an invertible $\mathbb{F}_q$-linear change of variables taking one to the other. We write $Q_1 \sim Q_2$ in this case.

The order, or the rank, of a quadratic form Q_1 is the minimum number of variables necessary to write any form equivalent to Q_1.

We say a quadratic form Q_1 is nondegenerate if it is not equivalent to another form in less variables.

A standard reference for quadratic form theory over fields of characteristic not 2 is [39].

We consider the system $\mathbf{Q} = \{Q_i\}_{i=1}^r$ where each $Q_i \in \mathbb{F}_q[x_1, \cdots, x_N]$ is a quadratic form.

Let $V(\mathbf{Q}) := V$ be the $\mathbb{F}_q$-variety defined by $\mathbf{Q}$.

Let $S(V)$ denote the cardinality of an $\mathbb{F}_q$-variety V, and let $S_0 = S(V(\mathbf{Q}))$.

By Theorem 2.1.1, if $N > 2r$, $|V| > 1$. We are interested in the isotropicity of a system of quadratic forms $\mathbf{Q} = \{Q_i\}_{i=1}^r$, assuming $N \leq 2r$. That is, at the critical bound given by Theorem 2.1.1.

By the $\mathbb{F}_q$-pencil $P(\mathbf{Q})$ of a system of quadratic forms $\mathbf{Q} = \{Q_i\}_{i=1}^r$ we mean the set of all quadratic forms of the type

$$\sum_{i=1}^{r} a_i Q_i$$

where the $a_i \in \mathbb{F}_q$.

Lemma 2.3.1. *Let* $\mathbf{a} \notin V(\mathbf{Q})$. *Then there exists precisely* q^{r-1} *quadratic forms* $Q \in P(\mathbf{Q})$ *such that* $Q(\mathbf{a}) = 0$.

Proof. Since $\mathbf{a} \notin V(\mathbf{Q})$, $Q_i(\mathbf{a}) \neq 0$ for some $1 \leq i \leq r$. Without loss of generality, suppose

$$Q_1(\mathbf{a}) \neq 0.$$

Let

$$Q = \sum_{i=1}^{r} c_i Q_i \in P(\mathbf{Q}),$$

and suppose $Q(\mathbf{a}) = 0$. Then,

$$c_1 Q_1(\mathbf{a}) + \cdots + c_r Q_r(\mathbf{a}) = 0$$

if and only if

$$c_1 = -\frac{c_2 Q_2(\mathbf{a}) + \cdots + c_r Q_r(\mathbf{a})}{Q_1(\mathbf{a})}.$$

In particular, c_1 is completely determined by $c_2, \cdots, c_r$. Since there are q choices for each c_i for $2 \leq i \leq r$, we have q^{r-1} forms in $P(\mathbf{Q})$ vanishing at $\mathbf{a}$.

□

Lemma 2.3.2. *If $\mathbf{a} \in V(\mathbf{Q})$, then every form in $P(\mathbf{Q})$ vanishes at $\mathbf{a}$. In particular, $Q(\mathbf{a}) = 0$ for q^r forms in $P(\mathbf{Q})$.*

Proof. Since $a \in V(\mathbf{Q})$, $Q_i(\mathbf{a}) = 0$ for $1 \leq i \leq r$. Since there are precisely q^r forms in $P(\mathbf{Q})$, and $Q \in P(\mathbf{Q})$ is a linear combination of the Q_i, the result is immediate.

□

Proposition 2.3.3.

$$\sum_{Q \in P(\mathbf{Q})} S(Q) = \sum_{\mathbf{c} \in \mathbb{F}_q^r} S\left(\sum_{i=1}^{r} c_i Q_i\right) = q^{r-1}(q^N - S_0) + q^r S_0.$$

In particular,

$$q^N + \sum_{\mathbf{c} \in \mathbb{F}_q^N - \mathbf{0}} S\left(\sum_{i=1}^{r} c_i Q_i\right) = q^{r-1+N} + q^{r-1}(q-1)S_0.$$

Proof. For the first string of equalities, notice that there are S_0 points in $V(\mathbf{Q})$ and $q^N - S_0$ points not in $V(\mathbf{Q})$ for a total of

$$S_0 + (q^N - S_0) = |\mathbb{F}_q^N|$$

points.

Then Lemma 2.3.1 accounts for the value of $q^{r-1}(q^N - S_0)$ on the right side and Lemma 2.3.2 accounts for the value $q^r S_0$.

The last equality follows from the first and observing that

$$\sum_{\mathbf{c} \in \mathbb{F}_q^r} S(\sum_{i=1}^{r} c_i Q_i) = S(\mathbf{0}) + \sum_{\mathbf{c} \in \mathbb{F}_q^r - \mathbf{0}} S(\sum_{i=1}^{r} c_i Q_i)$$

and

$$S(\mathbf{0}) = q^N,$$

where $\mathbf{0}$ denotes the zero element in $\mathbb{F}_q^r$ and the zero form. □

The following is a consequence of Witt's Cancellation Theorem and the classification of quadratic forms over finite fields, which can be found in [48, Chapter 6, Section 2].

Theorem 2.3.4. *Let $Q \in \mathbb{F}_q[x_1, \cdots, x_N]$ be a nonzero quadratic form. Then Q is equivalent to a non-degenerate form having order m of exactly one of the following types:*

1. $$x_1x_2 + \cdots + x_{m-1}x_m.$$
   In this case, we say Q is of type 1. Furthermore,
   $$S(Q) = q^{N-m}(q^{m-1} + (q-1)q^{\frac{m-2}{2}}).$$

2. $$x_1x_2 + x_3x_4 + \cdots + x_{m-3}x_{m-2} + c_1x_{m-1}^2 + c_2x_{m-1}x_m + c_3x_m^2$$
   where
   $$c_1x_{m-1}^2 + c_2x_{m-1}x_m + c_3x_m^2$$
   is irreducible over $\mathbb{F}_q$. In this case, we say Q is of type 2 and
   $$S(Q) = q^{N-m}(q^{m-1} - (q-1)q^{\frac{m-2}{2}}).$$

3. $$x_1x_2 + x_3x_4 + \cdots + x_{m-2}x_{m-1} + ax_m^2.$$
   In this case, we say Q is of type 3 and
   $$S(Q) = q^{N-m}q^{m-1} = q^{N-1}.$$

To summarize, we have the following:
If $Q \in \mathbb{F}_q[x_1, \cdots, x_N]$ is a quadratic form, then:

$$S(Q) = q^{N-m}\begin{cases} q^{m-1} + q^{\frac{m-2}{2}}(q-1) & \text{if } Q \text{ is of type 1} \\ q^{m-1} - q^{\frac{m-2}{2}}(q-1) & \text{if } Q \text{ is of type 2} \\ q^{m-1} & \text{if } Q \text{ is of type 3} \\ q^m & \text{if } Q \equiv 0. \end{cases}$$

We assume no form Q in the $\mathbb{F}_q$-pencil of $Q_1, \cdots, Q_r$ is the zero form, other than the trivial linear combination (this is essentially a benign assumption, for otherwise we could consider a system of less than r equations).

Theorem 2.3.5. *Let q be an odd prime power and let $Q_1, \cdots, Q_r \in \mathbb{F}_q[x_1, \cdots, x_N]$ be quadratic forms. Furthermore, assume $Q_1, Q_2, \cdots, Q_r$ are $\mathbb{F}_q$-linearly independent. Then*

$$S_0 = q^{N-r} + \sum_{\mathbf{c} \in \mathbb{F}_q^r - \mathbf{0}} \left(\begin{cases} q^{N-\frac{m}{2}-r} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 1} \\ -q^{N-\frac{m}{2}-r} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 2} \\ 0 & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 3} \end{cases} \right). \tag{2.1}$$

Proof. By Proposition 2.3.3, we have

$$q^N + \sum_{\mathbf{c}\in\mathbb{F}_q^r-\mathbf{0}} S\left(\sum_{i=1}^r c_iQ_i\right) =$$

$$q^N + \sum_{\mathbf{c}\in\mathbb{F}_q^r-\mathbf{0}} \left(q^{N-m} \begin{cases} q^{m-1} + q^{\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 1} \\ q^{m-1} - q^{\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 2} \\ q^{m-1} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 3} \end{cases} \right) =$$

$$q^N + \sum_{\mathbf{c}\in\mathbb{F}_q^r-\mathbf{0}} \left(q^{N-1} + \begin{cases} q^{N-m+\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 1} \\ -q^{N-m+\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 2} \\ 0 & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 3} \end{cases} \right) =$$

$$q^N + (q^r-1)q^{N-1} + \sum_{\mathbf{c}\in\mathbb{F}_q^r-\mathbf{0}} \left(\begin{cases} q^{N-m+\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 1} \\ -q^{N-m+\frac{m-2}{2}}(q-1) & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 2} \\ 0 & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 3} \end{cases} \right) =$$

$$q^{r-1+N} + q^{r-1}(q-1)S_0.$$

Hence,

$$q^{N-1} + \sum_{\mathbf{c}\in\mathbb{F}_q^r-\mathbf{0}} \left(\begin{cases} q^{N-m+\frac{m-2}{2}} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 1} \\ -q^{N-m+\frac{m-2}{2}} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 2} \\ 0 & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 3} \end{cases} \right) = q^{r-1}S_0.$$

Finally, dividing both sides by q^{r-1} we get

$$S_0 = q^{N-r} + \sum_{\mathbf{c}\in\mathbb{F}_q^r-\mathbf{0}} \left(\begin{cases} q^{N-m+\frac{m-2}{2}-r+1} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 1} \\ -q^{N-m+\frac{m-2}{2}-r+1} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 2} \\ 0 & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 3} \end{cases} \right) =$$

$$q^{N-r} + \sum_{\mathbf{c}\in\mathbb{F}_q^r-\mathbf{0}} \left(\begin{cases} q^{N-\frac{m}{2}-r} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 1} \\ -q^{N-\frac{m}{2}-r} & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 2} \\ 0 & \text{if } \sum_{i=1}^r c_iQ_i \text{ is of type 3} \end{cases} \right).$$

□

Lemma 2.3.6. *Consider a system of r quadratic forms,*

$$Q_1, \cdots, Q_r$$

in N variables over $\mathbb{F}_q$ where q is odd. Let

$$m_{(a_1,\cdots,a_r)}$$

denote the rank of

$$\sum_{i=1}^{r} a_i Q_i.$$

If

$$N - \frac{m_{\mathbf{a}}}{2} - r > 0$$

for all $\mathbf{a} \in \mathbb{F}_q^r - \mathbf{0}$*, the system* $\{Q_i\}_{i=1}^r$ *is* $\mathbb{F}_q$*-isotropic. In fact,* $q|S_0$*.*

Proof. Under these hypotheses, by equation 2.1 we see the number of solutions $S_0 \equiv 0 \mod q$ and is thus not equal to 1, since a system of homogeneous forms always has at least the trivial zero.

□

Although a much more general statement due to James Ax generalizes the following corollary, we present a special case here as an immediate consequence.

Corollary 2.3.7. *Let* $\mathbb{F}_q$ *denote a finite field where* q *is odd and let* $\mathbf{Q} = \{Q_1, \cdots, Q_r\}$ *be a system of quadratic forms in* $\mathbb{F}_q[x_1, \cdots, x_{2r+1}]$*. Then* $S(\mathbf{Q}) \equiv 0 \mod q$*.*

Proof. Using the notation of Lemma 2.3.6, we have $N = 2r + 1$. Then $N - \frac{m_{\mathbf{a}}}{2} - r = \frac{N}{2} + \frac{N}{2} - r - \frac{m_{\mathbf{a}}}{2} > \frac{N}{2} - \frac{m_{\mathbf{a}}}{2} \geq 0$ for all $\mathbf{a} \in \mathbb{F}_q^r - \mathbf{0}$.

The result now follows by Lemma 2.3.6.

□

Definition 2.3.8. Let k be a field of characteristic not 2 and let $V \subseteq k^N$ be a variety defined by linearly independent diagonal quadratic forms $\{f_1, \cdots, f_r\}$ where $N > r$. Let k^{alg} denote the algebraic closure of k. For a point $P \in V$, $Jac(P)$ is the matrix whose i, j entry is $\frac{\partial}{\partial x_j} f_i(P)$. If the rank of $Jac(P)$ is less than r, then P is a *singular point* of V. A projective variety with no singular points over the algebraic closure is said to be nonsingular. Otherwise, we say it is singular.

We now focus on $r = 3$, $N = 5$. The following are examples where $V(\mathbf{Q})$ is a nonsingular variety, yet it contains no rational points over $\mathbb{F}_q$. We remind the reader that the examples were found via a computer search using SageMath and have not been proven by hand to be anisotropic. They will be given in the following conventions. If

$$A = A_{\mathbf{Q}} = \begin{pmatrix} 1 & 0 & 0 & a_{14} & a_{15} \\ 0 & 1 & 0 & a_{24} & a_{25} \\ 0 & 0 & 1 & a_{34} & a_{35} \end{pmatrix}$$

is the matrix of coefficients of the system Q_i where $Q_i = \sum_{j=1}^{5} a_{ij} x_j^2$ for $1 \leq i \leq 3$, then the variety will be displayed in the form

$$(q, a_{14}, a_{15}, a_{24}, a_{25}, a_{34}, a_{35}) :$$

1. $(5, 2, 2, 1, 2, 4, 2)$

2. $(7, -3, -5, -1, -5, -1, -1)$

3. $(9, 1, 1, 1, a+2, 2 \cdot a, a+1)$ where $\mathbb{F}_9 = \mathbb{F}_3[a]/(a^2 + 2a + 2)$

4. $(11, -2, -2, -1, -5, -2, -1)$

5. $(13, -2, -2, -1, -3, -1, -5)$

6. $(17, -3, -3, -1, -3, -7, -1)$

7. $(19, 1, 1, 1, 2, 1, 6)$

8. $(23, 1, 1, 1, 2, 4, 3)$

9. $(25, 1, 1, 1, a, a, 2)$ where $\mathbb{F}_{25} = \mathbb{F}_5[a]/(a^2 + 4a + 2)$

10. $(27, 1, 1, 1, a^2 + 2a, a, 2a^2 + 2)$ where $\mathbb{F}_{27} = \mathbb{F}_3[a]/(a^3 + 2a + 1)$

11. $(29, 1, 1, 1, 3, 2, 3)$

12. $(31, 1, 1, 1, 2, 4, 1)$

13. $(37, 1, 1, 1, 6, 6, 1)$

14. $(41, 1, 1, 1, 13, 3, 34)$

15. $(43, 1, 1, 1, 5, 1, 19)$

16. $(47, 1, 1, 1, 3, 3, 19)$.

As mentioned in [17], the case of an irreducible variety defined by three quadratic forms in five variables defines an irreducible curve of degree eight and genus five in projective space $\mathbb{P}^4_{\mathbb{F}_q}$. Thus, the Hasse-Weil bounds may be applied and thus an irreducible variety over $\mathbb{F}_q$ defined by three quadratic forms in five variables is $\mathbb{F}_q$-isotropic, provided that $q > 10\sqrt{q} - 1$ ($q \geq 97$). Thus the examples above provide examples of some of the cases not treated by the Hasse-Weil bounds.

We conclude this section with the following conjecture, which we were unable to prove.

Conjecture 2.3.9. *A system of* 3 *quadratic forms defining a nonsingular variety in six variables over* $\mathbb{F}_q$ *where* q *is odd is* $\mathbb{F}_q$*-isotropic.*

Chapter 3 Finite Extensions of $\mathbb{Q}_p$

3.1 Preliminaries

Let p be a prime number and let $\mathbb{Q}_p$ denote the field of p-adic numbers. Let K be a finite extension of $\mathbb{Q}_p$ of degree n and let $\mathcal{O}$ denote the ring of integers of K. Let e denote the ramification degree of K over $\mathbb{Q}_p$ and f denote the inertia degree of K over $\mathbb{Q}_p$. Let $\pi \in \mathcal{O}$ denote a generator of the maximal ideal of $\mathcal{O}$.

In this section, unless otherwise specified, $\mathbb{F}_q$ will always denote the field $\mathcal{O}/(\pi)$.

Furthermore, it is important to recall the following definition.

Definition 3.1.1. Let $l_{\mathbb{F}_q}(d)$ be the smallest integer i such that $x_1^d + \cdots + x_i^d = 0$ has a nontrivial zero in $\mathbb{F}_q$.

Let $s_{\mathbb{F}_q}(d)$ be the smallest integer i such that $a_1x_1^d + \cdots + a_ix_i^d = 0$ has a nontrivial zero in $\mathbb{F}_q$ for every choice of $a_1, \ldots, a_i \in \mathbb{F}_q^\times$.

We will sometimes write $l(d)$ or l, and $s(d)$ or s, when d is understood from context.

Given a diagonal homogeneous form

$$a_1x_1^d + a_2x_2^d + \cdots + a_Nx_N^d, \qquad d \geq 1, a_i \in \mathcal{O}, \tag{3.1}$$

let $\Gamma_K(d)$ denote the smallest positive integer such that if $N \geq \Gamma_K(d)$, then any diagonal form of the type (3.1) has a nontrivial zero defined over K. Let $\Delta_K(d)$ denote the smallest positive integer such that if $N \geq \Delta_K(d)$, then any diagonal form of the type (3.1) with the additional restriction that $a_i \in \mathcal{O}^\times$ has a nontrivial zero defined over K.

For d the degree of a diagonal form of the type 3.1, we will always use the convention $d = mp^\tau$ where $(m, p) = 1$.

Let

$$\gamma = \begin{cases} 1 & \text{if } \tau = 0 \\ \left\lfloor \frac{e}{p-1} \right\rfloor + e\tau + 1 & \text{if } \tau \geq 1. \end{cases}$$

The main theorem in this dissertation is the following:

Theorem 3.1.2. *Let K be an unramified extension of $\mathbb{Q}_p$ of degree n. Let $d = mp^\tau$, where $(m, p) = 1$. The following statements hold:*

1. *If $p \geq 3$ and $n \geq 2$, then $\Delta_K(d) \leq d + 1$, except possibly when $p = 3$, $d = 2 \cdot 3^\tau$ with $\tau \geq 1$, and $n \equiv 1 \mod 2$.*

2. *If $p = 3$, $d = 2 \cdot 3^\tau$ with $\tau \geq 1$, and $n \equiv 1 \mod 2$, then $\Gamma_K(d) \leq d^2 + 1$.*

Consequently, $\Gamma_K(d) \leq d^2 + 1$ for all $p \geq 3$, $d \geq 1$, and all finite unramified extensions $K/\mathbb{Q}_p$ of degree $n \geq 2$.

As already mentioned, the case $K = \mathbb{Q}_p$ appeared in [18]. We can add the following result.

Theorem 3.1.3. *Let $d = mp^\tau$, where $(m, p) = 1$. The following statements hold:*

1. [18] $\Gamma_{\mathbb{Q}_p}(d) \leq d^2 + 1$ *for all p and all $d \geq 1$.*
2. *If $p \geq 3$ and $d \neq (p-1)p^\tau$ with $\tau \geq 1$, then $\Delta_{\mathbb{Q}_p}(d) \leq d + 1$.*
3. $\Delta_{\mathbb{Q}_p}((p-1)p^\tau) \geq p^{\tau+1}$.

A first issue to consider is if such an integer $\Gamma_K(d)$ exists. The following theorem guarantees the existence:

Theorem 3.1.4. [27, Theorem 8.2] $\Gamma_K(d) < \infty$, *a fortiori* $\Delta_K(d) < \infty$.

Although $\Delta_K(d)$ is interesting on its own, the next lemma relates $\Delta_K(d)$ with $\Gamma_K(d)$ and can be found in [56].

Lemma 3.1.5. $\Gamma_K(d) \leq d(\Delta_K(d) - 1) + 1$.

Lemma 3.1.6. *If $\Delta_K(d) \leq d + 1$, then $\Gamma_K(d) \leq d^2 + 1$.*

Proof. It is an immediate consequence of Lemma 3.1.5.

□

In other words, if one can prove $\Delta_K(d) \leq d+1$ for all K, d, then Artin's conjecture for diagonal forms will be proved. Unfortunately, for certain fields K and certain degrees d, $\Delta_K(d) > d + 1$.

Suppose $d = mp^\tau$ where $(m, p) = 1$.

We will need a version of Hensel's Lemma which is often difficult to find in the literature. Thus, we include a proof for the sake of completeness.

Theorem 3.1.7. *Consider a diagonal form*

$$F(x_1, \cdots, x_N) = a_1 x_1^d + \cdots + a_N x_N^d$$

where $a_i \in \mathcal{O}^\times$. Let $d = mp^\tau$ where $(m, p) = 1$. Suppose there exists $z = (z_1, \cdots, z_N) \in \mathcal{O}^N$ such that $F(z) \equiv 0 \bmod \pi^j$ where $j > \frac{e}{p-1} + e\tau$ and $z_i \in \mathcal{O}^\times$ for some $1 \leq i \leq N$. Then there exists $y = (y_1, \cdots, y_N) \in K^N$, $y \neq (0, \cdots, 0)$, such that $F(y) = 0$.

Theorem 3.1.7 is an immediate consequence of Theorem 3.1.9 below.

Lemma 3.1.8. *Let $a, b \in \mathcal{O}$ and let $i \in \mathbb{Z}$, $i \geq \frac{e}{p-1}$. If $a \equiv b \mod \pi^i$, then $a^p \equiv b^p \mod \pi^{i+e}$.*

Proof. Let $a = b + \pi^i k$ where $i \geq \frac{e}{p-1}$. By the Binomial Theorem, we have

$$a^p = b^p + pb^{p-1}\pi^i k + \binom{p}{2} b^{p-2}\pi^{2i}k^2 + \cdots + \pi^{ip}k^p.$$

Since $p \mid \binom{p}{i}$ for $1 \leq i < p$, and $ip \geq e + i$ by assumption, the result follows. □

Theorem 3.1.9. *Suppose that $b, c \in \mathcal{O}^\times$ and that the congruence $cx^d \equiv b \mod \pi^\nu$ has a solution $a \in \mathcal{O}$ for some $\nu \geq \gamma$. Then the congruence $cx^d \equiv b \mod \pi^{\nu+1}$ has a solution t where $t \equiv a \mod \pi^{\nu-e\tau}$. Consequently, the equation $cx^d = b$ has a solution in $\mathcal{O}$.*

Proof. Since $c \in \mathcal{O}^\times$, we may assume, without loss of generality, that $c = 1$.

The case $\tau = 0$ is a simple application of the standard version of Hensel's Lemma. Now assume $\tau \geq 1$. The proof is by induction on τ. We begin with the case $\tau = 1$. Since

$$a^d \equiv b \mod \pi^\nu,$$

we have $a \in \mathcal{O}^\times$ and

$$a^d - b = \pi^\nu j$$

for some $j \in \mathcal{O}$. We will find $g \in \mathcal{O}$ such that $(a + g\pi^{\nu-e})^d \equiv b \mod \pi^{\nu+1}$. By the Binomial Theorem, we have

$$a^d + da^{d-1}g\pi^{\nu-e} + \binom{d}{2}a^{d-2}g^2\pi^{2(\nu-e)} + \cdots + g^d\pi^{d(\nu-e)} \equiv b \mod \pi^{\nu+1}.$$

Hence, we want to find $g \in \mathcal{O}$ such that

$$\pi^\nu j + da^{d-1}g\pi^{\nu-e} + \binom{d}{2}a^{d-2}g^2\pi^{2(\nu-e)} + \cdots + g^d\pi^{d(\nu-e)} \equiv 0 \mod \pi^{\nu+1}.$$

We will show below that

$$\binom{d}{2}a^{d-2}g^2\pi^{2(\nu-e)} + \cdots + g^d\pi^{d(\nu-e)} \equiv 0 \mod \pi^{\nu+1}.$$

If this is true, then the congruence simplifies to

$$\pi^\nu j + da^{d-1}g\pi^{\nu-e} \equiv 0 \mod \pi^{\nu+1}.$$

We have $p = \pi^e k_0$ for some $k_0 \in \mathcal{O}^\times$. Since $d = pm$, we have

$$\pi^\nu j + \pi^e k_0 m a^{d-1}g\pi^{\nu-e} \equiv 0 \mod \pi^{\nu+1}.$$

The congruence simplifies to

$$j + k_0 m a^{d-1}g \equiv 0 \mod \pi,$$

which is solvable for g because $k_0, a, m \in \mathcal{O}^\times$. It remains to check that

$$\binom{d}{2}a^{d-2}g^2\pi^{2(\nu-e)} + \cdots + g^d\pi^{d(\nu-e)} \equiv 0 \mod \pi^{\nu+1}.$$

For $p = 2$, $\tau = 1$, we have $\gamma = 2e + 1$, and so for $i \geq 2$ we have

$$i(\nu - e) \geq 2(\nu - e) = \nu + \nu - 2e \geq \nu + \gamma - 2e = \nu + 1.$$

For $p > 2$, we have two distinct cases. First assume $2 \leq i < p$. Then $p|\binom{d}{i}$ and $\nu \geq \gamma \geq e+1$. Thus

$$v_\pi\left(\binom{d}{i}a^{d-i}g^i\pi^{i(\nu-e)}\right) \geq e+i(\nu-e) \geq e+2(\nu-e) = \nu+\nu-e \geq \nu+\gamma-e \geq \nu+1.$$

Now assume $i \geq p$. We can write $e = h(p-1)+j$ where $h \in \mathbb{Z}$ and $0 \leq j \leq p-2$. Then $\dfrac{e}{p-1} = h + \dfrac{j}{p-1}$. Thus

$$\left\lfloor \frac{e}{p-1} \right\rfloor (p-1) = h(p-1) = e-j \geq e-(p-2).$$

This gives

$$\begin{aligned} i(\nu-e) \geq p(\nu-e) &= \nu+(p-1)\nu-pe \geq \nu+(p-1)\gamma-pe \\ &= \nu+(p-1)\left(e+\left\lfloor \frac{e}{p-1}\right\rfloor+1\right)-pe \\ &\geq \nu+(p-1)e+e-(p-2)+(p-1)-pe = \nu+1. \end{aligned}$$

This finishes the proof for $\tau = 1$. We now assume that $\tau \geq 2$ and that the theorem has been proved for all smaller values of τ. We have

$$(a^p)^{mp^{\tau-1}} = a^d \equiv b \mod \pi^\nu.$$

By induction, there exists $b_0 \in \mathcal{O}$ such that

$$b_0^{mp^{\tau-1}} = b \text{ and } b_0 \equiv a^p \mod \pi^{\nu-e(\tau-1)}.$$

Since the congruence $x^p \equiv b_0 \mod \pi^{\nu-e(\tau-1)}$ has the solution $x = a$, and

$$\nu-e(\tau-1) = \nu-e\tau+e \geq \gamma-e\tau+e = \left\lfloor \frac{e}{p-1}\right\rfloor+e+1,$$

the case $\tau = 1$ of the theorem implies that there exists $t \in \mathcal{O}$ such that

$$t^p = b_0 \text{ and } t \equiv a \bmod \pi^{\nu-e(\tau-1)-e}.$$

Hence

$$t \equiv a \bmod \pi^{\nu-e\tau}.$$

Then $t^d = t^{mp^\tau} = b_0^{mp^{\tau-1}} = b$. This concludes the proof. □

3.2 The unramified case

Proposition 3.2.1. *If $\tau = 0$, then $\Delta_K(d) \leq d+1$.*

Proof. Let G be a diagonal form of degree d in $d+1$ variables where each coefficient of G lies in $\mathcal{O}^\times$. By Theorem 2.1.1 there is a nontrivial solution to $G \equiv 0 \mod \pi$. The result follows from Theorem 3.1.7. □

From here on we assume that $\tau > 0$. We now describe a simplified version of the method of contraction introduced in [18]. Later we will need the full method of contraction from [18].

Let $F = a_1x_1^d + \cdots + a_Nx_N^d$, where each $a_i \in \mathcal{O}^\times$. Let $a_{11}x_{11}^d + \cdots + a_{j1}x_{j1}^d$ be a subform of F that has a nontrivial solution $(y_1, \cdots, y_j)$ in $\mathcal{O}/(\pi) \cong \mathbb{F}_q$, where $q = p^f$. Choose $Y_i \in \mathcal{O}$ such that $\overline{Y_i} = y_i$ for $1 \leq i \leq j$. We may replace Y_1 with $Y_1 + b\pi$ for some $b \in \mathcal{O}$ if necessary so that $0 \neq a_{11}(Y_1z)^d + \cdots + a_{j1}(Y_jz)^d = \pi^g tz^d$ where $t \in \mathcal{O}^\times$, $g \geq 1$, and z is a variable. We call z a derived variable, and we say that z is a variable at level g. We now discard the variables $x_{11}, \ldots, x_{j1}$ from F and include $\pi^g tz^d$ as a new term in F. We repeat the process with the remaining terms in F, excluding any term involving a derived variable. Continue this process until there are no more subforms of F involving only the original variables that have a nontrivial solution in $\mathcal{O}/(\pi)$. We discard the remaining unused original variables of F. Only derived variables now remain in F.

For all $i \geq 1$, let $w_{1,i}$ denote the number of derived variables of F created by this process at level i. We now have a new form $G = \pi G^{(1)} + \pi^2 G^{(2)} + \cdots$ where for each $i \geq 1$, $G^{(i)}$ has $w_{1,i}$ variables and none of the coefficients of $G^{(i)}$ are divisible by π. We now repeat the method of contraction on $G^{(1)}$, leaving $G^{(2)}, G^{(3)}, \ldots$ untouched. We obtain a new form $H = \pi^2 H^{(2)} + \cdots$ where for each $i \geq 2$, $H^{(i)}$ has $w_{2,i}$ variables, none of the coefficients of $H^{(i)}$ is divisible by π, $w_{2,i}$ is the number of derived variables created at level i including those variables from $G^{(i)}$, and we discard any unused variables that occurred in $G^{(1)}$. We continue in this manner at each step, creating as many derived variables as possible from the bottom level form and discarding each unused variable from the bottom level form. Suppose we eventually obtain a form of the type $L = \pi^j L^{(j)} + \pi^{j+1} L^{(j+1)} + \cdots$ where $j > \frac{e}{p-1} + e\tau$. Then we set any derived variable $z = 1$ and set all other variables equal to zero. By tracing back to the ancestors of z, we find a primitive solution to the congruence $F \equiv 0 \bmod \pi^j$. By Theorem 3.1.7, F has a nontrivial zero in $\mathcal{O}$, as desired. See [18] for the original explanation of the contraction method.

We now describe quantitative results making use of these ideas. Since the solvability of the form in the residue field depends only on the coefficients modulo δ-powers, where $\delta = (d, p^f - 1)$, we can assume that all the coefficients of F in $\mathcal{O}/(\pi) \cong \mathbb{F}_q$ are one of $\delta = |\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^\delta| = |\mathbb{F}_q^\times/(\mathbb{F}_q^\times)^d|$ possible representatives, $\{b_1, \cdots, b_\delta\}$.

Two cases arise depending on whether -1 is or is not a $\delta = (d, p^f - 1)$ power in the residue field. First, suppose that -1 is not a $\delta = (d, p^f - 1)$ power in the residue field. If a_i, a_j appear as coefficients of F and $\overline{a_i} = \overline{-a_j}$ for $j \neq i$, we can form a derived variable using two variables from F. After forming as many derived variables as possible in this case, we may assume that the remaining coefficients of F are one of $\frac{\delta}{2}$ possible representatives, $\{b_1, \cdots, b_{\frac{\delta}{2}}\}$. Second, suppose that -1 is a $\delta = (d, p^f - 1)$ power in the residue field. Then $l_{\mathbb{F}_q}(d) = l_{\mathbb{F}_q}(\delta) = 2$. Thus if a_i, a_j appear as coefficients of F and $\overline{a_i} = \overline{a_j}$ for $j \neq i$, we can again form a derived variable using two variables from F. The usefulness of these observations will become more clear in the calculations and proofs of our later results.

Assume now that -1 is not a $\delta = (d, p^f - 1)$ power in the residue field. Suppose

that we can form M derived variables from M pairs of coefficients a_i, a_j of F where $\overline{a_i} = \overline{-a_j}$ for $j \neq i$. Then suppose that we can form M' additional derived variables from sets of l variables whose coefficients are equal in the residue field. Then by the Pigeonhole Principle, we have $N = 2M + lM' + R$ where $0 \leq R \leq (l-1)\frac{\delta}{2}$. Since $l \geq 2$, this gives $M + M' \geq \frac{N-R}{l} \geq \frac{N-(l-1)\frac{\delta}{2}}{l}$. Thus, $M + M' \geq \left\lceil \frac{N-(l-1)\frac{\delta}{2}}{l} \right\rceil$ and we may form at least $\left\lceil \frac{N-(l-1)\frac{\delta}{2}}{l} \right\rceil$ derived variables at the first step.

We continue similarly in the second step. With the $w_{1,1}$ variables we can create at least $\left\lceil \frac{w_{1,1}-(l-1)\frac{\delta}{2}}{l} \right\rceil$ derived variables at higher levels. Notice that a derived variable at level i costs at most l^i variables at level 0 to form.

We will also use the following observation. Let $f = ab$. By Chevalley's Theorem (Theorem 2.1.1) and the fact that $\mathbb{F}_{p^f}$ is a vector space over $\mathbb{F}_{p^b}$ of dimension a, if we have more than $a(d, p^b - 1)$ derived variables at level $\gamma - 1$, then we can find a primitive solution of $F \mod \pi^\gamma$ and thus by Theorem 3.1.7, F has a nontrivial zero in K.

Theorem 3.2.2. *Let K be an unramified extension of $\mathbb{Q}_p$ of degree $n = ab$, $a \geq b$, $p > 2$. Let $d = mp^\tau$, where $(m, p) = 1$, $\delta = (d, p^n - 1)$. Furthermore, suppose δ does not divide $\frac{p^n-1}{2}$. Then $\Delta_K(d) \leq d+1$, provided that at least one of the following bounds holds:*

1. $m\left(\frac{p}{l(\delta)}\right)^\tau \geq \frac{\delta}{2} + a(d, p^b - 1)$.
2. $d = mp^\tau \geq \frac{\delta}{2}(l(\delta)^{\tau+1} - 1)$.
3. $m\left(\frac{p}{l(\delta)}\right)^\tau \geq \frac{\delta}{2} + s(\delta) - 1$.

In particular, by (1), letting $a = n$, $b = 1$, if

$$m\left(\frac{p}{l(\delta)}\right)^\tau \geq \frac{\delta}{2} + n(d, p-1),$$

then $\Delta_K(d) \leq d + 1$.

Proof. Since K is unramified and $p > 2$, we have $e = 1$ and so $\gamma = \tau + 1$. Also, $q = p^f = p^n$. By Lemma 2.1.8, -1 is not a δ power in the residue field. Note that δ is even because δ does not divide $\frac{p^n-1}{2}$. Since $n = ab$, $\mathbb{F}_{p^n}$ is an extension of $\mathbb{F}_{p^b}$ of degree a.

We show that if we start with a form $\sum_{i=1}^{d+1} a_i x_i^d$ where $a_i \in \mathcal{O}^\times$, then through the method of contraction above we can create a derived variable at level γ or higher.

The number of discarded variables not used in creating derived variables at level $\gamma - 2 = \tau - 1$ or below to reach level $\gamma - 1 = \tau$ or above is at most

$$(l-1)\frac{\delta}{2} + (l-1)\frac{\delta}{2}l + \cdots + (l-1)\frac{\delta}{2}l^{\tau-1} = (l^\tau - 1)\frac{\delta}{2}.$$

A derived variable at level τ is created through this method of contraction from at most l^τ of the original variables. By Theorem 2.1.1, if we have more than $a(d, p^b - 1)$ derived variables at level τ, then we have a nontrivial solution in the residue field, thus creating a derived variable at level γ or above. Therefore, if $N > (l^\tau - 1)\frac{\delta}{2} + l^\tau a(d, p^b - 1)$, then either we already have a derived variable at level γ or higher or there are more than $a(d, p^b - 1)$ derived variables at level τ, and so we obtain a nontrivial zero of F over K. If the bound in (1) holds, then this gives $\Delta_K(d) \leq d + 1$ because $d + 1 > d = mp^\tau \geq l^\tau(\frac{\delta}{2} + a(d, p^b - 1)) > (l^\tau - 1)\frac{\delta}{2} + l^\tau a(d, p^b - 1)$.

The bound in (2) can be attained by just continuing the method as in the previous steps. Namely, if we have more than $(l-1)\frac{\delta}{2}$ variables at level τ, a derived variable at level γ or above can be created. Hence, the number of unused variables is at most

$$(l-1)\frac{\delta}{2} + (l-1)\frac{\delta}{2}l + \cdots + (l-1)\frac{\delta}{2}l^{\tau-1} + (l-1)\frac{\delta}{2}l^\tau = \frac{\delta}{2}(l^{\tau+1} - 1).$$

As before, if $N > \frac{\delta}{2}(l^{\tau+1} - 1)$, then a derived variable at level γ or above can be created, and so F has a nontrivial zero defined over K. Thus if

$$d + 1 > d = mp^\tau \geq \frac{\delta}{2}(l^{\tau+1} - 1),$$

then $\Delta_K(d) \leq d + 1$.

We obtain the bound in (3) by observing that if we have more than $s(\delta) - 1$ variables at level τ, then we can create a derived variable at level γ or above. If $N > (l(\delta)^\tau - 1)\frac{\delta}{2} + l(\delta)^\tau(s(\delta) - 1)$, then a derived variable at level γ or above can be created, and so F has a nontrivial zero defined over K. Thus if $d + 1 > d \geq (l(\delta)^\tau - 1)\frac{\delta}{2} + l(\delta)^\tau(s(\delta) - 1)$, then F has a nontrivial zero defined over K. In particular, if the bound in (3) holds, then $d = mp^\tau \geq ml(\delta)^\tau \geq l(\delta)^\tau\frac{\delta}{2} + l(\delta)^\tau(s(\delta) - 1) > (l(\delta)^\tau - 1)\frac{\delta}{2} + l(\delta)^\tau(s(\delta) - 1)$, and so F has a nontrivial zero defined over K. □

Lemma 3.2.3. *Let K be a unramified extension of $\mathbb{Q}_p$, $p > 2$, of degree n. Let $d = mp^\tau$, where $(m, p) = 1$, $\delta = (d, p^n - 1)$. If δ divides $\frac{p^n - 1}{2}$, then $\Delta_K(d) \leq d + 1$.*

Proof. By Lemma 2.1.8, $l = 2$ if and only if $\delta | \frac{p^n - 1}{2}$. As in the proof of Theorem 3.2.2, if we can show that

$$d = mp^\tau \geq \delta(2^{\tau+1} - 1),$$

then a nontrivial solution to $F \equiv 0 \mod p^{\tau+1}$ exists through the method of contraction. We have $m \geq \delta$ because $\delta \mid m$, and $p^\tau \geq 3^\tau \geq 2^{\tau+1} - 1$ for all odd p. Thus the inequality holds and the proof is finished. □

Lemma 3.2.4. *Let K be an unramified extension of $\mathbb{Q}_p$ of degree n, $p > 2$. Let $d = mp^\tau$, where $(m, p) = 1$, $\delta = (d, p^n - 1)$. Let $s(\delta)$ be defined as in Definition 2.1.5. If $mp^\tau \geq s(\delta)^{\tau+1} - 1$, then $\Delta_K(d) \leq d + 1$.*

Proof. We proceed as in the proof of Theorem 3.2.2, and notice that at each step we discard at most $s(\delta)-1$ variables at that level and that forming a variable at level i costs at most $s(\delta)^i$ variables from level 0. Hence, if

$$N > (s(\delta)-1)(1+s(\delta)+\cdots+s(\delta)^\tau) = s(\delta)^{\tau+1}-1,$$

then we can create a derived variable at level $\tau+1$ or higher. If $N \geq d+1 > mp^\tau \geq s(\delta)^{\tau+1}-1$, then the proof is finished. □

Lemma 3.2.5. *Let K be an unramified extension of $\mathbb{Q}_p$ of degree n, $p>2$. Let $d=mp^\tau$, where $(m,p)=1$, $\delta=(d,p^n-1)$. Suppose $\delta=(d,p-1)k$ and $k\geq 2n$. Then $\Delta_K(d)\leq d+1$.*

Proof. By Lemma 3.2.3, we may assume δ does not divide $\frac{p^n-1}{2}$. We have $\delta=(d,p-1)k\geq 2n(d,p-1)$. Thus $\delta\geq\frac{\delta}{2}+n(d,p-1)$. Since $p\geq l$ and $m\geq\delta$, this gives $m(\frac{p}{l})^\tau\geq m\geq\delta\geq\frac{\delta}{2}+n(d,p-1)$. This proves the result by Theorem 3.2.2 (1). □

Corollary 3.2.6. *Let K be an unramified extension of $\mathbb{Q}_p$ of degree n, $p>2$. Let $d=mp^\tau$, where $(m,p)=1$, $\delta=(d,p^n-1)$. If $p\geq\frac{l(\delta)^2}{2}$, then $\Delta_K(d)\leq d+1$.*

Proof. By Lemma 3.2.3, we may assume δ does not divide $\frac{p^n-1}{2}$ and hence $l>2$. Since $m\geq\delta, l>2, \tau\geq 1$, we have

$$mp^\tau \geq \delta\left(\frac{l^2}{2}\right)^\tau = \frac{\delta}{2}l^{\tau+1}\left(\frac{l}{2}\right)^{\tau-1} \geq \frac{\delta}{2}l^{\tau+1} > \frac{\delta}{2}(l^{\tau+1}-1).$$

The result follows by Theorem 3.2.2 (2). □

Theorem 3.2.7. *Let K be an unramified extension of $\mathbb{Q}_p$ of degree n with $p\geq 3$ and $\delta=(d,p^n-1)$.*

1. *If $\delta\leq p-2$, then $\Delta_K(d)\leq d+1$.*
2. *If $\delta=p-1$ and $n=2$, then $\Delta_K(d)\leq d+1$.*
3. *If $\delta=p-1$, $n\geq 3$, and $p\geq 5$, then $\Delta_K(d)\leq d+1$.*

Proof. First suppose that $\delta\leq p-2$. By Theorem 2.1.1, $s(\delta)\leq\delta+1\leq p-1$. By Lemma 3.2.4, if $mp^\tau\geq(s(\delta)-1)(1+s(\delta)+\cdots+s(\delta)^\tau)$, then $\Delta_K(d)\leq d+1$. Since $m\geq\delta\geq(s(\delta)-1)$, it suffices to show that $p^\tau\geq 1+s(\delta)+\cdots+s(\delta)^\tau$. The binomial expansion gives

$$p^\tau=(1+(p-1))^\tau\geq 1+(p-1)+(p-1)^2+\cdots+(p-1)^\tau\geq 1+s(\delta)+\cdots+s(\delta)^\tau.$$

Suppose $\delta=p-1$. If $n=2$, then δ is a divisor of $\frac{p^2-1}{2}$ and hence the result follows from Lemma 3.2.3.

Suppose that $n\geq 3$. Since $\delta<p\leq p^{\frac{n}{3}}=p^{n\frac{4-2}{2(4-1)}}$, we have $s(\delta)\leq 4$ by Lemma 2.1.7. Since $m\geq\delta=(p-1)$, and $p\geq 5$, we have $mp^\tau\geq(p-1)p^\tau\geq s(\delta)^{\tau+1}-1$. Thus the result follows by Lemma 3.2.4. □

Theorem 3.2.8. *Let K be an unramified quadratic extension of $\mathbb{Q}_p$ with $p \geq 3$. Then $\Delta_K(d) \leq d+1$.*

Proof. By Theorem 3.2.7, we may suppose $\delta \geq p+1$. Furthermore, by Lemma 3.2.3 and Lemma 3.2.5, we can suppose $\delta = (d, p-1)k$ with $k = 2, 3$. The case $k = 3$ is covered by Lemma 3.2.3 because $2|p+1$.

Suppose $\delta = 2(d, p-1)$. Since $\delta \geq p+1$, it follows that $\delta = 2(p-1)$. We can suppose δ does not divide $\frac{p^2-1}{2}$ by Lemma 3.2.3. Then each element of $\mathbb{F}_q^m = \mathbb{F}_q^\delta$ is a $\frac{p+1}{2}$ root of unity. Thus $l \leq \frac{p+1}{2}$ by Lemma 2.1.6. By Theorem 3.2.2, it is sufficient to show

$$2(p-1)\left(\frac{p}{\frac{p+1}{2}}\right)^\tau \geq 3(p-1),$$

for then we would have

$$\begin{aligned} m\left(\frac{p}{l}\right)^\tau \geq \delta\left(\frac{p}{l}\right)^\tau = 2(p-1)\left(\frac{p}{l}\right)^\tau &\geq 2(p-1)\left(\frac{p}{\frac{p+1}{2}}\right)^\tau \\ &\geq 3(p-1) = (p-1) + 2(p-1) \geq \frac{\delta}{2} + 2(d, p-1). \end{aligned}$$

Thus it is sufficient to show that

$$2\left(\frac{2p}{p+1}\right)^\tau \geq 3.$$

Since $\frac{2p}{p+1}$ is an increasing function of p, we may assume $p = 3$. Furthermore, since the bound holds for $\tau = 1$, the bound holds for all choices (p, τ) with $p \geq 3, \tau \geq 1$. □

Theorem 3.2.9. *Let K be an unramified cubic extension of $\mathbb{Q}_p$ with $p \geq 5$. Then $\Delta_K(d) \leq d+1$.*

Proof. By Lemma 3.2.5, it suffices to consider the cases $\delta = (d, p-1)k$ with $k = 1, 2, 3, 4, 5$. By Theorem 3.2.7, we may assume $k > 1$. Since $k|1+p+p^2$, $k \neq 2, 4, 5$. Thus $k = 3$. Then $\delta \mid 3(p-1)$, and so $l_{\mathbb{F}_q}(\delta) \leq l_{\mathbb{F}_q}(3(p-1)) \leq 3$, where the last inequality is proved in Theorem 2.1.11. The result now follows from Corollary 3.2.6. □

Remark. Originally, the following computations of levels via SageMath were included to prove Theorem 3.2.9:

Since

$$\mathbb{F}_{7^3} \cong \frac{\mathbb{F}_7[x]}{(x^3 + 6x^2 + 4)}$$

and

$$([4x^2 + 2x + 4])^{18} + ([3x^2 + 4x + 4])^{18} + [1] \equiv [0],$$

$l_{18} = 3$ for $\mathbb{F}_{7^3}$. Similarly, since

$$\mathbb{F}_{13^3} \cong \frac{\mathbb{F}_{13}[x]}{(x^3 + 2x + 11)}$$

and

$$([6x^2+11x+6])^{36}+([3x+7])^{36}+([7x^2+7x+5])^{36}\equiv[0],$$

$l_{36}=3$ for $\mathbb{F}_{13^3}$.

However, Theorem 2.1.11 made these computations unecessary.

Theorem 3.2.10. *Let K be an unramified extension of $\mathbb{Q}_p$ with $p\geq 5$ and $n\geq 4$. Then $\Delta_K(d)\leq d+1$.*

Proof. Let $d=mp^\tau$ where $(m,p)=1$ and let $\delta=(d,p^n-1)$. By Lemma 3.2.5, it suffices to consider $\delta<(p-1,d)2n$. By Theorem 3.2.7, it suffices to consider $m\geq\delta\geq p+1$. Hence, suppose $p+1\leq\delta\leq(d,p-1)(2n-1)$. We have $p<\delta\leq m$. Thus, by Lemma 3.2.4, it suffices to show $s(\delta)\leq p$.

By Lemma 2.1.3, it suffices to show that

$$\delta\leq(d,p-1)(2n-1)\leq(p-1)(2n-1)\leq p^{n\cdot\frac{p-2}{2(p-1)}}+1.$$

We will succeed for $p\geq 11$ and $n\geq 4$, $p=7$ and $n\geq 5$, and $p=5$ and $n\geq 7$. Separate arguments are needed for the remaining cases.

First assume that $n=4$. We will show that $7(p-1)\leq p^{\frac{2(p-2)}{p-1}}+1$ for $p\geq 11$. This is equivalent to showing that $7\leq p^{\frac{p-3}{p-1}}+\frac{8}{p}$. For $p\geq 13$, we have

$$7\leq 13^{\frac{5}{6}}\leq p^{\frac{p-3}{p-1}}<p^{\frac{p-3}{p-1}}+\frac{8}{p}.$$

For $p=11$, we have

$$7<11^{\frac{8}{10}}+\frac{8}{11}.$$

This proves the inequality for $n=4$ and $p\geq 11$. Now assume that $n\geq 4$. We consider n as a real variable and take the derivative of both sides with respect to n. It is sufficient to show that

$$p^{n\cdot\frac{p-2}{2(p-1)}}\frac{p-2}{2(p-1)}\ln(p)\geq 2(p-1)$$

for $p\geq 11$ and $n\geq 4$. First observe that for $p\geq 11$,

$$p^{\frac{p-3}{p-1}}\geq p^{\frac{8}{10}}\geq 11^{\frac{8}{10}}>\frac{4\cdot 10}{9}\geq\frac{4(p-1)}{p-2}.$$

Then for $n\geq 4$ we have

$$\begin{aligned}p^{n\cdot\frac{p-2}{2(p-1)}}\frac{p-2}{2(p-1)}\ln(p)&>p^{\frac{2(p-2)}{p-1}}\frac{p-2}{2(p-1)}=p^{\frac{p-3}{p-1}+1}\frac{p-2}{2(p-1)}\\&>\frac{4p(p-1)}{p-2}\frac{p-2}{2(p-1)}=2p>2(p-1).\end{aligned}$$

This finishes the proof for $p\geq 11$ and $n\geq 4$.

Now assume that $p = 7$ and $n \geq 5$. For $p = 7$ and $n = 5$ we have

$$(p-1)(2n-1) = 54 < 7^{\frac{25}{12}} = p^{n \cdot \frac{p-2}{2(p-1)}} < p^{n \cdot \frac{p-2}{2(p-1)}} + 1.$$

For $p = 7$ and $n \geq 5$, we apply the derivative criterion above to see that

$$7^{n \cdot \frac{5}{12}} \frac{5}{12} \ln(7) > 7^{\frac{25}{12}} \frac{5}{12} > 12 = 2(7-1).$$

This finishes the proof for $p = 7$ and $n \geq 5$.

Now assume that $p = 5$ and $n \geq 7$. For $p = 5$ and $n = 7$ we have

$$(p-1)(2n-1) = 52 < 5^{\frac{21}{8}} = p^{n \cdot \frac{p-2}{2(p-1)}} < p^{n \cdot \frac{p-2}{2(p-1)}} + 1.$$

For $p = 5$ and $n \geq 7$, we apply the derivative criterion above to see that

$$5^{n \cdot \frac{3}{8}} \frac{3}{8} \ln(5) > 5^{\frac{21}{8}} \frac{3}{8} > 8 = 2(5-1).$$

We now consider the remaining cases. Namely, $p = 7$ and $n = 4$, and $p = 5$ and $n = 4, 5, 6$.

Suppose that $p = 7$ and $n = 4$. Since $7^4 - 1 = 32 \cdot 75$, we may assume that $32 \mid \delta$ by Lemma 3.2.3. Let $\delta = (d, 7-1)k$. Then $16 \mid k$, and thus $k \geq 16 > 2 \cdot 4$. The result follows from Lemma 3.2.5.

Now assume that $p = 5$, $n \in \{4, 5, 6\}$, and $\delta = (d, 4)k$.

For $n = 4$, $5^4 - 1 = 16 \cdot 3 \cdot 13$. By Lemma 3.2.3, we may assume $\delta = 16 \cdot j$. If $j \geq 3$, then $k \geq 12 > 2 \cdot 4$, so the result holds by Lemma 3.2.5. If $j = 1$, then $l_\delta = 3$ by Lemma 2.1.6, and the result holds by Corollary 3.2.6.

For $n = 5$, $5^5 - 1 = 2^2 \cdot 11 \cdot 71$. By Lemma 3.2.3, we may assume $\delta = 4 \cdot j$. If $j \geq 11$, then $k \geq 11 > 2 \cdot 5$, so the result holds by Lemma 3.2.5. If $j = 1$, then the result holds by Theorem 3.2.7.

For $n = 6$, $5^6 - 1 = 7 \cdot 8 \cdot 9 \cdot 31$. By Lemma 3.2.3, we can assume $\delta = 8 \cdot j$. If $j < 9$, then $l_\delta = 3$ by Lemma 2.1.6, and the result holds by Corollary 3.2.6. If $j \geq 9$, then $k \geq 18 > 2 \cdot 6$, so the result holds by Lemma 3.2.5. □

We now treat the unramified extensions of $\mathbb{Q}_p$ of degree n in the case $p = 3$. Let $d = m \cdot 3^\tau$ where $(m, 3) = 1$ and $\delta = (d, 3^n - 1)$. By Lemma 3.2.5, we may assume that $\delta < (d, 2)2n$. If d is odd, then $\Delta_K(d) \leq d + 1$ by Lemma 3.2.3. From now on, we always assume that $2 \mid d$.

Proposition 3.2.11. *Let K be an unramified extension of $\mathbb{Q}_3$ of degree n with $d = m \cdot 3^\tau$, $(m, 3) = 1$, and $\delta = (d, 3^n - 1) = 2$. Then $\Delta_K(d) \leq d + 1$, unless (possibly) $m = 2$ and n is odd.*

Proof. By Theorem 2.1.1, $s(2) \leq 3$. If $m \geq 4$, the result holds by Lemma 3.2.4. If $m = 2$ and n is even, the result holds by Lemma 3.2.3, since $3^n - 1 \equiv 0 \mod 4$. □

Theorem 3.2.12. *Let K be an unramified extension of $\mathbb{Q}_3$ of degree $n \geq 2$ with $d = m \cdot 3^\tau$, $(m, 3) = 1$, and $\delta = (d, 3^n - 1)$. Then $\Delta_K(d) \leq d + 1$, unless (possibly) $m = 2$ and n is odd.*

Proof. We can assume that δ is even by Lemma 3.2.3. Since δ is even, by Lemmas 3.2.5 and 3.2.11, it suffices to show the result for $4 \leq \delta \leq 4n-2$. Let $3^n - 1 = 2^h j$ where j is odd. By Lemma 3.2.3, we can assume that $\delta = 2^h j'$ where $j' \mid j$. If n is even, then $8 \mid 3^n - 1$ and so $h \geq 3$. Thus $8 \mid \delta$ and so $\delta \geq 8$. If n is odd, then $h = 1$. The case $\delta = 2$ is already covered, and $\delta \neq 6$ because $6 \nmid 3^n - 1$. Thus $\delta \geq 10$ when n is odd. Hence we can assume that $\delta \geq 8$ in all cases.

First we consider the cases when $n \geq 10$. We now show that $4n - 2 \leq 3^{\frac{n}{3}}$ for all $n \geq 10$. The result holds for $n = 10$ because $38 < 3^{\frac{10}{3}}$. The result holds for $n \geq 10$ because $\frac{d}{dn}(3^{\frac{n}{3}}) = \frac{1}{3}3^{\frac{n}{3}}\ln(3) = 3^{\frac{n}{3}-1}\ln(3) > 3^{\frac{7}{3}} > 4$. Since $\delta \geq 8$ and $n \geq 10$, we have

$$\delta \leq 4n - 2 \leq 3^{\frac{n}{3}} = 3^{n\frac{4-2}{2(4-1)}} \leq 3^{n\frac{\delta/2-2}{2(\delta/2-1)}}.$$

Thus $s(\delta) \leq \frac{\delta}{2}$ by Lemma 2.1.7. We can finish the proof when $n \geq 10$ by applying Theorem 3.2.2 (3) because $m \geq \delta > \frac{\delta}{2} + s(\delta) - 1$.

The case $n = 2$ holds by Theorem 3.2.8. The cases $3 \leq n \leq 9$ must be dealt with individually. We will consider each δ satisfying $4 \leq \delta \leq 4n - 2$ and the other conditions above. Note that by Lemma 2.1.7, if $\delta \leq p^{\frac{n}{4}} + 1$, then $s(\delta) \leq 3$, and so we can finish by using Lemma 3.2.4. Also note that if $s(\delta) \leq \frac{\delta}{2}$, then we can finish by applying Theorem 3.2.2 (3), as above.

$n = 9$: $3^9 - 1 = 2 \cdot 13 \cdot 757$. Since $4 \leq \delta \leq 34$, we have $\delta = 26$. By Lemma 2.1.7, since $26 < 3^{9 \cdot \frac{4-2}{2(4-1)}} = 3^3$, we have $s(\delta) \leq 4$. We finish the proof by applying Theorem 3.2.2 (3) because $s(\delta) \leq \frac{\delta}{2}$.

$n = 8$: $3^8 - 1 = 32 \cdot 5 \cdot 41$. We have $\delta \leq 30$ and $32 \mid \delta$, a contradiction.

$n = 7$: $3^7 - 1 = 2 \cdot 1093$. Since $\delta \leq 26$, we have $\delta = 2$, an already covered case.

$n = 6$: $3^6 - 1 = 8 \cdot 7 \cdot 13$. Since $\delta \leq 22$, we have $\delta = 8$. By Lemma 2.1.7, since $8 < 3^{6 \cdot \frac{4-2}{2(4-1)}} = 3^2$, we have $s(\delta) \leq 4$. We finish by applying Theorem 3.2.2 (3) because $s(\delta) \leq \frac{\delta}{2}$.

$n = 5$: $3^5 - 1 = 2 \cdot 11^2$. Since $\delta \leq 18$, we have $\delta = 2$, an already covered case.

$n = 4$: $3^4 - 1 = 16 \cdot 5$. Then $\delta \leq 14$ and $16 \mid \delta$, a contradiction.

$n = 3$: $3^3 - 1 = 2 \cdot 13$. Then $\delta \leq 10$, so $\delta = 2$, an already covered case.

□

3.3 $\Gamma_K(2 \cdot 3^\tau)$ for $[K : \mathbb{Q}_3] \equiv 1 \mod 2$

We now outline how one can show $\Gamma_K(2 \cdot 3^\tau) \leq (2 \cdot 3^\tau)^2 + 1$ in the case that K is an odd degree unramified extension of $\mathbb{Q}_3$. We first recall a standard result in quadratic form theory over finite fields of characteristic not equal to 2.

Lemma 3.3.1 (Lemma 1,[11]). *The nonsingular zeros of a quadratic form $q \in k[x_1, \cdots, x_s]$ where char$(k) \neq 2$ cannot all lie in a proper linear subspace.*

Corollary 3.3.2. *A ternary quadratic form*

$$F = a_1x_1^2 + a_2x_2^2 + a_3x_2^2$$

where $a_i \in (\mathbb{F}_{3^n})^\times$ *for* $i = 1, 2, 3$ *has a zero with* $x_1 \neq 0$.

Proof. By Theorem 2.1.1, F has a nontrivial zero, and since F is diagonalized, it is nonsingular. By Lemma 3.3.1, there exists a zero that does not lie in the hyperplane $x_1 = 0$. □

Remark. Corollary 3.3.2 is the analog of [18, Lemma 1], which fails in general for nontrivial extensions of $\mathbb{F}_p$.

[18, Lemma 3] still holds for unramified extensions of $\mathbb{Q}_p$. We now use the original method of contraction of [18], noticing that the case $d = 2 \cdot 3^\tau$ over K where K is an unramified extension of $\mathbb{Q}_3$, reduces to quadratic forms in the residue field. Hence, we can apply the analogous method of contraction using 3 variables at a time. The same proof for [18, Lemma 5] now works.

3.4 Examples of $\Delta_K(d) > d + 1$.

It is natural to ask whether $\Delta_K(d) \leq d + 1$ for all unramified extensions K of $\mathbb{Q}_p$. However, we will see in this section that this is not the case.

Lemma 3.4.1. *Let* K *be an unramified extension of* $\mathbb{Q}_p$, *and let* $\mathcal{O}_K$ *be the ring of integers in* K. *If* $a, b \in \mathcal{O}_K$ *and* $a \equiv b \mod p$, *then* $a^{p^i} \equiv b^{p^i} \mod p^{i+1}$ *for* $i \geq 1$.

Proof. An immediate consequence of the Binomial Theorem.

□

Proposition 3.4.2. *Let* $K = \mathbb{Q}_p$, *and let* $d = mp^\tau$ *with* $(m, p) = 1$, $\tau \geq 1$, *and* $\delta = (d, p - 1)$. *Then the following statements hold.*

1. *For* $p = 2$, *we have*

   $$\Delta_{\mathbb{Q}_2}(d) = 5 \text{ for } (\tau, m) = (1, 1),$$
   $$\Delta_{\mathbb{Q}_2}(d) = 2^{\tau+2} \text{ for } (\tau, m) \neq (1, 1).$$

   Thus,

   $$\Delta_{\mathbb{Q}_2}(d) > d + 1 \text{ for } m = 1, 3,$$
   $$\Delta_{\mathbb{Q}_2}(d) \leq d + 1 \text{ for } m \geq 5.$$

2. *Assume that* $p \geq 3$. *If* $m \neq p - 1$, *then* $\Delta_{\mathbb{Q}_p}(d) \leq d + 1$.

3. *Assume that* $p \geq 3$ *and* $m = (p - 1)k$, $k \geq 1$. *Then* $\Delta_{\mathbb{Q}_p}(d) = p^{\tau+1}$. *Thus,* $\Delta_{\mathbb{Q}_p}(d) > d + 1$ *if* $k = 1$.

Proof. (1) Let $p = 2$. For $\tau = 1$, $m = 1$, the quadratic form $\sum_{i=1}^{4} x_i^2 \bmod 8$ has no primitive zero and hence no nontrivial zero over $\mathbb{Q}_2$. The form $\sum_{i=1}^{5} a_i x_i^2$ does have a nontrivial zero over $\mathbb{Q}_2$ by a classical result of Hasse (see [39, Chapter 6]). Thus $\Delta_{\mathbb{Q}_2}(2) = 5$.

Let $\tau = 1$, $m \geq 3$. Then $x_i^d \equiv 0, 1 \bmod 8$. Thus $\sum_{i=1}^{7} x_i^d \equiv 0 \bmod 8$ has no primitive solution and thus no nontrivial zero over $\mathbb{Q}_2$. However, $\sum_{i=1}^{8} a_i x_i^d \equiv 0 \bmod 8$ with $a_i \in \mathbb{Z}_2^\times$ has a primitive solution because $D(\mathbb{Z}/8\mathbb{Z}) = 8$. Thus $\sum_{i=1}^{8} a_i x_i^d$ has a nontrivial zero over $\mathbb{Q}_2$ by Hensel's Lemma. In conclusion, $\Delta_{\mathbb{Q}_2}(d) = 2^{\tau+2}$ for $\tau = 1$, $m \geq 3$.

Now assume that $\tau \geq 2$. If $x_i \equiv 0 \mod 2$, then $x_i^{m \cdot 2^\tau} \equiv 0 \mod 2^{\tau+2}$, since for $\tau \geq 2$ we have $2^\tau \geq \tau + 2$. If $x_i \not\equiv 0 \mod 2$, then $x_i^{m \cdot 2^\tau} \equiv 1 \mod 2^{\tau+2}$ by Lemma 3.4.1 and since the result holds for $\tau = 1$. Hence, $\sum_{i=1}^{2^{\tau+2}-1} x_i^{m \cdot 2^\tau} \equiv 0 \mod 2^{\tau+2}$ has no primitive zero and thus no nontrivial zero over $\mathbb{Q}_2$. Furthermore,

$$\sum_{i=1}^{2^{\tau+2}} a_i x_i^{m \cdot 2^\tau} \equiv 0 \mod 2^{\tau+2}$$

with $a_i \in \mathbb{Z}_2^\times$ has a primitive zero because $D(\mathbb{Z}/2^{\tau+2}\mathbb{Z}) = 2^{\tau+2}$, and thus there is a nontrivial zero in $\mathbb{Q}_2$ by Hensel's Lemma. Therefore, $\Delta_{\mathbb{Q}_2}(d) = 2^{\tau+2}$ for $\tau \geq 2$.

If $m \geq 5$, then $\Delta_{\mathbb{Q}_2}(d) = 2^{\tau+2} = 4 \cdot 2^\tau < m \cdot 2^\tau = d < d + 1$. If $m = 1, 3$ and $(\tau, m) \neq (1, 1)$, then $\Delta_{\mathbb{Q}_2}(d) = 2^{\tau+2} = 4 \cdot 2^\tau > m \cdot 2^\tau + 2 > d + 1$. If $(\tau, m) = (1, 1)$, then $\Delta_{\mathbb{Q}_2}(d) = 5 > 2 + 1$.

(2) Assume that $p \geq 3$. If $\delta \leq p - 2$, then $\Delta_{\mathbb{Q}_p}(d) \leq d + 1$ by Theorem 3.2.7. If $\delta = p - 1$ and $d \neq (p-1)p^\tau$, then $m \geq 2(p-1) > p$. Since $s(\delta) \leq p$ by Theorem 2.1.1, we have $m \cdot p^\tau > p^{\tau+1} - 1 \geq s(\delta)^{\tau+1} - 1$, and the result holds by Lemma 3.2.4.

(3) Assume that $m = (p-1) \cdot k$ where $k \geq 1$. If $x \not\equiv 0 \bmod p$, then $x^m \equiv 1 \bmod p$. By Lemma 3.4.1, we have $x^{m \cdot p^\tau} \equiv 1 \bmod p^{\tau+1}$. If $x \equiv 0 \mod p$, then $x^{m \cdot p^\tau} \equiv 0 \mod p^{\tau+1}$ because $p^\tau \geq \tau + 1$ for $p \geq 3$. Then the congruence

$$\sum_{i=1}^{p^{\tau+1}-1} x_i^{m \cdot p^\tau} \equiv 0 \bmod p^{\tau+1}$$

has no primitive solution and thus no nontrivial zero over $\mathbb{Q}_p$. However, the congruence

$$\sum_{i=1}^{p^{\tau+1}} a_i x_i^{m \cdot p^\tau} \equiv 0 \bmod p^{\tau+1}$$

with $a_i \in \mathbb{Z}_p^\times$ has a primitive solution because $D(\mathbb{Z}/p^{\tau+1}\mathbb{Z}) = p^{\tau+1}$. Thus there is a nontrivial zero over $\mathbb{Q}_p$ by Hensel's Lemma. Therefore, $\Delta_{\mathbb{Q}_p}(d) = p^{\tau+1}$ for $\tau \geq 1$.

If $k \geq 2$, then $p^{\tau+1} < 2(p-1)p^\tau \leq m \cdot p^\tau = d < d+1$. Thus $\Delta_{\mathbb{Q}_p}(d) \leq d+1$. If $k = 1$, then $\Delta_{\mathbb{Q}_p}(d) = p^{\tau+1} > (p-1)p^\tau + 1 = d+1$. □

Originally, the author had the statement that $\Delta_{\mathbb{Q}_2}(2) = 5$ and Leep generalized it to an arbitrary 2-adic field. The following is his proof:

Proposition 3.4.3. *Let K be any finite extension of $\mathbb{Q}_2$. Then $\Delta_K(2) = 5$.*

Proof. Let $U = \mathcal{O}^\times$, the group of units of $\mathcal{O}$. Thus $U = \{\alpha \in K^\times \mid v_\pi(\alpha) = 0\}$. Let $D_K(f)$ denote the elements of $K^\times$ represented by a quadratic form f defined over K. It is sufficient to show that there exists an anisotropic quadratic form $\langle a_1, a_2, a_3, a_4\rangle = \sum_{i=1}^4 a_i x_i^2$ where $a_i \in \mathcal{O}_K^\times$. We will use the following results from [39, Chapter 6].

Lemma 3.4.4. *Let K be a finite extension of $\mathbb{Q}_2$.*

1. $|K^\times/(K^\times)^2| \geq 8$
2. *The Hilbert symbol on K is non-degenerate.*
3. *Let $\alpha \in K^\times$, $\alpha \notin (K^\times)^2$. Then*
$$|D_K(\langle 1, -\alpha\rangle)/(K^\times)^2| = \frac{1}{2}|K^\times/(K^\times)^2| \geq 4.$$
4. *Let $\alpha, \beta \in K^\times$. Then $D_K(\langle 1, -\alpha\rangle) = D_K(\langle 1, -\beta\rangle)$ if and only if $\alpha\beta \in (K^\times)^2$.*

Note that (3) and (4) follow easily from (1), (2), and the definition of the Hilbert symbol on K.

Lemma 3.4.5. *There exists a non-square unit $u \in U$ such that $D_K(\langle 1, -u\rangle) \neq U$.*

Proof. There exists exactly one subgroup of index 2 in $K^\times/(K^\times)^2$ containing no element having odd valuation. That unique subgroup is U/U^2. (Note that U/U^2 injects into $K^\times/(K^\times)^2$ because $U \cap (K^\times)^2 = U^2$.) Since $[U : U^2] = \frac{1}{2}[K^\times : (K^\times)^2] \geq 4$, there are two units $u, v \in U$ such that u, v, uv are each non-squares. The subgroups $D_K(\langle 1, -u\rangle)$ and $D_K(\langle 1, -uv\rangle)$ have index 2 in $K^\times/(K^\times)^2$ by Lemma 3.4.4(3) because u, uv are non-squares. We have $D_K(\langle 1, -u\rangle) \neq D_K(\langle 1, -uv\rangle)$ by Lemma 3.4.4(4) because v is a non-square. Therefore, either $D_K(\langle 1, -u\rangle)$ or $D_K(\langle 1, -uv\rangle)$ does not equal U. □

We now finish the proof of Proposition 3.4.3. By Lemma 3.4.5, there exist non-square units $u, v \in U$ such that $v \notin D_K(\langle 1, -u\rangle)$. Then $\langle 1, -u, -v\rangle$ is anisotropic over K and thus $\langle 1, -u, -v, uv\rangle$ is anisotropic over K, which completes the proof. □

Remark. If $[K : \mathbb{Q}_2]$ is odd, then $\langle 1, 1, 1, 1\rangle$ is anisotropic over K by Springer's Theorem because $\langle 1, 1, 1, 1\rangle$ is anisotropic over $\mathbb{Q}_2$. Thus we could use $\langle a_1, a_2, a_3, a_4\rangle = \langle 1, 1, 1, 1\rangle$ when $[K : \mathbb{Q}_2]$ is odd.

Corollary 3.4.6. *Let K be a p-adic field with ramification degree e and inertia degree f. Let $d = mp^\tau$ where $(m, p) = 1$ and $\tau \geq 1$. Suppose $-1 \in K^d$. Then $\Delta_K(d) \leq d+1$, provided that*

$$2^{mp^\tau+1} \geq p^{ef\tau+f\left(\lfloor \frac{e}{p-1} \rfloor+1\right)} + 1.$$

Proof. Notice $\mid \mathcal{O}/(\pi^\gamma) \mid = p^{ef\tau+f\left(\lfloor \frac{e}{p-1} \rfloor+1\right)}$. This is easy to see by using the unique π-adic expansion of elements in $\mathcal{O}$.

Consider a form

$$\sum_{i=1}^{d+1} a_i x_i^d$$

where the $a_i \in \mathcal{O}^\times$. By Lemma 3.1.9, to find a nontrivial solution in K it suffices to find a primitive solution to

$$\sum_{i=1}^{d+1} a_i x_i^d \equiv 0 \mod \pi^\gamma.$$

Since $-1 \in K^d$ and, in particular, $-1 \in (\mathcal{O}/(\pi^\gamma))^d$, such a solution exists if $d+1 \geq D_\pm(\mathcal{O}/(\pi^\gamma))$. By Proposition 2.2.6, if $2^{d+1} \geq \mid (\mathcal{O}/(\pi^\gamma)) \mid +1$, then $d+1 \geq D_\pm(\mathcal{O}/(\pi^\gamma))$. Since $d = mp^\tau$ and $\mid \mathcal{O}/(\pi^\gamma) \mid = p^{ef\tau+f\left(\lfloor \frac{e}{p-1} \rfloor+1\right)}$, the statement immediately follows.

□

Part II

Group Theory

Chapter 4 The Chermak-Delgado measure of a finite group

4.1 Notation and standard facts about finite groups

> *"The universe is an enormous direct product of representations of symmetry groups."* Steven Weinberg.

We first remark that this portion of the dissertation is independent of Part I. In this section, we compute the Chermak-Delgado lattice for all p-groups of order p^3, p^4 and p-groups of order p^5 as long as the nilpotency class is not 3 (Theorem 4.5.22). We also compute the Chermak-Delgado lattice for extraspecial groups (Theorem 4.3.4) and the dihedral groups (Theorem 4.4.1).

As in the previous part of this dissertation, we have no desire nor hope of being complete with our treatment of finite groups. Such a treatise would (probably) be larger than any book ever written. However, the author refers the reader to his favorite book (granted, from limited experience and exposure) in the subject, [35].

For us, unless we explicitly state to the contrary, $(G, \cdot)$ will always denote a finite group. We will simply denote $(G, \cdot)$ as G.

Since group multiplication is associative, we are at no risk of ambiguity by writing $g \cdot h \cdot l$ for $(g \cdot h) \cdot l = g \cdot (h \cdot l)$. Furthermore, since the binary operation $\cdot$ is understood from context, we will denote $g \cdot h$ by gh.

By $X \subseteq G$ we mean the usual subset inclusion. By $H \leq G$ we mean that H is a subgroup of G.

Let $n \in \mathbb{N}$. Then C_n denotes the cyclic group of order n.

Let $H, K \leq G$ be subgroups. The join of H and K, written $\langle H, K \rangle$, is the smallest subgroup of G such that $H, K \leq \langle H, K \rangle$. A collection of subgroups of G that is closed under intersections and joins is called a lattice.

For a subset $X \subseteq G$, $C_G(X) := \{g \in G | xg = gx \text{ for all } x \in X\}$. We write $C_G(G) = Z(G)$. $Z(G)$ is called the center of the group. Notice a group G is abelian if and only if $Z(G) = G$. For $H \leq G$, let $H^\star := C_G(H)$.

Let p be a prime. A finite group P is a p-group if every element of P has order a power of p. Equivalently, $|P| = p^m$ for some $m \in \mathbb{N}$.

Let G be a finite group. Then G' is the commutator subgroup, or derived subgroup, of G. That is, $G' = \langle [g, h] | g, h \in G \rangle$ where $[g, h] = g^{-1}h^{-1}gh$.

$\Phi(G)$ will denote the intersection of the proper maximal subgroups of G. It is called the *Frattini* subgroup of G.

For a finite p-group P, one readily checks that $P/\Phi(P)$ is elementary abelian and thus isomorphic to an r-dimensional $\mathbb{F}_p$-vector space $\mathbb{F}_p^r$ for some $r \in \mathbb{N}$. We call this r the Frattini rank of P. Notice that since $P/\Phi(P)$ is elementary abelian (and, in particular, abelian), $P' \leq \Phi(P)$.

Definition 4.1.1. Let G be a group. Define $\gamma_1(G) = G$ and $\gamma_i(G) = [\gamma_{i-1}(G), G]$. The series $\{\gamma_i(G)\}_i$ is called the lower central series of G. If $\gamma_r(G) = \{e\}$ for some r, then G is said to be nilpotent. If G is nilpotent, let m be the smallest integer such

that $\gamma_m(G) = \{e\}$. We say G has nilpotency class $m-1$. If G is nilpotent, we will sometimes use $\text{nil}(G)$ to denote the nilpotency class of G.

A few things are readily verified:

1. If $|G| = p^n$, then G is nilpotent with nilpotency class less than or equal to $n-1$. In the case G has nilpotency class $n-1$, we say G has maximal class.

2. G has nilpotency class 1 if and only if G is abelian.

The following theorem will also be important. See, for example, [35, Problem 4.A.6].

Theorem 4.1.2. [35, Problem 4.A.6] *Let P be a p-group having maximal class, and let N be a normal subgroup of P with index greater or equal to p^2. Then N is a term of the lower central series of P.*

We remind the reader that if G is nonabelian, then $G/Z(G)$ cannot be cyclic. In particular, a finite group cannot have a center of index p.

We also have that if $G/\Phi(G)$ is cyclic, then G is cyclic. In particular, if $|G| = p^n$ and G is nonabelian, then $|G : \Phi(G)| \geq p^2$.

4.2 Some facts about the Chermak-Delgado lattice of a finite group

As usual, G denotes a finite group and P denotes a finite p-group. Recall the following definition and notations:

Definition 4.2.1. For $H \leq G$, define the Chermak-Delgado measure of H to be the integer $m_G(H) := |H||C_G(H)|$. The integer $M_G = \max\{m_G(H)|H \leq G\}$ will be called the CD-number of G. Let $\text{CD}(G)$ be the collection of subgroups H of G such that

$$m_G(H) = M_G.$$

For $H \leq G$, let $H^\star := C_G(H)$.

Lemma 4.2.2. [35, Lemma 1.42, Lemma 1.43] *Let $H \leq G$. Then $m_G(H) \leq m_G(H^\star)$ and if equality holds, then $H = H^{\star\star}$. If $H, K \leq G$, then*

$$m_G(H)m_g(K) \leq m_G(H \cap K)m_G(\langle H, K\rangle).$$

Theorem 4.2.3. [35, Theorem 1.44] *Given a finite group G, let $CD(G)$ be the collection of subgroups H of G such that*

$$m_G(H) = M_G.$$

Then, the following hold:

1. *$CD(G)$ is a lattice under inclusion (closed under joins and intersections).*

2. *If $H, K \in CD(G)$, then $\langle H, K\rangle = HK$. In particular, if $H, K \in CD(G)$ then $HK \leq G$ and $HK \in CD(G)$.*

3. *If $H \in CD(G)$, then $H^\star \in CD(G)$ and $H^{\star\star} = H$.*

4. *The minimal element K of $CD(G)$ is abelian and $Z(G) \leq K$.*

Definition 4.2.4. Let G be a finite group, and let $\mathrm{CD}(G)$ be defined as in Theorem 4.2.3. Then $\mathrm{CD}(G)$ is called the Chermak-Delgado lattice of G.

Lemma 4.2.5. *$CD(G) = \{G\}$ if and only if G is an abelian group.*

Proof. Let $H \leq G$. Then

$$|H||H^*| \leq |G|^2.$$

Since

$$|H| \leq |G|$$

and

$$|H^*| \leq |G|,$$

equality holds if and only if $|H| = |G|$ and $|H^*| = |G|$, and both these equalities hold if and only if $G = Z(G) = H$. But, of course, $Z(G) = G$ if and only if G is abelian. □

Corollary 4.2.6. *$CD(G)$ is isomorphic to a sublattice of the subgroup lattice for $G/Z(G)$.*

Proof. If $H \in \mathrm{CD}(G)$, then $Z(G) \leq H$ by Theorem 4.2.3. Thus, every subgroup contained in $\mathrm{CD}(G)$ contains the center $Z(G)$. The result follows immediately by the Correspondence Theorem of Subgroups. □

In particular, for a nonabelian group G, for the computation of $\mathrm{CD}(G)$ we only concern ourselves with subgroups H such that $Z(G) \leq H \leq G$.

Definition 4.2.7. Let G be a finite group. By a *dot* of order n in CD(G) we mean a subgroup $H \leq G$ of order n such that $m_G(H) = M_G = \max\{m_G(S) | S \leq G\}$.

We will use the following lemmas repeatedly.

Lemma 4.2.8. *Let P be a nonabelian p-group of order p^n. Then $M_P \leq p^{2n-2}$.*

Proof. Since P is nonabelian, $m_P(Z(P)) = m_P(P) \leq p^{2n-2}$. For any nontrivial subgroup H not contained in the center, $H^\star$ is strictly contained in P. Hence, $m_P(H) \leq p^{n-1} \cdot p^{n-1} = p^{2n-2}$. Now, notice $\sup\{m_P(T) | T \leq Z(P)\} = m_P(Z(P)) \leq p^{2n-2}$. □

Lemma 4.2.9. *Let G be a group. If Q is a subgroup of $Q^\star$ and $Q^\star/Q$ is cyclic, then $Q^\star$ is abelian.*

Proof. If Q is a subgroup of $Q^\star$, then $Q \leq Z(Q^\star)$. Suppose $Q^\star/Q$ is cyclic, and let zQ be a generator. Then every element of $Q^\star$ can be written in the form $z^m q$ where $q \in Q$, $m \in \mathbb{N}$. It is now straightforward to check that any two elements of this form commute.

□

Lemma 4.2.10. *Let $H \leq G$. Then $m_G(H) = m_G(H^g)$.*

Proof. Since $|H| = |H^g|$, it suffices to notice that $C_G(H^g) = C_G(H)^g$.

□

4.3 The Chermak-Delgado lattice of extraspecial groups

Definition 4.3.1. Let P be a nonabelian p-group such that $Z(P) = \Phi(P) = P'$ where $\Phi(P)$ is the Frattini subgroup of P. Then P is a *special* p-group. If P is a special group with $|Z(P)| = p$, then P is called extraspecial.

We first recall a few standard linear algebra facts and definitions.

Definition 4.3.2. Let V be a k-vector space. A map $\beta : V \times V \to k$ is a symplectic form if it is a bilinear form and

- β satisfies $\beta(v, v) = 0$ for all $v \in V$.
- β is non-degenerate.

A pair (V, β) is called a symplectic space if V is a k-vector space and β is a symplectic form on V.

Now, let (V, β) be a symplectic space and let U be a subspace of V. Then

$$U^\perp = \{v \in V | \beta(v, u) = 0 \text{ for all } u \in U\}.$$

Symplectic spaces have been widely studied. The following can be found in many textbooks. For example, see [29, Proposition 2.4].

Lemma 4.3.3. *Let (V, β) be a symplectic space and let $U \subseteq V$ be a subspace. Then*

$$\dim U + \dim U^\perp = \dim V.$$

Theorem 4.3.4. *Let P be a finite extraspecial group of order p^{2n+1}. Then $CD(P)$ is isomorphic to the subspace lattice of $\mathbb{F}_p^{2n}$.*

Proof. It is well known that $(P/Z(P), [\cdot, \cdot])$ is a symplectic space (see, for example, [59, Section 3.10.2]). Now, let W be any subgroup of P containing $Z(P)$ and let $\overline{W}$ be the image of W under the canonical projection to the quotient $P/Z(P)$. Let $\dim_{\mathbb{F}_p}(\overline{W}) = j$. Notice that $g \in C_P(W)$ if and only if $[g, W] = e$. Thus $C_P(W)$ is precisely the subgroup corresponding to $\overline{W}^\perp$ under the Correspondence Theorem. By Lemma 4.3.3, $\dim(\overline{W}^\perp) = 2n - j$, and thus $|C_P(W)| = p^{2n-j} \cdot p = p^{2n-j+1}$ and we have

$m_P(W) = |C_P(W)||W| = p^{2n-j+1} \cdot p^{j+1} = p^{2n+2}$. Thus, every subgroup containing the center has Chermak-Delgado measure p^{2n+2}. Since W was an arbitrary subgroup of P containing $Z(P)$, and since $\mathrm{CD}(P)$ is isomorphic to a sublattice of the subgroup lattice of $P/Z(P)$, the result is now immediate by the Correspondence Theorem.

□

4.4 The Chermak-Delgado lattice of the dihedral groups

Theorem 4.4.1. *Let G be a dihedral group. Then*

1. *If*
$$G = D_{2n} = \langle a, b | a^n = b^2 = e, bab = a^{-1} \rangle$$
with $n \geq 3$, $n \neq 4$, then $CD(G) = \{\langle a \rangle\}$.

2. *If*
$$G = D_{2\cdot 4} = \langle a, b | a^4 = b^2 = e, bab = a^{-1} \rangle,$$
then $CD(G)$ is isomorphic to the subspace lattice of $\mathbb{F}_2^2$.

Proof. Assume $n \geq 3$ and n is odd. Since $n \equiv 1 \mod 2$, $Z(G) = \{e\}$. Let $A = \langle a \rangle$. Since $b \notin C_G(A)$ and A is cyclic, it follows that $C_G(A) = A$. Thus $m_G(A) = |A|^2 = n^2$. Let K be any subgroup $\{e\} = Z(G) < K < G$ of order not equal to n. By Lagrange's Theorem, $|K| \leq \frac{2n}{3}$. Since $|K| \neq Z(G)$, $C_G(K) < G$ and thus $|C_G(K)| \leq n$. Thus $m_G(K) \leq n \cdot \frac{2n}{3} < n^2 = m_G(A)$, and so $K \notin \mathrm{CD}(G)$. Notice that $m_G(G) = 2n = m_G(Z(G))$. Since $m_G(G) = 2n < n^2 = m_G(A)$ for $n \geq 3$, it follows that $G \notin \mathrm{CD}(G)$. From the fact that $\mathrm{CD}(G)$ is closed under joins and $G \notin \mathrm{CD}(G)$, it follows that no other group of order n can be contained in $\mathrm{CD}(G)$. Thus $\{A\} = \mathrm{CD}(G)$.

If $n = 4$, then D_8 is extraspecial. Thus $\mathrm{CD}(G)$ is isomorphic to the subspace lattice of $\mathbb{F}_2^2$ by Theorem 4.3.4.

Assume $n \geq 6$ and n is even. Since $n \equiv 0 \mod 2$, $Z(G) = \langle a^{\frac{n}{2}} \rangle$. Thus $m_G(G) = m_G(Z(G)) = 2 \cdot 2n = 4n$. Let $A = \langle a \rangle$. Since $b \notin C_G(A)$ and A is cyclic, $C_G(A) = A$. Thus $m_G(A) = |A|^2 = n^2$. Since $n \geq 6$ we have $n^2 = m_G(A) > 4n = m_G(G)$ and thus $Z(G), G \notin \mathrm{CD}(G)$. Let K be any subgroup such that $Z(G) < K < G$ of order not equal to n. By Lagrange's Theorem, $|K| < n$. Since $K \neq Z(G)$, it follows that $C_G(K) < G$. In particular, $|C_G(K)| \leq n$. Thus $m_G(K) < n \cdot n = n^2$, and thus $K \notin \mathrm{CD}(G)$. From the fact that $\mathrm{CD}(G)$ is closed under joins and $G \notin \mathrm{CD}(G)$, it follows that no other group of order n can be contained in $\mathrm{CD}(G)$. Thus $\{A\} = \mathrm{CD}(G)$.

□

4.5 The Chermak-Delgado lattice of some p-groups

Theorem 4.5.1. *Let P be a group of order $|P| = p^n$ such that $|Z(P)| = p^{n-2}$. Then the lattice $CD(P)$ is equivalent to the subgroup lattice of $C_p \times C_p$. In particular, P contains exactly $p + 1$ abelian subgroups M_i such that $Z(P) \leq M_i$.*

Proof. Since P is nonabelian, $P/Z(P)$ is not cyclic, and thus $P/Z(P) \cong C_p \times C_p$. Now, let $M_1, \cdots, M_{p+1}$ be the subgroups corresponding to the intermediate subgroups of $P/Z(P)$. Then $M_1, \cdots, M_{p+1}$ are noncentral abelian, and thus $m_P(M_i) = p^{2(n-1)} = |P||Z(P)| = p^n p^{n-2} = m_P(P) = m_P(Z(P))$.

□

Remark. This completely classifies $\mathrm{CD}(P)$ for P nonabelian of order p^3.

Theorem 4.5.2. *Let P be a p-group of order p^n such that $|Z(P)| \leq p^{n-3}$. Then $M_P = p^{2n-2}$ if and only if P contains a unique maximal abelian group H of index p. In this case, $CD(P) = \{H\}$.*

Proof. Let P be a p-group of order p^n such that $|Z(P)| \leq p^{n-3}$. We first notice that $m_P(P) \leq p^{2n-3}$.

Suppose P contains an abelian group H of index p. Then $H = H^\star$ since H is maximal normal abelian. Thus $m_P(H) = p^{2n-2}$. Since $P \notin \mathrm{CD}(P)$, $\mathrm{CD}(P)$ does not contain any other subgroup of order p^{n-1} by the closure under joins. Thus H is the unique abelian subgroup of index p. For any other subgroup K not equal to H, it is straightforward to see that $m_P(K) < p^{2n-2}$.

Now, suppose $M_P = p^{2n-2}$. Since $m_P(P) < p^{2n-2}$ we have that $P \notin \mathrm{CD}(P)$. For any $T \leq P$ of index greater or equal to p^2 not contained in the center, we have $m_P(T) = |T||T^\star| \leq p^{n-2} \cdot p^{n-1} = p^{2n-3}$, and for any $T \leq Z(P)$, we have $m_P(T) \leq m_P(Z(P)) \leq p^{2n-3}$. Thus there must exist $H \leq P$ such that $|H| = p^{n-1}$ and $|H^\star| = p^{n-1}$. By closure under joins there must exist a unique subgroup $H \in \mathrm{CD}(P)$ of index p. Furthermore, $H^\star$ has index p and thus $H = H^\star$. In particular, H is abelian.

In either case, we see $\mathrm{CD}(P) = \{H\}$. □

Theorem 4.5.3. *Let P be a nonabelian group of order p^n such that $|Z(P)| = p^{n-3}$. Then one of the following cases occurs.*

- *P has a unique abelian normal subgroup H such that $Z(P) \leq H$ and $|H| = p^{n-1}$. If this happens, then $CD(P) = \{H\}$.*
- *$CD(P) = \{P, Z(P)\}$.*

Proof. We first notice that $m_P(P) = p^n \cdot p^{n-3} = p^{2n-3}$. By Lemma 4.2.8, $M_P \leq p^{2n-2}$.

Case 1 is Theorem 4.5.2.

Case 2: Suppose P has no abelian subgroups of order p^{n-1}. Then $\sup\{m_P(T) | T \leq P\} = p^{2n-3} = m_P(P)$ and thus $P \in \mathrm{CD}(G)$. Notice that if $T \in \mathrm{CD}(P)$ with $|T| = p^{n-2}$, then $|T^*| = p^{n-1}$. However, if $T \in \mathrm{CD}(P)$ is such that $|T| = p^{n-2}$, then $T/Z(T)$ is cyclic and thus T is abelian. But then $T \leq Z(T^*)$, and thus T^* has order p^{n-1} and is abelian. This contradicts that P has no abelian subgroups of order p^{n-1}. Thus $\mathrm{CD}(P)$ cannot contain any subgroups of order p^{n-2} and hence cannot contain any subgroups of order p^{n-1}, for if $H \in \mathrm{CD}(P)$, then $H^* \in \mathrm{CD}(P)$ with $|H^*| = p^{n-2}$. Thus $\mathrm{CD}(P) = \{P, Z(P)\}$.

□

Lemma 4.5.4. *Let P be a p-group of order p^n with $n \geq 3$, and let $H \trianglelefteq P$ be a normal subgroup of order p^2. Suppose H is not contained in the center $Z(P)$. Then $[P : C_P(H)] = p$.*

Proof. Let P act on H by conjugation. Then we get a homomorphism $\psi : P \to \mathrm{Aut}(H)$. Since H is of order p^2, $H \cong C_{p^2}$ or $H \cong C_p \times C_p$. Thus $\mathrm{Aut}(H) \cong (C_{p^2})^\times$ or $\mathrm{Aut}(H) \cong \mathrm{GL}_2(\mathbb{F}_p)$. It follows that $|\mathrm{Aut}(H)| = \phi(p^2) = p(p-1)$ or $|\mathrm{Aut}(H)| = (p^2-1)(p^2-p) = p(p^2-1)(p-1)$. Either way, $v_p(|\mathrm{Aut}(H)|) = 1$. Since $\mathrm{im}(\psi)$ is a nontrivial p-subgroup of $\mathrm{Aut}(H)$ by the assumption that H is not central, it follows that $\mathrm{im}(\psi)$ has order p. By the First Isomorphism Theorem, $P/\ker(\psi) \cong \mathrm{im}(\psi)$. The result follows by noticing that $\ker(\psi) = C_P(H)$.

□

Corollary 4.5.5. *Let P of order p^n, $n \geq 3$, be such that $Z(P) \in CD(P)$ and $|Z(P)| = p$. Then the number of dots in $CD(P)$ of order p^2 equals the number of dots of order p^{n-1}. Furthermore, for $Q \leq P$ of order p^2, we have $Q \in CD(P)$ if and only if Q is normal in P.*

Proof. Notice that by assumption the Chermak-Delgado measure of P is $M_P = |Z(P)||P| = p^{n+1}$.

Let H be a normal subgroup of order p^2. Since $H \neq Z(G)$, by Lemma 4.5.4, $H^\star$ has index p, and thus $m_P(H) = p^2 \cdot p^{n-1} = p^{n+1}$ and we have $H \in \mathrm{CD}(P)$. Now, suppose T is a dot of order p^2. Then $T^\star$ has index p in P and thus $T^\star \trianglelefteq P$. Since $T = (T^\star)^\star$, we have that T is the centralizer of a normal subgroup of P. Hence, we can conclude that T is a normal subgroup of P. Thus every dot of order p^2 is normal in P. Since every dot of order p^{n-1} is the centralizer of a dot of order p^2, and $(T^\star)^\star = T$, the dots of order p^2 and the dots of index p are in bijection.

□

Lemma 4.5.6. [35, Lemma 4.4] *Let P be a p-group of nilpotence class 2 , and assume that P' has exponent p^e. Then the exponent of $P/Z(P)$ divides p^e. In particular, if P' is elementary abelian, then $P/Z(P)$ is elementary abelian, and thus $\Phi(P) \leq Z(P)$.*

Lemma 4.5.7. *Let P be a group of order p^4 where $|Z(P)| = p$. Then P has a unique maximal abelian normal subgroup H of order p^3. In fact, $H = C_P(P')$. Furthermore, in this case $CD(P) = \{C_P(P')\}$.*

Proof. We first prove that P' is of order p^2. Notice that for any group P of order p^n where $n \geq 2$, $[P : P'] \geq p^2$ (this is because p-groups have a normal subgroup of each possible index). Thus, in the case $|P| = p^4$, we have $1 < |P'| \leq p^2$. Suppose that $|P'| = p$. Then $P' = Z(P)$ and thus P is of nilpotence class 2. But then, by Lemma 4.5.6, $\Phi(P) = Z(P) = P'$ and thus P is extraspecial. This is absurd, as there are no extraspecial groups of even power order.

Thus, it follows that $|P'| = p^2$. By Lemma 4.5.4, $C_P(P')$ has index p in P and thus $|C_P(P')| = p^3$. Furthermore, since P' is of order p^2, it is abelian and thus $P' \leq Z(C_P(P'))$ and $[C_P(P') : P'] = p$, and hence $C_P(P')$ is abelian of order p^3. The uniqueness follows from Theorem 4.5.3.

□

Let P be a nonabelian group of order p^5. By Theorems 4.5.2, 4.5.3, we may assume $|Z(P)| = p$, $m_P(P) \neq p^8$, and that P contains no abelian subgroups of order p^4. We exclude the possibility that $M_P(P) = p^7$.

Lemma 4.5.8. *Let P be a p-group of order p^5 with $|Z(P)| = p$. Then $M_P = p^7$ is impossible.*

Proof. Suppose $M_P = p^7$. Notice $P \notin \mathrm{CD}(P)$ in this case. Thus, there is a unique characteristic subgroup $H \in \mathrm{CD}(P)$ of order p^4 and $H^\star$ is of order p^3. But then $H^\star \leq H$ by the closure under joins and $H/H^\star$ is cyclic of order p. Thus H is abelian, and hence $m_P(H) = p^8 > p^7$. This is nonsense, as we assumed $M_P = p^7$.

□

Theorem 4.5.9. [35, Theorem 4.7] *Let P be a finite p-group and suppose A is an abelian normal subgroup of P where $|A| = p^m$. Assume P/A is cyclic and that $|A \cap Z(P)| = p$. Then the nilpotence class of P is m.*

Theorem 4.5.10. [23, Theorem 4.5] *Let P be a nonabelian 2-group of order 2^n with $n \geq 4$ and with either the property that $|P/P'| = 4$ or P is of maximal nilpotency class. Then P is dihedral, semi-dihedral or generalized quaternion.*

Corollary 4.5.11. *Let P be a nonabelian group of order 2^n with $n \geq 4$ of maximal class. Then CD(P) is a single dot corresponding to the maximal abelian subgroup of index 2.*

Proof. A 2-group P of maximal class of order 2^n where $n \geq 4$ is dihedral, semi-dihedral or generalized quaternion by Theorem 4.5.10. Therefore, it has a maximal abelian subgroup A of index 2 and $|Z(P)| \leq 2^{n-3}$. By Theorem 4.5.2, $\mathrm{CD}(P) = \{A\}$.

□

Corollary 4.5.12. *Let P be a p-group of order p^5 where $|Z(P)| = p$. Then if CD(P) is a single dot, then P is of nilpotence class 4 and this dot corresponds to an abelian subgroup of P of index p. Otherwise, $P, Z(P) \in$ CD(P).*

Proof. By Lemma 4.5.8, $M_P \neq 7$. Suppose $\mathrm{CD}(P)$ has a single dot. Then $M_P = 8$, for otherwise both $P, Z(P) \in \mathrm{CD}(P)$. Now, by Theorem 4.5.2, P contains a unique maximal abelian subgroup, call it A, of order p^4. Since A is maximal, it must be normal. Thus, by Theorem 4.5.9, P has nilpotence class four. In other words, P is of maximal class.

□

Theorem 4.5.13. *Let P be a group of order p^5 of nilpotency class four such that $M_P(P) = p^6$. Then the CD(P) lattice has a unique dot of order p^5, p^4, p^2, p and $p+1$ dots of order p^3. The dots of order p^3 are abelian.*

Proof. If N is a normal subgroup of P with $|P : N| \geq p^2$, then N is a term of the lower central series since P has maximal class (see Theorem 4.1.2). Thus, there is a unique dot of order p^2, namely $\gamma_3(P)$, by Corollary 4.5.5. Thus, $(\gamma_3(P))^*$ is the unique dot of order p^4.

Since $\gamma_3(P) \leq (\gamma_3(P))^\star$ and $(\gamma_3(P))^\star$ is nonabelian, $(\gamma_3(P))^*/\gamma_3(P) \cong C_p^2$. By the Correspondence Theorem, there are exactly $p+1$ subgroups, H, such that $\gamma_3(P) \leq H \leq (\gamma_3(P))^\star$, and since $|H : \gamma_3(P)| = p$, H is abelian and so $H = H^\star \in \mathrm{CD}(P)$. Notice exactly one of these dots of order p^3 is normal in P, and it is P'.

It remains to show that there can be no more dots of order p^3 other than the $p+1$ abelian dots, A, such that $\gamma_3(P) < A < \gamma_3(P)^\star$.

We prove this by contradiction. To simplify notation, let $Q = \gamma_3(P)$. Suppose R is a dot of order p^3 such that R is not contained in $Q^\star$. Then $Q^\star R = P$ and thus $|Q^\star \cap R| = p^2$. Since $Q^\star, R \in \mathrm{CD}(P)$, $Q^\star \cap R \in \mathrm{CD}(P)$ and thus $Q^\star \cap R = Q$, as Q is the unique dot of order p^2 in $\mathrm{CD}(P)$. In particular, $Q < R$. Now, let A be a dot of order p^3 such that $Q < A < Q^\star$. Then $A \cap R = Q$ and $AR \in \mathrm{CD}(P)$. By assumption, R is not contained in $Q^\star$, and thus $AR = P$. But this is nonsense, since $|AR| = \frac{|A||R|}{|A \cap R|} = p^4$.

Thus, every dot of order p^3 is contained in $Q^\star$. Now, we have both $R < Q^\star$ and $R^\star < Q^\star$. Notice that $R^\star < Q^\star$ implies $Q = Q^{\star\star} < R^{\star\star} = R$, and thus $Q < R < Q^\star$ for every dot of order p^3.

□

Lemma 4.5.14. *Let P be a group of order p^5 where $|Z(P)| = p$, and let P have nilpotency class two. Then P is extraspecial.*

Proof. Since P is of nilpotence class 2 (a fortiori nonabelian) by assumption, $1 < P' \leq Z(P)$ and thus $P' = Z(P)$. Furthermore, by Lemma 4.5.6 and the fact that $\Phi(P) \cap Z(P) \neq \{e\}$, $\Phi(P) = Z(P)$.

It follows that P is extraspecial.

□

Corollary 4.5.15. *Let P be a group of order p^5 where $|Z(P)| = p$, and let P have nilpotency class two. Then $CD(P)$ is isomorphic to the subspace lattice of $\mathbb{F}_p^4$.*

Proof. By Lemma 4.5.14 and Theorem 4.3.4.

□

Lemma 4.5.16. *Let P be a p-group of order p^5 of nilpotency class three, with $|Z(P)| = p$. Then $M_P = p^6$ and $P, Z(P) \in CD(P)$.*

Furthermore, the number of dots in $CD(P)$ of order p^2 equals the number of dots of order p^4 equals the number of normal subgroups of order p^2.

Proof. The first statement follows by Corollary 4.5.12 and Lemma 4.5.8. The second statement follows by Corollary 4.5.5.

□

Corollary 4.5.17. *Let P be a 2-group of order 32 of nilpotency class three with $|Z(P)| = 2$. Then P' is of order 4.*

Proof. Otherwise, P' is of order 8 and thus $|P/P'| = 4$. But then, by Theorem 4.5.10, P is dihedral, semi-dihedral or generalized quaternion, and thus of maximal class, which is absurd as we assumed P is of nilpotency class three.

□

Theorem 4.5.18. [6, Theorem 9.10] *If a group G of order $p^m > p^3$ has a subgroup of order p^{m-1} of maximal class, then G is either of maximal class or $G/G' \cong C_p^3$.*

Corollary 4.5.19. *Let P be of order p^5 with $M_P = p^6$. If P has nilpotency class three and contains a maximal subgroup of maximal class, then $P' = \Phi(P)$ is of order p^2.*

Otherwise, if P does not contain any maximal subgroups of maximal class, every maximal subgroup of P has nilpotency class two.

Proof. We first note that since P is of nilpotency class three, $|P'| = p^2$ or p^3. Furthermore, since P does not contain any maximal abelian subgroups of order p^4, the maximal subgroups have nilpotency class three or two.

If P has a maximal subgroup of nilpotency class three, then by Theorem 4.5.18, $P/P' \cong C_p^3$, and thus $P' = \Phi(P)$ is of order p^2.

□

Corollary 4.5.20. *Let P be a group of order p^5 of nilpotency class three with $|Z(P)| = p$, and assume P does not contain any maximal subgroups of maximal class. Then every maximal subgroup of P is in $CD(P)$.*

Proof. By Corollary 4.5.12, $M_P = p^6$. Let M be a maximal subgroup of P. Then $|M| = p^4$. Suppose $|Z(M)| = |Z(P)| = p$. By Lemma 4.5.7 and Theorem 4.5.9, M is of maximal class, which contradicts the fact that M is of nilpotency class two (as M is nonabelian, otherwise P is of maximal nilpotency class). Thus $|Z(M)| = p^2$. Notice that since $Z(M)$ is abelian and $Z(M) \leq C_P(M)$, $C_P(M) = M^\star$ is of order p^2. Thus, for any maximal subgroup M of P, M^* is of order exactly p^2. It follows that $m_P(M) = p^6 = M_P$, as desired.

□

Corollary 4.5.21. *Let P be a group of order p^5 of nilpotency class three with $|Z(P)| = p$, and assume P does not contain any maximal subgroups of maximal class. Then*

1. *If $\Phi(P)$ is of order p^3, then $CD(P)$ contains exactly $p+1$ dots of order p^4 and exactly $p+1$ dots of order p^2.*
2. *If $\Phi(P)$ is of order p^2, then $CD(P)$ contains exactly $1+p+p^2$ of order p^4 and exactly $1+p+p^2$ dots of order p^2 (although we conjecture that this case does not happen).*

Proof. By Corollary 4.5.20, the number of dots of order p^4 is exactly the number of maximal subgroups of $P/\Phi(P)$. The statement about the dots of order p^2 follows by Corollary 4.5.5.

□

We summarize some our results for convenience.

Theorem 4.5.22. *Let P be a nonabelian p-group of order p^n. Then:*

1. If $|Z(P)| = p^{n-2}$, then the lattice $\mathrm{CD}(P)$ is equivalent to the subspace lattice of $\mathbb{F}_p^2$. In particular, nonabelian p-groups of order p^3 have such $\mathrm{CD}(P)$.

2. If $|Z(P)| = p^{n-3}$, then one of the following cases occurs.

   (i) P has a unique abelian normal subgroup H such that $Z(P) \leq H$ and $|H| = p^{n-1}$. If this happens, then $\mathrm{CD}(P) = \{H\}$. In the case $n = 4$, $H = C_P(P')$.

   (ii) $\mathrm{CD}(P) = \{P, Z(P)\}$. This case does not happen for $n = 4$.

3. If $n = 5$ and $|Z(P)| = p$, then

   (i) If P has nilpotency class 2, then P is extraspecial and thus $\mathrm{CD}(P) = \mathbb{F}_p^4$.

   (ii) If P has nilpotency class 4 with $M_P(P) = p^6$, then the $\mathrm{CD}(P)$ lattice has a unique dot of order p^5, p^4, p^2, p and $p+1$ dots of order p^3. The dots of order p^3 are abelian.

   (iii) If $\mathrm{CD}(P)$ is a single dot, then P is of maximal class. If $p = 2$, $\mathrm{CD}(P)$ is a single dot if and only if P is of maximal class.

This research area is still in its infancy. It is clear that much work is left to be done, although categorizing $\mathrm{CD}(P)$ of p-groups based on the index $[P : Z(P)]$ has proved fruitful for small indices so far.

Bibliography

[1] Yismaw Alemu, *On zeros of diagonal forms over* $\mathfrak{p}$*-adic fields*, Acta Arith. **48** (1987), no. 3, 261–273. MR921089

[2] Emil Artin, *The collected papers of Emil Artin*, Edited by Serge Lang and John T. Tate, Addison–Wesley Publishing Co., Inc., Reading, Mass.-London, 1965. MR0176888

[3] James Ax and Simon Kochen, *Diophantine problems over local fields. I*, Amer. J. Math. **87** (1965), 605–630. MR0184930

[4] ———, *Diophantine problems over local fields. II. A complete set of axioms for p-adic number theory*, Amer. J. Math. **87** (1965), 631–648. MR0184931

[5] ———, *Diophantine problems over local fields. III. Decidable fields*, Ann. of Math. (2) **83** (1966), 437–456. MR0201378

[6] Yakov Berkovich, *Groups of prime power order. Vol. 1*, De Gruyter Expositions in Mathematics, vol. 46, Walter de Gruyter GmbH & Co. KG, Berlin, 2008. With a foreword by Zvonimir Janko. MR2464640

[7] Ronald Gale Bierstedt, *Some problems on the distribution of kth power residues modulo a prime*, ProQuest LLC, Ann Arbor, MI, 1963. Thesis (Ph.D.)–University of Colorado at Boulder. MR2616571

[8] B. J. Birch, *Forms in many variables*, Proc. Roy. Soc. Ser. A **265** (1961/1962), 245–263. MR0150129

[9] ———, *Diagonal equations over* $\mathfrak{p}$*-adic fields*, Acta Arith. **9** (1964), 291–300. MR0167456

[10] B. J. Birch and D. J. Lewis, $\mathfrak{p}$*-adic forms*, J. Indian Math. Soc. (N.S.) **23** (1959), 11–32 (1960). MR0123534

[11] B. J. Birch, D. J. Lewis, and T. G. Murphy, *Simultaneous quadratic forms*, Amer. J. Math. **84** (1962), 110–115. MR0136582

[12] J. D. Bovey, $\Gamma^*(8)$, Acta Arith. **25** (1973/74), 145–150. MR0347713

[13] Ben Brewster and Elizabeth Wilcox, *Some groups with computable Chermak-Delgado lattices*, Bull. Aust. Math. Soc. **86** (2012), no. 1, 29–40. MR2960225

[14] D. Brink, H. Godinho, and P. H. A. Rodrigues, *Simultaneous diagonal equations over p-adic fields*, Acta Arith. **132** (2008), no. 4, 393–399. MR2413361

[15] C. Chevalley, *Démonstration d'une hypothèse de M. Artin*, Abh. Math. Sem. Univ. Hamburg **11** (1935), no. 1, 73–75. MR3069644

[16] S. Chowla, *On a conjecture of J. F. Gray*, Norske Vid. Selsk. Forh. Trondheim **33** (1960), 58–59. MR0125079

[17] Daniel F. Coray, *On a problem of Pfister about intersections of three quadrics*, Arch. Math. (Basel) **34** (1980), no. 5, 403–411. MR593766

[18] H. Davenport and D. J. Lewis, *Homogeneous additive equations*, Proc. Roy. Soc. Ser. A **274** (1963), 443–460. MR0153655

[19] V. B. Demyanov, *On cubic forms over discrete normed fields*, Dokl. Akad. Nauk SSSR **74** (1950), 889–891.

[20] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 7.2)*, 2016. http://www.sagemath.org.

[21] M. Dodson, *Homogeneous additive congruences*, Philos. Trans. Roy. Soc. London Ser. A **261** (1967), 163–210. MR0213296

[22] M. M. Dodson, *Some estimates for diagonal equations over* $\mathfrak{p}$*-adic fields*, Acta Arith. **40** (1981/82), no. 2, 117–124. MR649113

[23] Daniel Gorenstein, *Finite groups*, Second Edition, Chelsea Publishing Co., New York, 1980. MR569209

[24] Fernando Q. Gouvêa, *p-adic numbers*, Second Edition, Universitext, Springer-Verlag, Berlin, 1997. MR1488696

[25] Torbjörn Granlund and the GMP development team, *GNU MP: The GNU Multiple Precision Arithmetic Library*, 5.1.3, 2013. `http://gmplib.org/`.

[26] James Francis Gray, *Diagonal forms of prime degree*, ProQuest LLC, Ann Arbor, MI, 1959. Thesis (Ph.D.)–University of Notre Dame. MR2939062

[27] Marvin J. Greenberg, *Lectures on forms in many variables*, W. A. Benjamin, Inc., New York-Amsterdam, 1969. MR0241358

[28] Newcomb Greenleaf, *Irreducible subvarieties and rational points*, Amer. J. Math. **87** (1965), 25–31. MR0182625

[29] Larry C. Grove, *Classical groups and geometric algebra*, Graduate Studies in Mathematics, vol. 39, American Mathematical Society, Providence, RI, 2002. MR1859189

[30] P. Hall, *The classification of prime-power groups*, J. Reine Angew. Math. **182** (1940), 130–141. MR0003389

[31] Franz Halter-Koch, *Arithmetical interpretation of weighted Davenport constants*, Arch. Math. (Basel) **103** (2014), no. 2, 125–131. MR3254355

[32] Helmut Hasse, *Über die Darstellbarkeit von Zahlen durch quadratische Formen im Körper der rationalen Zahlen*, J. Reine Angew. Math. **152** (1923), 129–148. MR1581005

[33] D. R. Heath-Brown, *Artin's conjecture on zeros of p-adic forms*, Proceedings of the International Congress of Mathematicians. Volume II, 2010, pp. 249–257. MR2827794

[34] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, Second Edition, Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716

[35] I. Martin Isaacs, *Finite group theory*, Graduate Studies in Mathematics, vol. 92, American Mathematical Society, Providence, RI, 2008. MR2426855

[36] Michael P. Knapp, *Artin's conjecture for forms of degree 7 and 11*, J. London Math. Soc. (2) **63** (2001), no. 2, 268–274. MR1810128

[37] ———, *Exact values of the function* $\Gamma^*(k)$, J. Number Theory **131** (2011), no. 10, 1901–1911. MR2811557

[38] ———, *Pairs of additive forms of odd degrees*, Michigan Math. J. **61** (2012), no. 3, 493–505. MR2975257

[39] T. Y. Lam, *Introduction to quadratic forms over fields*, Graduate Studies in Mathematics, vol. 67, American Mathematical Society, Providence, RI, 2005. MR2104929

[40] Serge Lang, *On quasi algebraic closure*, ProQuest LLC, Ann Arbor, MI, 1951. Thesis (Ph.D.)–Princeton University. MR2938192

[41] ———, *On quasi algebraic closure*, Ann. of Math. (2) **55** (1952), 373–390. MR0046388

[42] R. R. Laxton and D. J. Lewis, *Forms of degrees* 7 *and* 11 *over* $\mathfrak{p}$*-adic fields*, Proc. Sympos. Pure Math., Vol. VIII, 1965, pp. 16–21. MR0175884

[43] D. B. Leep and W. M. Schmidt, *Systems of homogeneous equations*, Invent. Math. **71** (1983), no. 3, 539–549. MR695905

[44] David B. Leep and Laura Mann Schueller, *Zeros of a pair of quadratic forms defined over a finite field*, Finite Fields Appl. **5** (1999), no. 2, 157–176. MR1680530

[45] David B. Leep and Charles C. Yeomans, *Quintic forms over p-adic fields*, J. Number Theory **57** (1996), no. 2, 231–241. MR1382749

[46] D. J. Lewis, *Cubic homogeneous polynomials over p-adic number fields*, Ann. of Math. (2) **56** (1952), 473–478. MR0049947

[47] ———, *Cubic congruences*, Michigan Math. J. **4** (1957), 85–95. MR0084013

[48] Rudolf Lidl and Harald Niederreiter, *Finite fields*, Second Edition, Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997. With a foreword by P. M. Cohn. MR1429394

[49] Luz E. Marchan, Oscar Ordaz, and Wolfgang A. Schmid, *Remarks on the plus-minus weighted Davenport constant*, Int. J. Number Theory **10** (2014), no. 5, 1219–1239. MR3231411

[50] Karl Kenneth Norton, *On homogeneous diagonal congruences of odd degree*, ProQuest LLC, Ann Arbor, MI, 1966. Thesis (Ph.D.)–University of Illinois at Urbana-Champaign. MR2616020

[51] John E. Olson, *A combinatorial problem on finite Abelian groups. I*, J. Number Theory **1** (1969), 8–10. MR0237641

[52] ———, *A combinatorial problem on finite Abelian groups. II*, J. Number Theory **1** (1969), 195–199. MR0240200

[53] Philippe Revoy, *The generalized level of a nonprime finite field is two*, Amer. Math. Monthly **105** (1998), no. 2, 167–168. MR1605867

[54] Wolfgang M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics, Vol. 536, Springer-Verlag, Berlin-New York, 1976. MR0429733

[55] Christopher Skinner, *Local solvability of diagonal equations (again)*, Acta Arith. **124** (2006), no. 1, 73–77. MR2262141

[56] Christopher M. Skinner, *Solvability of* $\mathfrak{p}$*-adic diagonal equations*, Acta Arith. **75** (1996), no. 3, 251–258. MR1387863

[57] Guy Terjanian, *Un contre-exemple à une conjecture d'Artin*, C. R. Acad. Sci. Paris Sér. A-B **262** (1966), A612. MR0197450

[58] Aimo Tietäväinen, *On a problem of Chowla and Shimura*, J. Number Theory **3** (1971), 247–252. MR0285484

[59] Robert A. Wilson, *The finite simple groups*, Graduate Texts in Mathematics, vol. 251, Springer-Verlag London, Ltd., London, 2009. MR2562037

Vita

Luis Alfonso Sordo Vieira

Birthplace

Valencia, Venezuela.

Education

- Bachelor of Science, Wayne State University, May 2012.
- Master of Arts, University of Kentucky, December 2014.

Scholastic Awards

- Outstanding Undergraduate Award, Wayne State University, May 2012.
- Kentucky Opportunity Fellowship, University of Kentucky, August 2012.
- National Science Foundation Graduate Research Fellowship, April 2013.

Publications

- Ping Ngai Chung, Miguel A. Fernandez, Yifei Li, Michael Mara, Frank Morgan, Isamar Rosa Plata, Niralee Shah, Luis Sordo Vieira, Elena Wikner, *Isoperimetric pentagonal tilings*, Notices Amer. Math. Soc. 59 (May, 2012), 632-640.
- Ping Ngai Chung, Miguel A. Fernandez, Niralee Shah, Luis Sordo Vieira, Elena Wikner, *Perimeter- minimizing pentagonal tilings*, Involve, V. 7., N. 4, (2014).
- Ping Ngai Chung, Miguel A. Fernandez, Niralee Shah, Luis Sordo Vieira, *Are Circles Isoperimetric in the Plane with Density e^r?* Rose-Hulman Undergraduate Journal, V.16, N. 1. (2015).