MAXIMAL SUBSPACES OF ZEROS OF QUADRATIC FORMS OVER FINITE FIELDS

MARK HUBENTHAL

Abstract. This paper introduces the reader to quadratic forms defined over finites field in the general sense. In short, a quadratic form $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ with n indeterminates is a homogeneous polynomial of degree-2 with coefficients taken from the field $\mathbb{F}_q$. We will classify all quadratic forms as being one of three fundamental types and compute the number of solutions to an arbitrary quadratic form equation $f(x_1, \ldots, x_n) = b$, where f is one of the three types. Finally, we consider that the zeros of a quadratic form f (i.e. solutions to the equation $f(x_1, \ldots, x_n) = 0$), can form subspaces of $\mathbb{F}_q^n$. The maximum size of such a subspace can be shown only to depend on q (the field characteristic), the number of indeterminates n, and the particular type of f.

Date: May 19, 2006.

Contents

1. Introduction

The solution of polynomial equations in multiple variables represents a fundamental area of mathematics. For example, what are the solutions (x, y, z) to the equation $x^3 + x^2y^2z + z^2 + yz + 2xz^3 = 0$ if $x, y, z \in \mathbb{R}$? In this paper, we investigate quadratic forms, which are a special type of polynomial. More specifically, a quadratic form is a homogeneous polynomial of degree 2. From the preceding example, if we consider that each solution (x, y, z) is a vector in the vector space $\mathbb{R}^3$, what can be said about the set of all solutions? In general, this question is rather daunting. Note, however, that the field of interest $\mathbb{R}$ is infinite in size. In this paper, we will be dealing exclusively with finite fields.

Suppose that $\mathbb{F}_q$ is a finite field with q elements. The zeros of a quadratic form (in n indeterminates) $f \in \mathbb{F}_q[x_1, \ldots, x_n]$ are all n-tuples, or vectors in $\mathbb{F}_q^n$ that satisfy the equation $f(x_1, \ldots, x_n) = 0$. We present a theorem which determines the number of such zeros that an arbitrary quadratic form has. In light of the fact that subsets of these zeros generate subspaces of the vector space $\mathbb{F}_q^n$, we can also state the size of the maximal subspaces.

The algebraic theory of quadratic forms was first introduced by Ernest Witt in a 1937 paper. However, while quadratic form theory over local and global fields seemed to thrive throughout the 20th century, it was not until the late 1960's, thanks to the work of Pfister, that quadratic form theory over general fields grew in popularity. Much of the content herein is motivated by a comprehensive text on finite fields by Rudolf Lidl and Harald Niederreiter [4]. A recent forerunner in the field of quadratic forms is T.Y. Lam, and the reader is referred to Lam [5]. More accessible background information on abstract algebra and specifically, fields, can be obtained from Gallian [3].

The next section is devoted to a brief review of fields, and more specifically, finite fields. We then cover some important results and theorems regarding fields that will be helpful throughout the rest of the paper.

In section 3 we present the definition of a quadratic form as well as some of their fundamental properties. Section 4 looks at a key result which establishes that quadratic forms defined over $\mathbb{F}_q$, where q is odd, are diagonalizable. In particular, close attention is paid to the idea of equivalent quadratic forms. This idea is very instrumental in proving later theorems. Specifically, in section 5 we prove that any arbitrary quadratic form defined over a finite field is equivalent to a quadratic form of one of three types.

Finally, sections 6 and 7 both concern the solutions of a given quadratic form equation. Important theorems are presented that allow us to deduce about the number of solutions to the equation $f(x_1, \ldots, x_n) = b$, where f is a quadratic form. Finally, in section 8 we determine the size of the maximal subspaces of $\mathbb{F}_q^n$ generated by the zeros of a quadratic form $f \in \mathbb{F}_q[x_1, \ldots, x_n]$.

2. Background

2.1. **Fields.** In order to understand the behavior of quadratic forms over finite fields, it is first important to know what a field is. Specifically, one must have some familiarity with the properties of finite fields. Recall that a field is a special kind of ring in which there exists a multiplicative identity, every nonzero element has a multiplicative inverse, and in which the multiplicative operation is commutative. To be more precise, we present the following complementary definitions.

Definition 1. *A **ring** $(R, +, \cdot)$ is a set R, coupled with two binary operations, denoted by $+$ and $\cdot$, such that:*

1. *R is an abelian group under the operation $+$.*
2. *$(a \cdot b) \cdot c = a \cdot (b \cdot c)$ for all $a, b, c \in R$.*
3. *The distributive property holds, such that for all $a, b, c \in R$, $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$.* [4]

An obvious example of a ring is the set of all integers. However, as we shall see shortly, the integers do not form a field.

Definition 2. *A **field** F is a commutative ring with a multiplicative identity in which every nonzero element has a multiplicative inverse.*

One example of a field is the set of rational numbers $\mathbb{Q}$. Commutativity under multiplication holds trivially, and any nonzero rational number $\frac{p}{q}$ where $p, q \in \mathbb{Z} \setminus \{0\}$ has a multiplicative inverse $\frac{q}{p}$. The set of integers is not a field because there does not exist an integer x such that $2 \cdot x = 1$. However, the set $\mathbb{Z}$ does form an integral domain, which we will now define.

Definition 3. *An **integral domain** is a commutative ring with identity $e \neq 0$ where $ab = 0$ implies that $a = 0$ or $b = 0$.*

One might ask why the definition of an integral domain has been stated. To answer that, we state an important theorem that connects finite fields to finite integral domains.

Theorem 1. *Every finite integral domain is a field.*

The proof of Theorem 1 relies on listing the elements of the integral domain and multiplying each one by a nonzero element a contained in the set. It is then a simple matter of realizing that the new set of elements obtained are all distinct, and thus one of them must equal the identity e. The result follows.

Also of considerable use when constructing finite fields is the **polynomial ring** $R[x]$, where R is any ring. Elements of $R[x]$ are called polynomials in the indeterminate x with coefficients in R. In addition, any given element has only finitely many nonzero coefficients. We usually write this element as

$$\sum_{k=0}^{n} a_k x^k = a_0 + a_1 x + \cdots + a_n x^n$$

where $a_k \in R$ for all $1 \leq k \leq n$.

2.2. **Finite Fields.** In this section, we consider some important properties of finite fields and establish a set notation to be followed in future sections. Specifically, we consider the question of what possible sizes a given finite field can have. Two short theorems are instrumental in arriving at the desired conclusion. However, we must first define what is meant by the term *characteristic*.

Definition 4. *If R is an arbitrary ring and there exists a positive integer n such that $nr = 0$ for every $r \in R$, (The expression nr represents the element r added to itself n times) then the least such positive integer n is called the* ***characteristic*** *of R and R is said to have characteristic n. If no such positive integer n exists, then R is said to have characteristic 0.* [4]

This naturally leads to a theorem addressing the possible characteristic of any finite field. For a detailed proof, the reader is referred to [4].

Theorem 2. *A finite field has prime characteristic.*

For the next theorem, we need to know the following definition, which is presented for reference.

Definition 5. *Let $f \in K[x]$ be of positive degree and F be an extension field of K. Then f is said to* ***split*** *in F if f can be written as a product of linear factors in $F[x]$–that is, if there exist elements $\alpha_1, \alpha_2, \cdots, \alpha_n \in F$ such that*

$$f(x) = a(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_n). \tag{1}$$

The field F is a splitting field of f over K if f splits in F and if, moreover, $F = K(\alpha_1, \alpha_2, \cdots, \alpha_n)$. [4]

In short, the splitting field F of a polynomial f over K is the smallest field containing all the roots of f. For more information regarding the theory behind field extensions and the ideas covered thus far, the reader is referred to [4], [3] or [2].

Now we arrive at a key property of finite fields: every finite field has size p^n where p is a prime and n is a positive integer. Furthermore, any two finite fields of identical size p^n are isomorphic. The theorem goes as follows.

Theorem 3. *For each prime p and each positive integer n, there is a unique finite field, up to isomorphism, of order p^n.* [3]

The proof of Theorem 3 involves considering the splitting field F of the polynomial $f(x) = x^q - x \in \mathbb{F}_p[x]$ over $\mathbb{F}_p$. Counting multiplicity, f has p^n roots over F. Using the derivative test, we have that $f'(x) = qx^{q-1} - 1 = -1$ in $\mathbb{F}_p[x]$. In other words, f' has no roots at all . Thus, f and f' have no roots in common, and so all the roots of f in F are unique (see [4]). We then consider the set $S = \{a \in F : a^q - a = 0\}$. It follows that S is a subfield of F with q elements (see [3]). From Lemma **??**, S contains all the roots of $x^q - x$, and so f must split in S. Thus, $F = S$ and is a finite field with q elements.

As for subfields of finite fields, it turns out that every subfield of $\mathbb{F}_q$ for $q = p^n$, has order p^m where m divides n. One final interesting thought on finite fields is that the set of non-zero elements in $\mathbb{F}_q$ form a cyclic group under multiplication. We denote this group by $\mathbb{F}_q^*$.

Now that we have established that every finite field has order p^n for some prime p and positive integer n, we will write $\mathbb{F}_q$ to denote any field of order q. It is assumed here that $q = p^n$ for some prime p and $n > 0$. Moreover, we write $\mathbb{F}_q[x]$ to denote the field of polynomials in the indeterminate x with coefficients in $\mathbb{F}_q$. Of course, we will be dealing with polynomials in multiple indeterminates, and so we consider frequently the polynomial ring $\mathbb{F}_q[x_1, \cdots, x_n]$. The elements of $\mathbb{F}_q[x_1, \cdots, x_n]$ are expressions of the form

$$f = f(x_1, \cdots, x_n) = \sum a_{i_1 \cdots i_n} x_1^{i_1} \cdots x_n^{i_n} \tag{2}$$

with coefficients $a_{i_1 \cdots i_n} \in \mathbb{F}_q$.

2.2.1. *Example.* Consider that if we can find a polynomial $f \in \mathbb{F}_p[x]$ of degree n that is irreducible over $\mathbb{F}_p$, we can construct a field extension $\mathbb{F}_p(\alpha)$ of order p^n where α is any root of f. Let us construct the finite field $\mathbb{F}_{3^2}$ using this method. We start by finding a degree-2 irreducible polynomial in $\mathbb{F}_3[x]$. It is easy to verify that $f(x) = x^2 + 1$ is irreducible over $\mathbb{F}_3$. Thus, the ideal $< f(x) >$ is maximal and so the factor ring $\mathbb{F}_3/ < f(x) >$ is a field. The elements of this field are listed below. Note that multiplication and addition are computed mod $x^2 + 1$.

$$\begin{array}{ccc} 0 & 1 & 2 \\ x & 2x & 1+x \\ 2+x & 1+2x & 2+2x \end{array}$$

Alternatively, we could just find the splitting field for the polynomial $x^9 - x$ over $\mathbb{F}_3$. However, this method is more cryptic and cumbersome to resolve in an actual computation.

Note that in the example just mentioned, $p = 3$ and $n = 2$. Since 1 is the only positive divisor of 3 besides 3 itself, it follows that there exists only one proper subfield of $\mathbb{F}_3/ < x^2 + 1 >$, namely, the subfield $\mathbb{F}_3$. This particular subfield is generated by the element 1.

3. Quadratic Forms

It is possible to define a quadratic form in a more abstract setting or in a manner more akin to linear algebra. For the purpose of simplicity, we take the latter approach.

Definition 6. *A **Quadratic Form** in n indeterminants over $\mathbb{F}_q$ is a homogeneous polynomial $f(x_1, x_2, \ldots, x_n) \in \mathbb{F}_q[x_1, x_2, \ldots, x_n]$ of degree 2, or the zero polynomial. In general then,*

$$f(x_1, x_2, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j \tag{3}$$

where each a_{ij} is an element of $\mathbb{F}_q$.

Note that by homogeneous we mean each term has the same degree. We are also interested in solutions to the equation $f(x_1, \ldots, x_n) = b$ where f is a quadratic form over $\mathbb{F}_q$ and $b \in \mathbb{F}_q$. The following definition will thus prove useful.

Definition 7. *A quadratic form f over $\mathbb{F}_q$ **represents** the value $a \in \mathbb{F}_q$ if the equation $f(x_1, x_2, \ldots, x_n) = a$ has a solution in $\mathbb{F}_q^n$.*

We can define a quadratic form in a more compact way by associating with it a coefficient matrix A, where the row i column j entry is simply a_{ij}. If q is odd (i.e. $p \neq 2$), we can write the mixed terms as $\frac{1}{2}a_{ij}x_ix_j + \frac{1}{2}a_{ji}x_jx_i$. Thus, we can arrange that $a_{ij} = a_{ji}$ to get a symmetric coefficient matrix A. By convention, all coefficient matrices are made symmetric when q is odd. Now, if we define $\mathbf{x}$ as the column vector of indeterminates $x_1, x_2, \ldots, x_n$, we can write f as just

$$\mathbf{x}^T A\mathbf{x}.$$

In expanded form this reads

$$f(x_1, x_2, \ldots, x_n) = (x_1, x_2, \ldots, x_n) \begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \ldots & a_{nn} \end{bmatrix} \begin{pmatrix} x_1 \\ x_2 \\ \vdots \\ x_n \end{pmatrix}. \tag{4}$$

If the coefficient matrix A of f has rank n, then we say that f is nondegenerate. Equivalently, f is nondegenerate if $\det A \neq 0$.

3.1. **Equivalence.** Two quadratic forms f and g over a finite field $\mathbb{F}_q$ are equivalent if f can be transformed into g using a linear substitution of the form $\mathbf{x} = C\mathbf{y}$, where C is an $n \times n$ nonsingular matrix, $\mathbf{x}$ is the indeterminate vector for f, and $\mathbf{y}$ is the indeterminate vector for g. If f and g are two equivalent quadratic forms, we can relate their respective coefficient matrices, A and B, as follows:

$$B = C^T AC \tag{5}$$

$$\mathbf{x}^T A\mathbf{x} = (C\mathbf{y})^T A(C\mathbf{y}) = \mathbf{y}^T (C^T AC)\mathbf{y} = \mathbf{y}^T B\mathbf{y}. \tag{6}$$

4. Quadratic Forms Over a Finite Field $\mathbb{F}_q$ Where q is Odd Are Diagonalizable

This section establishes a result that will be useful in proving the existence of categories of quadratic forms in the q-odd case. That is, we will prove that any quadratic form falls into one of three types. The proofs of the following two results can be found in [4] and are stated only for reference.

Lemma 1. *If q is odd and the quadratic form $f \in \mathbb{F}_q[x_1, x_2, \ldots, x_n], n \geq 2$, represents $a \in \mathbb{F}_q^*$, then f is equivalent to $ax_1^2 + g(x_2, \ldots, x_n)$, where g is a quadratic form over $\mathbb{F}_q$ in at most $n-1$ indeterminates.* [4]

Using Lemma 1 and induction on the number of indeterminates n, it is possible to prove the following theorem, noting first that a diagonal quadratic form looks like

$$\sum_{i=1}^{n} a_{ii} x_i^2.$$

Theorem 4. *Every quadratic form over $\mathbb{F}_q$, q odd, is equivalent to a diagonal quadratic form.* [4]

4.1. **Example.** We will show the process by which to find an equivalent diagonal quadratic form to $f(x_1, x_2, x_3) = x_1^2 + x_1x_2 + 2x_2x_3 + x_2^2 + 2x_3^2$ over $\mathbb{F}_3$. The general idea is quite simple as we need only apply Lemma 1 repeatedly. Eventually, depending on the order of f, we will obtain the desired equivalent diagonal quadratic form. To begin, the coefficient matrix A of f is given by

$$A = \begin{pmatrix} 1 & 2 & 0 \\ 2 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix},$$

and $\det(A) = 1(2-1) - 2(4) + 0 = 1 - 8 = -7 = 2$.

Thus f is nondegenerate. If f were degenerate, we would end up with an equivalent quadratic form that has less than n indeterminates. Note that $f(1,1,1) = 1$, and so f represents 1. We now construct C, a nonsingular matrix with $(1,1,1)$ as the first column. This will transform f into an equivalent quadratic form with 1 as the coefficient of x_1^2. Thus,

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

Saving some computation,

$$C^T A C = \begin{pmatrix} 1 & 1 & 0 \\ 1 & 1 & 1 \\ 0 & 1 & 2 \end{pmatrix}.$$

Substituting into Equation (6) and expanding yields

$$(y_1, y_2, y_3) \begin{pmatrix} y_1 + y_2 \\ y_1 + y_2 + y_3 \\ y_2 + y_3 \end{pmatrix} = y_1^2 + 2y_1y_2 + y_2^2 + 2y_2y_3 + y_3^2.$$

In hindsight, the goal of the above transformation was to get the coefficient of x_1^2 to be $f(1,1,1) = 1$. This was already the case before we made the transformation, but going through the steps anyway better illustrates the entire process. We can rewrite the above equation as

$$\begin{aligned} y_1^2 + 2y_1y_2 + (y_2^2 + 2y_2y_3 + y_3^2) &= (y_1 + y_2)^2 - y_2^2 + (y_2^2 + 2y_2y_3 + y_3^2) \\ &= (y_1 + y_2)^2 + 2y_2y_3 + y_3^2. \end{aligned}$$

Substituting $z_1 = y_1 + y_2$ and $z_2 = y_2$, $z_3 = y_3$, we get

$$z_1^2 + 2z_2z_3 + z_3^2.$$

Note that the substitution here can be written in matrix form as $C_2\mathbf{z} = \mathbf{y}$ where

$$C_2 = \begin{pmatrix} 1 & 2 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}.$$

Now we can apply the same algorithm to $2z_2z_3 + z_3^2$. This will certainly lead us to an equivalent diagonal quadratic form. But it is relatively easy to guess the substitution $w_1 = z_1$, $w_2 = z_2$, and $w_3 = z_2 + z_3$. In matrix form it is $C_3\mathbf{w} = \mathbf{z}$ where

$$C_3 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 2 & 1 \end{pmatrix}.$$

Applying this transformation we get

$$w_1^2 - w_2^2 + w_3^2 = z_1^2 - z_2^2 + z_2^2 + 2z_2z_3 + z_3^2 = z_1^2 + 2z_2z_3 + z_3^2.$$

The resulting quadratic form is diagonal, so we are done.

In retrospect, observe that

$$CC_2C_3\mathbf{w} = \mathbf{x}.$$

Let $B = CC_2C_3$. Multiplying the matrices yields

$$B = \begin{pmatrix} 1 & 2 & 0 \\ 1 & 0 & 0 \\ 1 & 1 & 1 \end{pmatrix}.$$

Since $B\mathbf{w} = \mathbf{x}$ and B is nonsingular, the quadratic form we started with is equivalent to the diagonal one we ended with.

5. The Existence of Categories

It is nice to be able to diagonalize any quadratic form over a field of odd order q. However, diagonalization is impossible when q is some power of 2. This is simply because of the fact that every finite field of even order has 2^k elements for some positive integer k, and therefore has characteristic 2. This means that $a + a = 0$ for all elements a in the field.

Consider that for characteristic-2 fields, the equation $(x_1 + x_2)^2$ simplifies to $x_1^2 + x_1x_2 + x_2x_1 + x_2^2 = x_1^2 + x_2^2$. In the general case, we have

$$x_1^2 + x_2^2 + \cdots + x_n^2 = (x_1 + x_2 + \cdots + x_n)^2.$$

Of course, this is equivalent to a quadratic form of one variable via the nonsingular substitution $z_1 = \sum_{i=1}^{n} x_i$ and $z_i = x_i$ for $2 \leq i \leq n$. Consequently, we must be careful when trying to prove results pertaining to quadratic forms over a general finite field $\mathbb{F}_q$.

The primary purpose of classifying all quadratic forms is to make it easier to prove generalized theorems about them. For example, how many different zeros can any quadratic form possibly have? The important ideas that follow make it feasible to address such questions. The result in the following section will be instrumental in establishing the existence of three fundamental types of quadratic forms.

5.1. Important Definitions.

Before continuing, we must consider a few important definitions.

Definition 8. *Let G be a finite abelian group of order $|G|$ with identity 1_G. A **character** χ of G is a homomorphism from G into the multiplicative group U of complex numbers of absolute value 1. Thus $\chi : G \to U$ such that $\chi(g_1g_2) = \chi(g_1)\chi(g_2)$ for all $g_1, g_2 \in G$.*

Following is a special character that will be useful in determining the number of solutions to a quadratic form equation.

Definition 9. *Let q be odd and let η be the real-valued function of $\mathbb{F}_q^*$ with $\eta(c) = 1$ if c is the square of an element of $\mathbb{F}_q^*$ and $\eta(c) = -1$ otherwise. Then η is called the **quadratic character** of $\mathbb{F}_q$.*

And finally we present another function useful when the number of indeterminates in a quadratic form is even.

Definition 10. *For a finite field $\mathbb{F}_q$ the integer-valued function v on $\mathbb{F}_q$ is defined by $v(b) = -1$ for $b \in \mathbb{F}_q^*$ and $v(0) = q - 1$.*

5.2. **Reduction Result.** In order to prove that there are only three different types of quadratic forms, we must first be able to pull off cross terms, or as they are more commonly named, **hyperplanes**.

Lemma 2. *A nondegenerate quadratic form $f \in \mathbb{F}_q[x_1, \dots, x_n]$, q odd, $n \geq 3$, is equivalent to $x_1x_2 + g(x_3, \dots, x_n)$, where g is a nondegenerate quadratic form over $n-2$ indeterminates.*

Proof. First consider f in the form

$$f(x_1, x_2, \dots, x_n) = \sum_{1 \leq i \leq j \leq n} a_{ij} x_i x_j. \tag{7}$$

By Theorem 6.21 of [4], f is equivalent to a diagonal quadratic form in n indeterminates (given that f is non-degenerate). Thus, we can assume without loss of generality that f is diagonal. We will now show that f is equivalent to a quadratic form in which the coefficient of x_1^2 is 0. We write

$$f(x_1, x_2, \dots, x_n) = \sum_{1 \leq i \leq n} a_{ii} x_i^2. \tag{8}$$

Now we want to make a substitution of the form

$$\begin{aligned} x_2 &= rz_1 + z_2 \\ x_3 &= sz_1 + z_3 \text{ where } r, s \in \mathbb{F}_q \\ x_i &= z_i \text{ for } i \neq 2, 3 \end{aligned}$$

where r and s are to be determined. This yields the quadratic form

$$a_{22}(r^2z_1^2 + 2rz_1z_2 + z_2^2) + a_{11}z_1^2 + a_{33}(s^2z_1^2 + 2sz_1z_3 + z_3^2) + g_1(z_4, \dots, z_n)$$

The coefficient on z_1^2 is then equal to $a_{22}r^2 + a_{33}s^2 + a_{11}$. This gives us the nondegenerate quadratic form $h_1(r, s) = a_{22}r^2 + a_{33}s^2$, which we want equal to 0. To find solutions for r and s, solve $h_1(r, s) = -a_{11}$ over $\mathbb{F}_q^2$. By Theorem 6.26 of [4], the number of solutions to $h_1(r, s) = -a_{11}$ over $\mathbb{F}_q^2$ is

$$q + \nu(-a_{11})\eta\left(-\Delta\right) = q - \eta\left(-\Delta\right). \tag{9}$$

Note that $\Delta = \det A$, where A is the coefficient matrix of h_1. Now we can't have both r and s equal to 0 since $a_{11} \neq 0$ by assumption. Thus there exists at least one nontrivial solution for r and s such that the coefficient on z_1^2 is 0.

Now let f be as in (7) with $a_{11} = 0$ (the substitution above has already been applied so f is no longer diagonal). Since f is nondegenerate, not all a_{1j} can be 0, and so we may assume that $a_{12} \neq 0$. The nonsingular linear substitution

$$\begin{aligned} x_2 &= a_{12}^{-1}(y_2 - a_{13}y_3 - \cdots - a_{1n}y_n), \\ x_i &= y_i \text{ for } i \neq 2, \end{aligned}$$

transforms f into a quadratic form of the type

$$y_1y_2 + \sum_{2 \leq i \leq j \leq n} c_{ij} y_i y_j.$$

The nonsingular substitution

$$\begin{aligned} y_1 &= z_1 - c_{22}z_2 - c_{23}z_3 - \cdots - c_{2n}z_z \\ y_i &= z_i \text{ for } i \neq 1, \end{aligned}$$

then yields an equivalent quadratic form $z_1z_2 + g(z_3, \ldots, z_n)$, where g must clearly be nondegenerate.

□

The main result in Lemma 2 can be applied repeatedly to any quadratic form until only the last two indeterminates remain, x_{n-1} and x_n.

5.3. **Proving that the Three Types are Complete.** Here we present essentially an extension of a theorem contained in [4], since we cover the case when q is odd in addition to the q-even case. The main idea is to apply Lemma 2 repeatedly and then to consider the possible forms in the last two indeterminates. The q-even case relies on the following lemma. Its proof can be found in [4].

Lemma 3. *A nondegenerate quadratic form $f \in \mathbb{F}_q[x_1, \ldots, x_n]$, q even, $n \geq 3$, is equivalent to $x_1x_2 + g(x_3, \ldots, x_4)$, where g is a nondegenerate quadratic form over $\mathbb{F}_q$ in $n-2$ indeterminates.* [4]

Theorem 5. *If f is a quadratic form in n variables defined over $\mathbb{F}_q$, then f is equivalent to a nondegenerate quadratic form having order m, for some $0 \leq m \leq n$, of exactly one of the following types.*

1. $x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m$
2. $x_1x_2 + x_3x_4 + \cdots + x_{m-3}x_{m-2} + (\alpha_1 x_{m-1}^2 + \alpha_2 x_{m-1}x_m + \alpha_3 x_m^2), \alpha_i \in \mathbb{F}_q$
3. $x_1x_2 + x_2x_3 + \cdots + x_{m-2}x_{m-1} + ax_m^2, a \in \mathbb{F}_q^*$

Proof. If f is degenerate and has order $m < n$, then we can rewrite it as an equivalent nondegenerate quadratic form in m indeterminates. So we will assume that f is nondegenerate with m indeterminates. If m is odd, then using induction on m and Lemma 2 if q is odd, or Lemma 3 if q is even, one shows that f is equivalent to a quadratic form $x_1x_2 + x_3x_4 + \cdots + x_{m-2}x_{m-1} + ax_m^2$ with $a \in \mathbb{F}_q^*$. This is a quadratic form of type 3 from above, so we are done.

If m is even, then using induction on m and Lemma 2 for q odd, or Lemma 6.29 of [4] for q even, one shows that f is equivalent to a quadratic form of the type

$$x_1x_2 + x_3x_4 + \cdots + x_{m-3}x_{m-2} + \alpha_1 x_{m-1}^2 + \alpha_2 x_{m-1}x_m + \alpha_3 x_m^2 \tag{10}$$

If the quadratic in the last two indeterminates is irreducible over $\mathbb{F}_q$, then f is of type 2 and we are done. Otherwise, the quadratic $\alpha_1 x_{m-1}^2 + \alpha_2 x_{m-1}x_m + \alpha_3 x_m^2$ reduces to $(ax_{m-1} + cx_m)(bx_{m-1} + dx_m)$, in which case we make the substitution

$$\begin{aligned} y_{m-1} &= ax_{m-1} + cx_m \\ y_m &= bx_{m-1} + dx_m \\ y_i &= x_i \text{ for } i < m-1. \end{aligned}$$

This yields the equivalent quadratic form $y_1y_2 + y_3y_4 + \cdots + y_{m-3}y_{m-2} + y_{m-1}y_m$, which is of Type I.

□

5.4. **Example.** Consider the quadratic form $f(x_1, x_2, x_3) = x_1^2 + 2x_1x_3 + 3x_2^2 + x_2x_3 + x_3^2$ over the field $\mathbb{Z}_5$. It is easy to verify that this is a nondegenerate quadratic form by computing the determinate of its coefficient matrix. Using the method of section 4, we find that f is equivalent to

$$g_1(y_1, y_2, y_3) = 3y_1^2 + 2y_2^2 + y_3^2.$$

We now use the algorithm in the proof of Lemma 2 to find the substitution

$$\begin{aligned} x_1 &= z_1 \\ x_2 &= 2z_1 + z_2 \\ x_3 &= 2z_1 + z_3. \end{aligned}$$

This yields the equivalent quadratic form

$$g_2(z_1, z_2, z_3) = 3z_1z_2 + 4z_1z_3 + 2z_2^2 + z_3^2.$$

We now use the substitution (also obtained in the proof of Lemma 2)

$$\begin{aligned} z_1 &= t_1 \\ z_2 &= 2(t_2 - 4t_3) \\ z_3 &= t_3. \end{aligned}$$

Applying this gives yet another equivalent quadratic form:

$$g_3(t_1, t_2, t_3) = t_1t_2 + t_2t_3 + 3t_2^2 + 4t_3^2.$$

Finally, we apply the substitution

$$\begin{aligned} t_1 &= u_1 - 3u_2 - u_3 \\ t_2 &= u_2 \\ t_3 &= u_3, \end{aligned}$$

to get

$$g_4(u_1, u_2, u_3) = u_1u_2 + 4u_3^2.$$

According to Theorem 5, the quadratic form we have been working with is Type III.

6. The Number of Solutions of a Given Quadratic Form Equation

What separates a finite field with even order from one with odd order are two primary facets. First, the *characteristic* of any finite field with q even is 2, since $q = p^k$ for p prime is even if and only if $p = 2$. As was stated earlier, adding any element to itself yields 0, which means that every element is it's own additive inverse. The other interesting thing to consider is that $x^2 = a$ will always have a solution for $a \in \mathbb{F}_q$ when q is even. Observe that $a^q - a = 0 \Rightarrow a^q = a \Rightarrow (a^{q/2})^2 = a$. Note that since q is even, the element $a^{q/2}$ always makes sense because $q/2$ is an integer.

In an attempt to generalize things, I will cover both the q-odd and q-even cases when counting the number of solutions to a quadratic form equation. Before stating the theorem, it will be useful to consider the following lemmas; the proof of the first can be found in [4].

Lemma 4. *For odd q, let $b \in \mathbb{F}_q$, $a_1, a_2 \in \mathbb{F}_q^*$, and η be the quadratic character of $\mathbb{F}_q$. Then*

$$N(a_1x_1^2 + a_2x_2^2 = b) = q + \nu(b)\eta(-a_1a_2). \tag{11}$$

Lemma 5. *Given a finite field $\mathbb{F}_q$ and some element $b \in \mathbb{F}_q$,*

$$\sum_{c\in\mathbb{F}_q} \nu(c)\eta(b-c) = q\eta(b). \tag{12}$$

Proof. By definition, $\sum_{c\in\mathbb{F}_q} \eta(b-c) = 0$. Thus,

$$\begin{aligned}
\sum_{c\in\mathbb{F}_q} \nu(c)\eta(b-c) &= (q-1)\eta(b) + \sum_{c\in\mathbb{F}_q^*}(-1)\eta(b-c) \\
&= (q-1)\eta(b) - \sum_{c\in\mathbb{F}_q^*}\eta(b-c) \\
&= (q-1)\eta(b) - (0 - \eta(b-0)) \\
&= q\eta(b).
\end{aligned}$$

□

Lemma 6. *For any finite field $\mathbb{F}_q$ we have*

$$\sum_{c\in\mathbb{F}_q} \nu(c) = 0, \tag{13}$$

and for any $b \in \mathbb{F}_q$,

$$\sum_{c_1+\cdots+c_m=b} \nu(c_1)\cdots\nu(c_k) = \begin{cases} 0 & \text{if } 1 \le k \le m, \\ \nu(b)q^{m-1} & \text{if } k = m, \end{cases} \tag{14}$$

where the sum is over all $c_1, \ldots, c_m \in \mathbb{F}_q$ with $c_1 + \cdots + c_m = b$. [4]

The proof of this uses induction on m and fairly straightforward manipulations of sums.

Now we are ready to find the number of solutions to an arbitrary quadratic form equation.

Theorem 6. *Let $f(x_1, \ldots, x_n)$ be a quadratic form defined over $\mathbb{F}_q$ having order m, $1 \le m \le n$, and let $b \in \mathbb{F}_q$. Then, the number of solutions*

$$N(f(x_1,\ldots,x_n) = b) = \begin{cases} q^{n-m}(q^{m-1} + \nu(b)q^{\frac{m-2}{2}}) & \text{if } f \text{ is of Type 1} \\ q^{n-m}(q^{m-1} - \nu(b)q^{\frac{m-2}{2}}) & \text{if } f \text{ is of Type 2} \\ q^{n-m}(q^{m-1} + \eta(ab)q^{\frac{m-1}{2}}) & \text{if } f \text{ is of Type 3, } q \text{ odd} \\ q^{n-m}(q^{m-1}) & \text{if } f \text{ is of Type 3, } q \text{ even.} \end{cases} \tag{15}$$

6.1. **Type 1 Case.** *Proof.* We will assume that f has been reduced to a nondegenerate quadratic form in m indeterminates. Thus, there are $n-m$ free variables, which will simply introduce the multiplicative factor q^{n-m} to the number of solutions. First note that $N(x_1x_2 = b) = q-1$ if $b \neq 0$ and $N(x_1x_2 = b) = 2q-1$ if $b = 0$. In both cases, we can write $N(x_1x_2) = q + \nu(b)$. Recall that a Type I quadratic form looks like

$$x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m.$$

Now, if $m = 2k$, then

$$\begin{aligned} N(x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m = b) &= \sum_{c_1+\cdots+c_k=b} N(x_1x_2 = c_1)\cdots N(x_{m-1}x_m = c_k) \\ &= \sum_{c_1+\cdots+c_k=b} [q+\nu(c_1)]\cdots[q+\nu(c_k)]. \end{aligned}$$

By Lemma 6 the cross terms in the last sum go to zero, and so we have

$$\begin{aligned} N(x_1x_2 + x_3x_4 + \cdots + x_{m-1}x_m = b) &= \sum_{c_1+\cdots+c_k=b} q^k + \nu(c_1)\cdots\nu(c_k) \\ &= q^k \sum_{c_1+\cdots+c_k=b} 1 + \sum_{c_1+\cdots+c_k=b} \nu(c_1)\cdots\nu(c_k) \\ &= q^k q^{k-1} + \nu(b)q^{k-1} \\ &= q^{m-1} + \nu(b)q^{\frac{m-2}{2}}. \end{aligned}$$

This concludes the proof in the Type 1 case.

□

6.2. **Type 2 Case.** *Proof.* We consider the case that q is odd. The proof for even q is vaguely similar and can be seen in [4]. We will again assume that f has been reduced to an equivalent nondegenerate quadratic form g, where g is of Type 2 and has m indeterminates. There are thus $n-m$ free variables in f, which will introduce the multiplicative factor q^{n-m} to the number of solutions. Recall that for Type 2, $g(x_1,\ldots,x_m) = x_1x_2 + \cdots + x_{m-3}x_{m-2} + \alpha_1x_{m-1}^2 + \alpha_2x_{m-1}x_m + \alpha_3x_m^2$, where $\alpha_i \in \mathbb{F}_q$ and the quadratic in the last two indeterminates is irreducible. Carrying out the nonsingular substitution

$$\begin{aligned} y_i &= x_i \text{ for } 1 \leq i \leq m-2 \\ y_{m-1} &= x_{m-1} + \alpha_2(2\alpha_1)^{-1}x_m \\ y_m &= x_m, \end{aligned}$$

we get the equivalent quadratic form

$$h(y_1,\ldots,y_m) = y_1y_2 + \cdots + y_{m-3}y_{m-2} + \alpha_1y_{m-1}^2 + \left(\alpha_3 - \alpha_2^2(4\alpha_1)^{-1}\right)y_m^2. \tag{16}$$

Since m is even, we have $m = 2k$ for some $k \in \mathbb{Z}^+$. Moreover, for $c_1, \ldots, c_k \in \mathbb{F}_q$,

$$\begin{aligned} N(h(y_1,\ldots,y_m)=b) &= \sum_{c_1+\cdots+c_k=b} N(y_1y_2=c_1)\cdots N(y_{m-3}y_{m-2}=c_{k-1}) \\ &\qquad \cdot N\left(\alpha_1 y_{m-1}^2 + \left(\alpha_3 - \alpha_2^2(4\alpha_1)^{-1}\right) y_m^2 = c_k\right) \\ &= \sum_{c_1+\cdots+c_k=b} [q+\nu(c_1)]\cdots[q+\nu(c_{k-1})] \\ &\qquad \cdot [q+\nu(c_k)\eta\left(-\alpha_1\left(\alpha_3-\alpha_2^2(4\alpha_1)^{-1}\right)\right)] \\ &= \sum_{c_1+\cdots+c_k=b} q^k \\ &\quad + \sum_{c_1+\cdots+c_k=b} \nu(c_1)\cdots\nu(c_{k-1})\nu(c_k)\eta\left(-\alpha_1\alpha_3+\alpha_2^2(4)^{-1}\right) \\ &= q^k q^{k-1} + \eta\left(\alpha_2^2 - 4\alpha_1\alpha_3\right)\nu(b)q^{k-1}. \end{aligned}$$

We must now show that $\eta(\alpha_2^2 - 4\alpha_1\alpha_3) = -1$. Suppose that $\eta(\alpha_2^2 - 4\alpha_1\alpha_3) = 0$. Then by Lemma 4, $N(\alpha_1 y_{m-1}^2 + \left(\alpha_3 - \alpha_2^2(4\alpha_1)^{-1}\right) y_m^2 = 0) = q + \nu(0)(0) = q$. This contradicts the fact that $\alpha_1 y_{m-1}^2 + \left(\alpha_3 - \alpha_2^2(4\alpha_1)^{-1}\right) y_m^2$ is an irreducible quadratic. Now suppose that $\eta(\alpha_2^2 - 4\alpha_1\alpha_3) = 1$. Again, using Lemma 4 we have that $N(\alpha_1 y_{m-1}^2 + \left(\alpha_3 - \alpha_2^2(4\alpha_1)^{-1}\right) y_m^2 = 0) = q + \nu(0)(1) = 2q-1$, which gives the same contradiction. In the case that $\eta(\alpha_2^2 - 4\alpha_1\alpha_3) = -1$, we have $N(\alpha_1 y_{m-1}^2 + \left(\alpha_3 - \alpha_2^2(4\alpha_1)^{-1}\right) y_m^2 = 0) = q + \nu(0)(-1) = q-(q-1) = 1$. Therefore, our claim is true.

From this, we deduce the number of solutions to our equivalent quadratic form equation $h(y_1, \ldots, y_m) = b$ to be

$$N(h(y_1,\ldots,y_m)=b) = q^{2k-1} - \nu(b)q^{k-1} = q^{m-1} - \nu(b)q^{\frac{m-2}{2}}. \tag{17}$$

The number of solutions to the equation $f(x_1, \ldots, x_n) = b$ is thus

$$q^{n-m}\left(q^{m-1} - \nu(b)q^{\frac{m-2}{2}}\right).$$

□

6.3. **Type 3 Case.** *Proof.* We will assume that f has been reduced to a nondegenerate quadratic form in m indeterminates. Thus, there are $n-m$ free variables, which will simply introduce the multiplicative factor q^{n-m} to the number of solutions. Recall that $f(x_1, \ldots, x_m) = x_1x_2 + \cdots + x_{m-2}x_{m-1} + ax_m^2$ for some $a \in \mathbb{F}_q^*$. If q is even, there is always a unique solution to the equation $x^2 = c$ for $c \in \mathbb{F}_q$, namely $x = c^{q/2}$. Thus, we can choose x_1 through x_{m-1} independently and there will be a unique value of x_m such that $f(x_1, \cdots, x_m) = b$. Therefore,

$$N(f(x_1,\ldots,x_m)=b) = q^{m-1}.$$

For q odd, we explicitly write the number of solutions as

$$\begin{aligned}
&\sum_{c_1+c_2=b} N(x_1x_2+\cdots+x_{m-2}x_{m-1}=c_1)N(ax_m^2=c_2)\\
=&\sum_{c_1+c_2=b}(q^{m-2}+\nu(c_1)q^{\frac{m-3}{2}})(1+\eta(ac_2))\\
=&\sum_{c_1\in\mathbb{F}_q}(q^{m-2}+\nu(c_1)q^{\frac{m-3}{2}})(1+\eta(a(b-c_1)))\\
=&\sum_{c_1\in\mathbb{F}_q}\Big[q^{m-2}+q^{m-2}\eta(ab-ac_1)+\nu(c_1)q^{\frac{m-3}{2}}+q^{\frac{m-3}{2}}\nu(c_1)\eta(a)\eta(b-c_1)\Big]\\
=&\;q^{m-1}+q^{m-2}\sum_{c_1\in\mathbb{F}_q}\eta(ab-ac_1)+q^{\frac{m-3}{2}}\sum_{c_1\in\mathbb{F}_q}\nu(c_1)+q^{\frac{m-3}{2}}\eta(a)\sum_{c_1\in\mathbb{F}_q}\nu(c_1)\eta(b-c_1)\\
=&\;q^{m-1}+q^{\frac{m-3}{2}}\eta(a)\sum_{c_1\in\mathbb{F}_q}\nu(c_1)\eta(b-c_1)\\
=&\;q^{m-1}+q^{\frac{m-3}{2}}\eta(a)q\nu(b)\\
=&\;q^{m-1}+q^{\frac{m-1}{2}}\eta(ab).
\end{aligned}$$

The second to last step applied Lemma 5. This completes the proof.

□

7. Zeros of a Quadratic Form

Often times, we are interested in the solutions $(x_1,\ldots,x_n)\in\mathbb{F}_q^n$ to the equation $f(x_1,\ldots,x_n)=0$ where f is a quadratic form over $\mathbb{F}_q$. Such solutions are said to be **zeros** of f. Later on, we will see that subspaces of $\mathbb{F}_q^n$ can be generated from the zeros of f.

Using Theorem 6, it is easy to compute the number of zeros of any quadratic form f. If f is Type I and nondegenerate with n indeterminates, then it has $q^{n-1}+\nu(0)q^{\frac{n-2}{2}}=q^{n-1}+(q-1)q^{\frac{n-2}{2}}=q^{n-1}+q^{n/2}-q^{\frac{n-2}{2}}$ zeros. In general, the number of zeros of a quadratic form f of order m with n indeterminates is

$$\begin{array}{ll}
q^{n-m}(q^{m-1}+(q-1)q^{\frac{m-2}{2}}) & \text{if } f \text{ is of Type 1,}\\
q^{n-m}(q^{m-1}-(q-1)q^{\frac{m-2}{2}}) & \text{if } f \text{ is of Type 2,}\\
q^{n-m}(q^{m-1}-q^{\frac{m-1}{2}}) & \text{if } f \text{ is of Type 3, } q \text{ odd, and}\\
q^{n-m}(q^{m-1}) & \text{if } f \text{ is of Type 3, } q \text{ even.}
\end{array}\tag{18}$$

8. Finding the Size of the Maximal Subspace of Zeros

Recall that a vector space V is a set of elements defined under addition and scalar multiplication with a zero vector. Moreover, V is closed under these two operations. For a more complete definition, see [4] or [3]. A set $S\subset V$ is a subspace of V if it contains the zero vector and is closed under the two operations. The simplest example of a vector space is $\mathbb{R}^n$, which is the set of all n-tuples of real numbers. We can write such a vector as $(a_1,a_2,\ldots,a_n)$ where $a_i\in\mathbb{R}$ for $1\le i\le n$.

Thus, the zeros of an arbitrary quadratic form f defined over the field $\mathbb{F}$ are simply vectors in the vector space $\mathbb{F}^n$. It is also possible to construct subspaces of $\mathbb{F}^n$ using only these zeros. However, for large order quadratic forms, these subspaces become increasingly difficult to compute and validate.

Our ultimate goal in this section is to relate the size of the maximal subspaces of zeros for an arbitrary quadratic form f to its order and type. It is relatively straight forward to come up with a conjecture to this dependence. However, proving the size of the maximal subspaces is of considerable difficultly. For now, we start with some simple examples.

Consider the Type I quadratic form

$$x_1x_2 + x_3x_4 \text{ over } \mathbb{F}_3.$$

A vector space can be generated from the zeros $(1, 0, 1, 0)$ and $(1, 0, 0, 0)$. This vector space is actually a subspace of $\mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3 \oplus \mathbb{F}_3$. The main goal is to throw in as many zeros as we can while maintaining the property that every subspace element is a zero.

From the two vectors above, we generate the following subspace:

$$\{(0, 0, 0, 0), (1, 0, 1, 0), (2, 0, 2, 0), (1, 0, 0, 0), (2, 0, 0, 0),$$
$$(2, 0, 1, 0), (1, 0, 2, 0), (0, 0, 1, 0), (0, 0, 2, 0)\}.$$

Thus, drawing from a fairly simple example, it *seems* that the size of the maximal subspace of zeros for this quadratic form is 9. This leads us to make the following conjecture.

Conjecture 1. *If f is a Type I quadratic form over $\mathbb{F}_q$ with order n, then the size of its maximal subspace of zeros is given by $q^{\frac{n}{2}}$.*

Recall that a Type II quadratic form over a field $\mathbb{F}_q$ is written as $x_1x_2 + x_2x_3 + \cdots + x_{n-3}x_{n-2} + \alpha_1x_{n-1}^2 + \alpha_2x_{n-1}x_n + \alpha_3x_n^2$, where the quadratic in the last two indeterminates is irreducible. That is, there are no nontrivial zeros in $\mathbb{F}_q^2$ to the equation $\alpha_1x_{n-1}^2 + \alpha_2x_{n-1}x_n + \alpha_3x_n^2$.

Consider the Type II quadratic form $f(x_1, x_2, x_3, x_4) = x_1x_2 + 3x_3^2 + 2x_3x_4 + x_4^2$ over $\mathbb{Z}_5$. It is relatively tedious but straightforward to verify that the quadratic in the last two indeterminates is in fact irreducible. The 4-tuple $(1, 1, 2, 2)$ is a zero of f and generates the subspace

$$\{(0, 0, 0, 0), (1, 1, 2, 2), (2, 2, 4, 4), (3, 3, 1, 1), (4, 4, 3, 3)\}.$$

I was unable to find any other zeros that can be added to this set without violating closure under addition. Thus, it is my conjecture that 5 is the size of the maximal subspace. To make sense of this, consider that x_1x_2 is the only hyperplane of f, and so 5 is simply q to the power of the number of hyperplanes. That is, $5 = 5^{\frac{n-2}{2}} = 5^{\frac{n}{2}-1}$. For Type I quadratic forms, we ended up with essentially the same result except that the number of hyperplanes was given by $\frac{n}{2}$ instead of $\frac{n}{2} - 1$.

Conjecture 2. *If f is a Type II quadratic form over $\mathbb{F}_q$ with order n, then the size of its maximal subspace of zeros is given by $q^{\frac{n}{2}-1}$.*

Now consider the Type III quadratic form

$$x_1x_2 + x_3x_4 + 2x_5^2 \text{ over } \mathbb{F}_3.$$

Note that the last term can only take on the values 2 or 0. If we generate a subspace of zeros where $x_5 = 0$, we will get something very similar to the above example. Otherwise, suppose we start with the elements $(2, 1, 1, 2, 1)$ and $(0, 1, 0, 1, 0)$. This generates the subspace

$$\{(0,0,0,0,0),(0,1,0,1,0),(0,2,0,2,0),(2,1,1,2,1),$$
$$(1,2,2,1,2),(1,0,2,2,2),(2,0,1,1,1),(2,2,1,0,1),(1,1,2,0,2)\}.$$

Notice that this has size 9, which is equal to $3^{\frac{n-1}{2}}$.

Conjecture 3. *If f is a Type III quadratic form over $\mathbb{F}_q$ with order n, then the size of its maximal subspace of zeros is given by $q^{\frac{n-1}{2}}$.*

9. Conclusion

The theory of quadratic forms is heavily rooted in abstract algebra. As a result, many of the problems in the subject require a graduate level of mathematics to solve. In this paper, we primarily focused on defining quadratic forms exactly, classifying the three types a given form can assume, and proving some results for each type. Specifically, we looked at the number of solutions to the equation $f(x_1,\ldots,x_n)=b$ where f is a quadratic form in n indeterminates over the field $\mathbb{F}_q$. We also derived the number of zeros of f or the number of solutions to the equation $f(x_1,\ldots,x_n)=0$. Finally, we considered the maximally-sized subspaces that can be generated from the set of zeros of a quadratic form and produced conjectures for each type.

There still remains much to be learned of quadratic forms, and as stated earlier, many of these concepts would require a more advanced knowledge of abstract algebra. For example, one might ask how many unique maximally-sized subspaces can be generated from the zeros of f. In order to reasonably tackle this problem, I suggest looking at [5] closely. Additionally, it would be interesting to investigate higher degree polynomial equations such as quintic or quartic forms. How many zeros do they have and how would these results compare to those for quadratic forms? A paper on the nonsingular zeros of quintic forms over finite fields by David Leep, [1], could be a helpful starting point to analyze this problem. These questions and numerous others would be of particular interest to anyone diligently researching within the field.

References

[1] D.B. Leep, C. Yeomans, *Nonsingular zeros of quintic forms over finite fields*, Rocky Mountain J. Math., **26** (1996), *no.* 3, 1043-1055.

[2] I. Stewart, *Galois Theory*, Chapman & Hall, 1999.

[3] J. Gallian, *Contemporary Abstract Algebra*, Houghton Mifflin Company, 2001.

[4] R. Lidl, and H. Niederreiter, *Finite Fields*, 1-83, 191, 278-289, Cambridge University Press, 1997.

[5] T.Y. Lam, *Introduction to Quadratic Forms Over Fields*, AMS Publications, 2004.