7-2012

Strongly Real Conjugacy Classes of the Finite Unitary Group

Zach Gates
College of William and Mary

Strongly Real Conjugacy Classes of the Finite Unitary Group

A thesis submitted in partial fulfillment of the requirement
for the degree of Bachelor of Science in Mathematics from
The College of William and Mary

by

Zach Gates

Accepted for _____

_____

C. Ryan Vinroot, Director

_____

Gexin Yu

_____

Wouter Deconinck

Williamsburg, VA
May 1, 2012

Acknowledgements

I would first like to thank my adviser Professor Ryan Vinroot. It has been a pleasure working with him this year, and his guidance and enthusiasm for mathematics has been very helpful throughout. I would also like to thank my close friends and family for listening to me blather on about mathematics and pretending to care.

Abstract

An element g in a group G is real if there exists $x \in G$ such that $xgx^{-1} = g^{-1}$. It is considered strongly real if there exists such an x where $x^2 = 1$. It is true that all elements in the conjugacy class of g are real (strongly real) if g is real (strongly real). Gow and Vinroot [6] have given a sufficient condition for the strong reality of an element, say x, in the finite unitary group $\mathrm{U}(n, \mathbb{F}_{q^2})$ in terms of the elementary divisors of x. It follows from the work of Wall [8] and Ennola [3] that the strong reality of x actually depends only on the strong reality of the unipotent part of x. We examine the strong reality of unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$, q odd, and we provide a method for reducing the powers of elementary divisors into a form that is easier to examine. This reduces the question of whether the sufficient condition given in [6] is also a necessary condition to unipotent classes with elementary divisors of the form $(t-1)^k$, for $k \geq 2$. Then we show that any $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ is strongly real if the elementary divisor $(t-1)^k$, where k is the highest even power of $(t-1)$ in the list of divisors, appears with multiplicity one. We also obtain partial results for q even and some applications to classes of the finite symplectic group for q odd.

Contents

Chapter 1

Introduction

Consider a group G. Then an element $g \in G$ is a *real* element of G if there exists an element $x \in G$ such that $xgx^{-1} = g^{-1}$. That is, g is real if it can be conjugated to its inverse by some element of the group. An element g is *strongly real* if there exists an *involution* $t \in G$, that is, an element with the property $t^2 = 1$, such that $tgt^{-1} = g^{-1}$. We show now that if g is real, then every element in the conjugacy class of g, $c.c.(g)$, is also real. Therefore we can talk about the real conjugacy classes of the group. It is also the case that all elements in the conjugacy class of a strongly real element are strongly real so we can talk about strongly real conjugacy classes as well.

Lemma 1.1. *Let G be a group. If $g \in G$ is real, then every element in its conjugacy class $c.c.(g)$ is also real. Furthermore, if $h \in G$ is strongly real, then every element in its conjugacy class $c.c.(h)$ is also strongly real.*

Proof. Consider the element $xgx^{-1} \in c.c.(g)$. Since $xgx^{-1} \in c.c.(g)$, it is conjugate to g. Since g is real, g is conjugate to its inverse g^{-1} by some $y \in G$. That is, $ygy^{-1} = g^{-1}$. Then we conjugate xgx^{-1} by xyx^{-1}, and $(xyx^{-1})(xgx^{-1})(xyx^{-1})^{-1} = xygy^1x^{-1} = xg^{-1}x^{-1} = (xgx^{-1})^{-1}$ so xgx^{-1} is real and thus all elements in $c.c.(g)$ are real.
Let h be a strongly real element of the group G so $tht^{-1} = h^{-1}$ for some t in G where $t^2 = 1$. Now consider the element xtx^{-1} where x is any element in G. We see that $(xtx^{-1})^2 = (xtx^{-1})(xtx^{-1}) = 1$ so xtx^{-1} is an involution. Then any element of the conjugacy class of h can be written xhx^{-1} and $(xtx^{-1})(xhx^{-1})(xtx^{-1}) = xthtx^{-1} = xh^{-1}x^{-1} = (xhx^{-1})^{-1}$. Thus we have conjugated xhx^{-1} to its inverse by an involution so all elements of $c.c.(h)$ are strongly real. □

An equivalent statement to saying that g is strongly real is to say that g is a product of two involutions. Indeed, let $s, t \in G$ such that $s^2 = t^2 = 1$. Let $g = st$. Then $g^{-1} = ts$ so $sgs = s^2ts = ts = g^{-1}$. Now let $sgs = g^{-1}$. Then $g = sg^{-1}s$

where $s^2 = 1$ and $(g^{-1}s)^2 = g^{-1}sg^{-1}s = 1$, so g is a product of two involutions.

It is not true in general that all real elements of a group are also strongly real. We will see this later when we examine the finite unitary group, which we will define and discuss in Section 2.3. However, there are groups where all real elements are strongly real. For example, it is true that all real elements are also strongly real in S_n, the group of permutations on n elements. In fact, all elements are real so all elements are strongly real.

Proposition 1.2. *All elements of S_n are strongly real.*

Proof. We know in S_n that all conjugacy classes are determined by cycle types. For instance, consider $\sigma \in S_n$. Then σ can be written as a product of disjoint cycles, say of lengths $k_1, k_2, \ldots, k_l$. Then we consider σ to have cycle type $(k_1, k_2, \ldots, k_l)$, and then any conjugate of σ has cycle type $(k_1, k_2, \ldots, k_l)$. Also, if $\rho \in S_n$ has cycle type $(k_1, k_2, \ldots, k_l)$, then σ is conjugate to ρ. Consider a single k-cycle $\beta = (a_1 a_2 a_3 \cdots a_k) \in S_n$. Its inverse can be written $\beta^{-1} = (a_k a_{k-1} a_{k-2} \cdots a_1)$. Also it is a fact that for any $\sigma \in S_n$, $\sigma(a_1 a_2 \cdots a_k)\sigma^{-1} = (\sigma(a_1)\sigma(a_2)\cdots\sigma(a_k))$. Then we define

$$\sigma_\beta = \begin{cases} (a_1\ a_k)(a_2\ a_{k-1})\cdots(a_{k/2}\ a_{k/2+1}) & \text{if } k \text{ is even} \\ (a_1\ a_k)(a_2\ a_{k-1})\cdots(a_{(k-1)/2}\ a_{(k+3)/2}) & \text{if } k \text{ is odd} \end{cases}$$

Then σ_β is a product of disjoint cycles which commute and is also an involution. By construction, we have $\sigma_\beta \beta \sigma_\beta^{-1} = (\sigma_\beta(a_1)\cdots\sigma_\beta(a_k)) = (a_k \cdots a_1) = \beta^{-1}$. Then for any $\alpha \in S_n$ with $\alpha = \beta_1\beta_2\cdots\beta_m$, a product of disjoint cycles β_i, let $\tau = \sigma_{\beta_1}\sigma_{\beta_2}\cdots\sigma_{\beta_m}$. Since the β_i are disjoint, then so are the σ_{β_i}. Therefore, $\tau^2 = \sigma_{\beta_1}^2 \cdots \sigma_{\beta_m}^2 = (1)$, so τ is an involution. Thus we have $\tau\alpha\tau^{-1} = \alpha^{-1}$ where τ is an involution so α is strongly real. □

The problem we will be examining is to describe exactly which conjugacy classes of $\mathrm{U}(n, \mathbb{F}_{q^2})$, the finite unitary group, are strongly real. We will formally describe the finite unitary group later, but we define the group $\mathrm{U}(n, \mathbb{F}_{q^2}) = \{A \in \mathrm{GL}(n, \mathbb{F}_{q^2}) : {}^tA^{-1} = \bar{A}\}$, that is, all $n \times n$ invertible matrices with entries from the finite field with q^2 elements, denoted $\mathbb{F}_{q^2}$, such that the inverse-transpose of the matrix is equal to the conjugate of the matrix, where, in this case, by taking the conjugate we mean raising each entry to the qth power. We already have a sufficient condition from Vinroot and Gow [6] for when an element is strongly real. Our conjecture is that this is also necessary.

We will first state our conjecture before introducing the groups with which we will be working. Then we will present bilinear forms and Hermitian forms. Next we give the necessary background on how conjugacy classes are parameterized in these

groups. Finally, we will begin our work on the conjecture itself. The conjecture is stated in terms of elementary divisors, which we will define and discuss in Section 3.1. Here is the conjecture:

Conjecture 1.3. *Let x be a real element in $\mathrm{U}(n, \mathbb{F}_{q^2})$. Then x is strongly real if and only if:*
(a) q is odd and each elementary divisor of x of the form $(t \pm 1)^{2m}$ occurs with even multiplicity;
(b) q is even, n is even, and each elementary divisor of x of the form $(t+1)^{2m+1}$ occurs with even multiplicity.

In this paper, we will focus mostly on the case of q odd before considering the case of q even. We know from Vinroot and Gow[6, Proposition 5.2] that if (a) or (b) are true, then x is strongly real. We believe that these are indeed the only cases that x is strongly real.

We proceed by giving background information on the linear groups that we will be examining as well as background on elementary divisors. We will then look at a proof that regular unipotent elements in the finite unitary group are not strongly real[6, Proposition 5.1]. This allows us to derive our strategy for looking at any unipotent elements in the finite unitary group. Next we provide a process to reduce the powers of $(t-1)$ appearing in the list of elementary divisors of a unipotent element so that we are left with the case where only divisors of the form $(t-1)^2$ and $(t-1)$ appear, which becomes our base case when q is odd. We then show that an element of the finite unitary group is not strongly real when it has elementary divisors $(t-1)^2$ with multiplicity one and $(t-1)$ with any multiplicity. Then, if the highest even power of $(t-1)$ appears with multiplicity one in the list of elementary divisors of $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$, then x is not strongly real. In particular, these results reduce Conjecture 1.3 to the case that the only elementary divisors which appear are $(t-1)^2$ and $t-1$, in the case that q is odd, or $(t-1)^3$, $(t-1)^2$, and $t-1$ in the case that q is even. We then take a brief look at the case where we have multiplicity of $(t-1)^2$ greater than 1 and also at the case where q is even. Lastly, we are able to use our results to make a statement about the strong reality of some elements in the finite symplectic group.

Chapter 2

Classical Groups and Bilinear Forms

2.1 The General Linear Group

Consider any field F and let V be an n-dimensional vector space over F. Then the general linear group of V, denoted $\mathrm{GL}(V)$, is the group of all invertible linear transformations from V to V. By choosing any basis in V, we provide an isomorphism between $\mathrm{GL}(V)$ and $\mathrm{GL}(n, F)$, the group of all $n \times n$ invertible matrices with entries in F, since any linear transformation from V to V can be represented by an $n \times n$ matrix given a basis.

Another important linear group is $\mathrm{SL}(V)$, the subgroup of $\mathrm{GL}(V)$ defined $\mathrm{SL}(V) = \{\tau \in \mathrm{GL}(V) | \det \tau = 1\}$. This allows us to define $\mathrm{SL}(n, F)$ as the group of all $n \times n$ invertible matrices with determinant 1.

2.2 Bilinear Forms

In this section we will introduce the idea of bilinear forms over a vector space, specifically non-degenerate bilinear forms. The study of bilinear forms and sesquilinear forms will allow us to define the unitary group as well as the symplectic group. In fact, these groups are determined by certain types of these forms which create a type of geometry and structure in a vector space. All of these groups are subgroups of the general linear group.

Definition 2.1. Let F be any field and V be a vector space over F. Then a *bilinear*

form on V is a function $B : V \times V \to F$ that is linear in both terms. That is,

$$B(u+v,w) = B(u,w) + B(v,w) \quad \text{and} \quad B(au,w) = aB(u,w);$$
$$B(u,v+w) = B(u,v) + B(u,w) \quad \text{and} \quad B(u,aw) = aB(u,w)$$

for all $u, v, w \in V$ and all $a \in F$.

Definition 2.2. A bilinear form is said to be *non-degenerate* if $B(v,w) = 0$ for all $v \in V$ if and only if $w = 0$.

With these definitions in mind, we can look at specific types of bilinear forms and sesquilinear forms (which we will define) to define the unitary and symplectic groups.

2.3 Hermitian Forms and the Unitary Group

To define a Hermitian form and then the unitary group, we must first have a degree 2 extension field of our initial field F. We can extend a field F by considering the field $F[x]/(p(x))$ where $p(x) \in F[x]$ is a degree 2 irreducible polynomial and $(p(x))$ is the ideal generated by $p(x)$. That is, we take the quotient of $F[x]$ by the ideal generated by a degree 2 irreducible polynomial to obtain a larger field containing F. This extension is indeed a field since the ideal generated by an irreducible polynomial is a maximal ideal so the quotient is a field. An example of an extension field is $\mathbb{C}$ over $\mathbb{R}$. This is a degree 2 extension or quadratic extension since $\mathbb{C} \cong \mathbb{R}/(x^2+1)$. Note that x^2+1 has no real roots, but it does have the roots i and $-i$, where $i^2 = -1$, of multiplicity 2. We can actually look at $\mathbb{C}$ as $\mathbb{R}$ adjoining the element i so all elements in $\mathbb{C}$ can be written $a + bi$ where $a, b \in \mathbb{R}$.

Definition 2.3. An *automorphism* on the extension field E over F, denoted E/F, is an isomorphism α from E to E that fixes F pointwise.

In the case of a quadratic extension, there exist only two distinct automorphisms, one being the trivial automorphism which fixes every element of E. The other automorphism α is of order 2 so $\alpha^2 = 1$. We again look at $\mathbb{C}$ over $\mathbb{R}$ for our example. This is a degree 2 extension. There exists of course the trivial automorphism which fixes all of $\mathbb{C}$. Then we have the automorphism of complex conjugation $\alpha : \mathbb{C} \to \mathbb{C}$ such that $\alpha(a+bi) = a - bi$, written $a \bar{+} bi$. Observe that $\alpha^2 = 1$. In general we will write this order 2 automorphism as α and say $\alpha(a) = \bar{a}$ for any $a \in F$.
Now we will define first a sesquilinear form and then a Hermitian form:

Definition 2.4. Let E/F be a degree 2 extension of fields, and let α be the unique nontrivial automorphism of E/F. For any $a \in E$, denote $\alpha(a) = \bar{a}$. Let V be a vector space of dimension n over E. Then $B : V \times V \to E$ is a *sesquilinear form on* V if:

(1) $B(u+v, w) = B(u, w) + B(v, w)$,

(2) $B(u, v+w) = B(u, v) + B(u, w)$, and

(3) $B(au, v) = aB(u, v) = B(u, \bar{a}v)$

for all $u, v, w \in V$ and all $a \in E$. If, in addition, the form satisfies

(4) $B(u, v) = \overline{B(v, u)}$

for all $u, v \in V$, then B is a *Hermitian bilinear form.*

Now that we have defined a Hermitian bilinear form, we are able to define a unitary space and then the unitary group.

Definition 2.5. If V is a vector space over E/F with a non-degenerate Hermitian form H with respect to E/F, then V is called a *unitary space* over E/F.

Definition 2.6. Let V be a unitary space over E/F. Then an invertible linear transformation τ such that $H(\tau u, \tau v) = H(u, v)$ for all $u, v \in V$ is an isometry of the Hermitian form H and is called a *unitary transformation.* The group of unitary transformations is the *unitary group*, defined $\mathrm{U}(V) = \{\tau \in \mathrm{GL}(V) : H(\tau u, \tau v) = H(u, v)$, all $u, v \in V\}$.

We define $\mathrm{U}(n, E) = \{A \in \mathrm{GL}(n, E) : {}^tA^{-1} = \bar{A}\}$.The unitary group $\mathrm{U}(V)$ is isomorphic to $\mathrm{U}(n, E)$, the group of $n \times n$ unitary matrices, upon choosing a basis for V. Also, if a basis is chosen in V, and $\tau \in \mathrm{GL}(V)$ is represented by the matrix T, then $\tau \in \mathrm{U}(V)$ if and only if $T^t\hat{H}\bar{T} = \hat{H}$ where $\hat{H}$ is the $n \times n$ matrix representing the Hermitian form H. Furthermore, there is a subgroup of the unitary group called the *special unitary group*, denoted $\mathrm{SU}(V) \cong \mathrm{SU}(n, F))$ which is defined analogously to $\mathrm{SL}(V)$ and $\mathrm{SL}(n, E)$. The group $\mathrm{SU}(V)$ is the group of unitary transformations with determinant 1, and $\mathrm{SU}(n, E)$ is the group of unitary matrices with determinant 1. Later in this chapter, we will discuss specifically the unitary group over a finite field after a brief introduction to finite fields.
First, however, we will show an example of a matrix of a Hermitian form and then a unitary matrix.

Example 2.7. Let H be our Hermitian form on $\mathbb{C}^2$, a 2-dimensional vector space over $\mathbb{C}$. In this case, a common Hermitian form would be H with the matrix $\hat{H} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Given vectors $u = [x_1\ x_2]^t$ and $v = [y_1\ y_2]^t$ in $\mathbb{C}^2$, $H(u,v) = {}^t\bar{u}Hv$. Any invertible matrix $A \in \mathrm{U}(2,\mathbb{C})$ must satisfy ${}^tA\hat{H}\bar{A} = \hat{H}$. Let $A = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$. Then ${}^tA = \begin{pmatrix} 1 & 0 \\ i & 1 \end{pmatrix}$ and $\bar{A} = \begin{pmatrix} 1 & -i \\ 0 & 1 \end{pmatrix}$ so, with some brief calculations, we see that $A \in \mathrm{U}(2,\mathbb{C})$.

2.4 The Symplectic Group

Let B be a bilinear form on the vector space V. Then B is a *symmetric bilinear form* if $B(v,w) = B(w,v)$ for all $v, w \in V$. We say that B is an *alternating form* if $B(v,v) = 0$ for all $v \in V$. In this case, B is also called a *symplectic* or *skew-symmetric* form since $B(v,w) = -B(w,v)$ for all $v, w \in V$. This is true since

$$\begin{aligned} 0 &= B(v+w, v+w) \\ &= B(v,v) + B(v,w) + B(w,v) + B(w,w) \\ &= B(v,w) + B(w,v) \end{aligned}$$

so $B(v,w) = -B(w,v)$ for all $v, w \in V$.
Note that if we are in characteristic 2, then an alternating form and skew-symmetric form are different since skew-symmetric and symmetric are the same in characteristic 2. Now that we have defined an alternating form, we can define the symplectic group.

Definition 2.8. Let V be a vector space of dimension $n = 2m$ over a field F and let B be a non-degenerate alternating form on V. Then an invertible linear transformation τ is *symplectic* if $B(\tau v, \tau w) = B(v,w)$ for all $v, w \in V$, that is, if τ is an isometry of the alternating form B. The group of all symplectic transformations of B is the *symplectic group* denoted $\mathrm{Sp}(V)$.

We define $\mathrm{Sp}(2m,F)$ to be the group of $2m \times 2m$ invertible matrices A such that $A^t\hat{B}A = \hat{B}$ where $\hat{B}$ is the skew-symmetric matrix of our form B. Again, if we choose a basis in V then $\mathrm{Sp}(V) \cong \mathrm{Sp}(2m,F)$. Note here that the symplectic group is not actually dependent on the choice of our alternating form B. Indeed, it is a result of linear algebra (see [8, Theorem 2.10]) that any other non-degenerate alternating form, say $\tilde{B}$ on V, must be equivalent to B. That is, there exists bases

of V such that $\hat{B} = \hat{\tilde{B}}$ where these are the respective matrices for B and $\tilde{B}$. Then the symplectic group here is unique up to isomorphism.

Example 2.9. Here is an example of a matrix $\hat{B}$ for a symplectic form B on $\mathbb{R}^2$, a 2-dimensional vector space over $\mathbb{R}$:

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

An invertible matrix $A \in \mathrm{Sp}(2, \mathbb{R})$ if and only if $A^t \hat{B} A = \hat{B}$. For example, let $A = \begin{pmatrix} 2 & 7 \\ 1 & 4 \end{pmatrix}$. Then we can see by quick calculations that $A \in \mathrm{Sp}(2, \mathbb{R})$. This is also true since it is known that $\mathrm{Sp}(2, F) = \mathrm{SL}(2, F)$ for any field F. Since our matrix A has $det(A) = 1$ and A is invertible, A is symplectic.

Generally, we may choose the matrix for an alternating form B over any field to be $B = \begin{pmatrix} & I_m \\ -I_m & \end{pmatrix}$, where I_m is the $m \times m$ identity matrix.

2.5 Finite Fields

A *finite field* is a field F of finite order. It is a fact that any finite field must have $q = p^n$ elements for some prime p and some integer $n \geq 1$. Consider, for example, the field $\mathbb{Z}/p\mathbb{Z}$ for any prime p. This is a field, and it has finite order p.

It is an important fact that we have uniqueness of finite fields. Let E_1, E_2 be finite fields where $|E_1| = |E_2| = p^n$ for some prime p and positive integer n. Then:

(i) If E_1 and E_2 are both subfields of the same field K, then $E_1 = E_2$.

(ii) $E_1 \cong E_2$.

We typically denote the finite field with $q = p^n$ elements by $\mathbb{F}_q$.

Given the finite field $\mathbb{F}_q$, there is a quadratic extension field $\mathbb{F}_{q^2}/\mathbb{F}_q$. This extension $\mathbb{F}_{q^2}$ has q^2 elements and also has a unique nontrivial automorphism α such that $\alpha(a) = a^q$ for any $a \in \mathbb{F}_{q^2}$. Now we define the finite unitary group, which will be our main interest, and we will show that there is indeed only one unitary group over a given finite field. We define $\mathrm{U}(n, \mathbb{F}_{q^2}) = \{h \in \mathrm{GL}(n, \mathbb{F}_{q^2}) : {}^t h^{-1} = \bar{h}\}$, where, in this case, our Hermitian form is defined by I_n. Now before we can prove that there is only one unitary group, we must state a theorem that we will employ in our proof. This the Lang-Steinberg Theorem[1, Theorem 3.10] which we will state only for the finite general linear group over $\bar{\mathbb{F}}_q$, an algebraic closure of the finite field $\mathbb{F}_q$ (see [2, Section 13.4]). Fixing our extension $\mathbb{F}_{q^2}$, we can find an algebraic closure of $\mathbb{F}_q$ which contains $\mathbb{F}_{q^2}$ so looking at $\bar{\mathbb{F}}_q$ will suffice.

Theorem 2.10 (Lang-Steinberg)**.** *Let* $\boldsymbol{G} = \mathrm{GL}(n, \bar{\mathbb{F}}_q)$ *and let* $\boldsymbol{F}$ *be a surjective endomorphism of* $\boldsymbol{G}$ *with a finite number of fixed points. Then the map* $\mathcal{L} : \mathbf{G} \to \mathbf{G}$ *given by* $\mathcal{L}(g) = g^{-1}\mathbf{F}(g)$ *is surjective.*

We will now employ this theorem to show that the finite unitary group is unique up to isomorphism.

Proposition 2.11. *Let* V *be an* n*-dimensional vector space over* $\mathbb{F}_{q^2}$ *on which we can define a Hermitian form. Then the unitary group* $U(V)$ *with respect to the Hermitian form is isomorphic to* $U(n, \mathbb{F}_{q^2})$*.*

Proof. Suppose J is an invertible Hermitian matrix with entries in $\mathbb{F}_{q^2}$, so ${}^tJ = \bar{J}$. Also, note that I, the $n \times n$ identity matrix, is an invertible Hermitian matrix over $\mathbb{F}_{q^2}$. Both J and I provide non-degenerate Hermitian forms on V, an n-dimensional vector space over $\mathbb{F}_{q^2}$. Let $G = \{g \in \mathrm{GL}(n, \mathbb{F}_{q^2}) | {}^t\bar{g}Jg = J\}$. Let $H = \mathrm{U}(n, \mathbb{F}_{q^2}) = \{h \in \mathrm{GL}(n, \mathbb{F}_{q^2}) | {}^t\bar{h}h = I\}$. We will show that G and H are isomorphic and thus that there is a unique finite unitary group up to isomorphism since the elements of G are the elements of the unitary group corresponding to the Hermitian form J, and the elements of H are the elements of the unitary group corresponding to the Hermitian form I. We can apply the Lang-Steinberg Theorem here where $\mathbf{F}(g) = {}^t\bar{g}^{-1}$ is our surjective endomorphism. We know that there are a finite number of fixed points because the fixed points of this map are the elements in the unitary group, and we are dealing with the finite unitary group in this case. Therefore, there must be a finite number of fixed points. Then we have the Lang map $\mathcal{L} : \mathbf{G} \to \mathbf{G}$ defined by $\mathcal{L}(g) = g^{-1t}\bar{g}^{-1}$, which is surjective by the Lang-Steinberg Theorem. We know that the inverse map is also surjective so we can compose $\mathcal{L}$ with the inverse map to obtain $\tilde{\mathcal{L}}$ which sends g to ${}^t\bar{g}g$, which is also a surjective map. Since this is a surjective map, we know that there exists some $x \in \mathbf{G}$ such that $\tilde{\mathcal{L}}(x) = J$. That is, $J = {}^t\bar{x}x$. Now consider any $g \in G$ so ${}^t\bar{g}Jg = J$. We substitute for J and obtain ${}^t\bar{g}{}^t\bar{x}xg = {}^t\bar{x}x$. Then ${}^t\bar{x}^{-1}{}^t\bar{g}{}^t\bar{x} = xg^{-1}x^{-1} = (xgx^{-1})^{-1}$. Then, taking the inverse of both sides, we see that $xgx^{-1} = {}^t\bar{x}^{-1}{}^t\bar{g}^{-1}{}^t\bar{x} = {}^t\bar{xg\bar{x}}^{-1}$. Therefore, for any $g \in G$, we see that $xgx^{-1} \in H$. Since x conjugates elements of G to elements of H, G and H are isomorphic, and thus all unitary groups over $\mathbb{F}_{q^2}/\mathbb{F}_q$ are isomorphic to $U(n, \mathbb{F}_{q^2})$. □

Chapter 3

Real Conjugacy Classes of $\mathrm{GL}(n, \mathbb{F}_q)$ and $\mathrm{U}(n, \mathbb{F}_{q^2})$

3.1 Elementary Divisors and Rational Canonical Form

In this section we will introduce modules, specifically modules over principal ideal domains, which will allow us to define an element of a group by its action on a vector space by its elementary divisors.

Definition 3.1. Let R be a ring (not necessarily commutative nor with 1). Then a *left R-module* is a set M together with

(1) a binary operation $+$ on M under which M is an abelian group, and

(2) an action of R on M denoted by rm, for all $r \in R$ and for all $m \in M$ which satisfies

   (a) $(r+s)m = rm + sm$, for all r,$s \in R$, $m \in M$,

   (b) $(rs)m = r(sm)$, for all r,$s \in R$, $m \in M$, and

   (c) $r(m+n) = rm + rn$, for all $r \in R$, m,$n \in M$
   If the ring R has a 1 we impose the additional axiom:

   (d) $1m = m$, for all $m \in M$.

Note that a module over a field F is the same as a vector space over F.
We now provide a relevant example of a module. Let F be a field and let t be an indeterminate. Let R be the polynomial ring $F[t]$. Let V be a vector space over F and let T be a linear transformation from V to V. We can use the linear map T to

make V into an $F[t]$-module. We can define by composition $T^0 = I$, $T^1 = T$, ..., $T^n = \overbrace{T \circ T \circ \cdots \circ T}^{n \text{ times}}$. where I is the identity map from V to V. Also, for any two linear transformations A, B from V to V and elements α, $\beta \in F$, let $\alpha A + \beta B$ be defined by $(\alpha A + \beta B)(v) = \alpha(A(v)) + \beta(B(v))$ for any $v \in V$.
Now we define the action of any polynomial in the indeterminate t on V. Let $p(t) = a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0$, where $a_0, a_1, \ldots, a_n \in F$. Then for each $v \in V$, we define the action of the polynomial $p(t) \in F[t]$ on v by

$$\begin{aligned} p(t)v &= (a_n T^n + a_{n-1} T^{n-1} + \cdots + a_1 T + a_0)(v) \\ &= a_n T^n(v) + a_{n-1} T^{n-1}(v) + \cdots + a_1 T(v) + a_0 v. \end{aligned}$$

That is, we replace the indeterminate t in $p(t)$ with the linear transformation T. This action of $F[t]$ on V makes V into an $F[t]$-module.

Before we discuss elementary divisors, we must first define a few terms.

Definition 3.2. A *principal ideal domain*, or PID, is an integral domain in which every ideal is a principal ideal. That is, every ideal is generated by one element in a PID.

Definition 3.3. A *unique factorization domain*, or UFD, is an integral domain R in which every nonzero element $r \in R$ which is not a unit has the following properties:

(i) r can be written as a finite product of irreducibles p_i of R (not necessarily distinct): $r = p_1 p_2 \cdots p_n$ and

(ii) the decomposition in (i) is unique up to associates. That is, if $r = q_1 q_2 \cdots q_m$ is another factorization of r into irreducibles, then $m = n$ and there is some renumbering of the factors such that p_i is associate to q_i for $i = 1, 2, \ldots, n$, i.e. $p_i = u_i q_i$ where u_i is a unit for all i.

Definition 3.4. The *torsion submodule*, $\mathrm{Tor}(M)$, of an R-module M is defined $\mathrm{Tor}(M) = \{m \in M | rm = 0 \text{ for some nonzero } r \in R\}$.

Definition 3.5. If N is a submodule of M, then the *annihilator of N in R* is defined to be $\{r \in R | rn = 0 \text{ for all } n \in N\}$.

Furthermore, a module M is *torsion free* if $\mathrm{Tor}(M) = \{0\}$, and an R-module M is a *free* module if with generator $A \subseteq M$ if for every nonzero $x \in M$, there exist unique $r_1, r_2, \ldots, r_n$ of R and unique $a_1, a_2, \ldots, a_n$ in A such that $x = r_1 a_1 + r_2 a_2 + \cdots + r_n a_n$, for some positive integer n. Then A

is a basis or set of free generators for M. Also, this form is unique. That is, if two finitely generated R-modules M_1 and M_2 are isomorphic if and only if they have the same free rank(in this case r in (1)) and same list of invariant factors.

Now we consider modules over principal ideal domains, which provides especially nice and useful structure. This is the Fundamental Theorem of Finitely Generated Modules over a PID. We will state this theorem in two forms, first in invariant factor form and next in elementary divisor form. This theorem actually proves the Fundamental Theorem of Finitely Generated Abelian Groups if we consider $\mathbb{Z}$ as our PID. We will state our theorem without proof although the statement of these theorems with full proofs can be found in Dummit and Foote [2, Section 12.1].

Theorem 3.6 (Fundamental Theorem of Finitely Generated Modules over PIDs: Invariant Factor Form)**.** *Let R be a PID and let M be a finitely generated R-module.*

(1) Then M is isomorphic to the direct sum of finitely many cyclic modules. More precisely

$$M \cong R^r \oplus R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$$

for some integer $r \geq 0$ and nonzero elements $a_1, a_2, \ldots, a_m$ of R which are not units in R and which satisfy the divisibility relations $a_1|a_2|\cdots|a_m$.

(2) M is torsion free if and only if M is free.

(3) In the decomposition in (1), Tor(M) $\cong R/(a_1) \oplus R/(a_2) \oplus \cdots \oplus R/(a_m)$.

Note here that M is a torsion module if and only if $r = 0$ and the annihilator of M is the ideal (a_m).

It is true that a PID is also a UFD, and thus for any nonzero $a \in R$ where R is a PID can be written $a = up_1^{\alpha_1}p_2^{\alpha_2}\cdots p_s^{\alpha_s}$ where each p_i is a distinct irreducible and u is a unit. This factorization is unique up to units by the definition of a UFD. We are now able to state the theorem in elementary divisor form.

Theorem 3.7 (Fundamental Theorem of Finitely Generated Modules over PIDs: Elementary Divisor Form)**.** *Let R be a PID and let M be a finitely generated R-module. Then M is the direct sum of a finite number of cyclic modules whose annihilators are either (0) or generated by powers of irreducibles in R. That is,*

$$M \cong R^r \oplus R/(p_1^{\alpha_1}) \oplus R/(p_2^{\alpha_2}) \oplus \cdots \oplus R/(p_s^{\alpha_s}) \tag{3.1}$$

where $r \geq 0$ is an integer and $p_1^{\alpha_1}, p_2^{\alpha_2}, \ldots, p_t^{\alpha_s}$ are positive powers of irreducibles in R, not necessarily distinct.

Now we are able to proceed and discuss how we are able to employ these elementary divisors. Let V be a finite-dimensional vector space of dimension n over any field F, and let $T : V \to V$ be any linear transformation on V. Then V is an $F[t]$-module through the action of T by our earlier example. Since V has finite dimension over F, it is finitely generated as an F-module and therefore also finitely generated as an $F[t]$-module. Also it must be a torsion $F[t]$-module so, by our theorem, V is a direct sum of cyclic torsion $F[t]$-modules. We can choose a basis for V using this decomposition such that the matrix for the transformation T is in a simple form.

This desired form is the *Jordan canonical form* which is the matrix as close as possible to a diagonal matrix for T. First assume that F is algebraically closed so all invariant factors in the decomposition of V, say $a_1(t), \ldots, a_n(t)$ factor into linear factors of the form $(t-\alpha)^k$ where these $(t-\alpha)^k$ are the elementary divisors and the product of these elementary divisors is the characteristic polynomial of the transformation T. Then we obtain V as the direct sum of finitely many cyclic $F[x]$-modules of the form $F[t]/(t-\alpha)^k$ where α is an eigenvalue of T.

Then we can choose a basis for each direct summand so that we obtain a matrix for T restricted to this basis of the form

$$\begin{pmatrix} \alpha & 1 & & & \\ & \alpha & \ddots & & \\ & & \ddots & 1 & \\ & & & \alpha & 1 \\ & & & & \alpha \end{pmatrix}$$

where the blank entries are zero.
This matrix is called the *Jordan block of size k with eigenvalue α*. We can apply this to each factor in the decomposition of V to obtain the matrix for T as a block diagonal matrix with Jordan blocks along the diagonal: $\begin{pmatrix} J_1 & & & \\ & J_2 & & \\ & & \ddots & \\ & & & J_t \end{pmatrix}$.
This form is unique up to permutation of the Jordan blocks on the diagonal. Also, this list of elementary divisors uniquely determines V up to $F[t]$-module isomorphism. Note that we must have all eigenvalues of T in F to obtain the

Jordan canonical form, so it is important that we examine an algebraically closed field. Also, any $n \times n$ matrix A with entries in F and all eigenvalues in F is similar to a matrix in Jordan canonical form. That is, there exists an invertible $n \times n$ matrix P over F such that $P^{-1}AP$ is block diagonal with Jordan blocks on the diagonal corresponding to the elementary divisors of A. Also note that a Jordan matrix is diagonal if and only if all eigenvalues are distinct.

Now consider an arbitrary field F. We now introduce the *rational canonical form* with respect to the linear transformation T. Let $a(t)$ be a monic polynomial in $F[t]$, say $a(t) = t^k + b_{k-1}t^{k-1} + \cdots + b_1 t + b_0$. We can give a basis for the vector space $F[t]/(a(t))$ of the elements 1, $\bar{t}$, $\bar{t}^2$,..., $\bar{t}^{k-1}$, where $\bar{t} = t \mathrm{mod}(a(t))$. Then the *companion matrix* is the matrix for multiplication by x with respect to this basis:

$$\begin{pmatrix} 0 & 0 & \dots & \dots & \dots & -b_0 \\ 1 & 0 & \dots & \dots & \dots & -b_1 \\ 0 & 1 & \dots & \dots & \dots & -b_2 \\ 0 & 0 & \ddots & & & \vdots \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & 1 & -b_{k-1} \end{pmatrix}.$$

The companion matrix of $a(t) = t^k + b_{k-1}t + \cdots + b_1 t + b_0$ is the $k \times k$ matrix with 1's down the first subdiagonal, $-b_0$, $-b_1$, ..., $-b_{k-1}$ down the last column, and zeros elsewhere. We denote this matrix $\mathcal{C}_{a(t)}$. When considering our linear transformation T, we have by Theorem 3.6, we have the isomorphism $V \cong F[t]/(a_1(t)) \oplus F[t]/(a_2(t)) \oplus \cdots \oplus F[t]/(a_m(t))$, where $a_1(t)|a_2(t)|\cdots|a_m(t)$. Then we can give this basis with respect to each of the direct summands and obtain the companion matrices for each invariant factor of V. This gives us the rational canonical form of T, which is the direct sum of the companion matrices for the invariant factors, that is,

$$\begin{pmatrix} \mathcal{C}_{a_1(t)} & & & \\ & \mathcal{C}_{a_2(t)} & & \\ & & \ddots & \\ & & & \mathcal{C}_{(a_m(t))} \end{pmatrix}.$$

This matrix is uniquely determined from the invariant factors which uniquely determine the module V up to isomorphism as an $F[t]$-module.

This theory allows us to consider an element $x \in \mathrm{GL}(n, F)$ and its natural action on an n-dimensional vector space V over F as an invertible transformation.

Then we can examine its characteristic polynomial in $F[t]$ and derive its Jordan form in the algebraic closure $\bar{F}$ where the characteristic polynomial will break down into linear factors. We will use elementary divisors, the rational canonical form, and the Jordan canonical form to examine conjugacy classes in $\mathrm{GL}(n, \mathbb{F}_q)$ and $\mathrm{U}(n, \mathbb{F}_{q^2})$ and whether or not they are real or strongly real.

3.2 Real Conjugacy Classes of $\mathrm{GL}(n, \mathbb{F}_q)$

It follows from the theory of elementary divisors and rational canonical forms that there is a one-to-one correspondence between the conjugacy classes of $\mathrm{GL}(n, \mathbb{F}_q)$ and lists of powers of monic irreducible polynomials in $\mathbb{F}_q[t]$, as we now discuss. That is, the conjugacy class of an element g in $\mathrm{GL}(n, \mathbb{F}_q)$ is defined by a list of powers of monic irreducible polynomials in $\mathbb{F}_q[t]$ with multiplicities such that the product is the characteristic polynomial of g. In particular, we assign a partition $\lambda^{(f)}$ to each irreducible polynomial f over $\mathbb{F}_q$ such that $\sum_f \deg(f) \left|\lambda^{(f)}\right| = n$. If the partition $\lambda^{(f)}$ has parts $(\lambda_1, \lambda_2, \ldots, \lambda_k)$, then $f^{\lambda_1}, f^{\lambda_2}, \ldots, f^{\lambda_k}$ are elementary divisors of g over $\mathbb{F}_q$. It is true, in fact, that g is conjugate in $\mathrm{GL}(n, \mathbb{F}_q)$ to the block diagonal matrix which is the direct product of the companion matrices of all elementary divisors of g. That is, the conjugacy class of g in $\mathrm{GL}(n, \mathbb{F}_q)$ is the conjugacy class of the matrix $\prod_f \mathcal{C}_{\lambda^{(f)},f}$ where our product is over the irreducible factors f of the characteristic polynomial of g. Here $\mathcal{C}_{\lambda^{(f)},f} = \mathcal{C}_{\lambda_1,f} \times \cdots \times \mathcal{C}_{\lambda_k,f}$ where $\lambda^{(f)} = (\lambda_1, \ldots, \lambda_k)$ and each $\mathcal{C}_{\lambda_i,f}$ is the companion matrix corresponding to the divisor f^{λ_i}.

Furthermore, irreducible polynomials over $\mathbb{F}_q$ are given by orbits of elements $\alpha \in \bar{\mathbb{F}}_q^{\times}$ under the Frobenius map which maps α to α^q. Over $\bar{\mathbb{F}}_q$, any polynomial will break into linear factors. When $f(t)$ is irreducible, these roots are distinct. Also, we know that these roots are exactly $\{\alpha, \alpha^q, \alpha^{q^2}, \ldots, \alpha^{q^{d-1}}\}$, where $d = \deg(f)$. This is the orbit of α under the Frobenius map. Thus, over $\bar{\mathbb{F}}_q$, f factors into linear polynomials of the form $(t-\alpha)(t-\alpha^q)\cdots(t-\alpha^{q^{d-1}})$. Then we can obtain the Jordan canonical form for f as the block diagonal matrix of Jordan blocks corresponding to α, α^q, $\ldots$, $\alpha^{q^{d-1}}$. Over $\mathrm{GL}(n, \bar{\mathbb{F}}_q)$, the matrix $\mathcal{C}_{\lambda^{(f)},f}$ in rational canonical form is conjugate to this matrix in Jordan canonical form since they have the same elementary divisors. Then over $\mathrm{GL}(n, \bar{\mathbb{F}}_q)$, g is conjugate to the matrix $\prod_f J_{\lambda^{(f)},f}$, and $J_{\lambda^{(f)}} = J_{\lambda_1,f} \times \cdots \times J_{\lambda_k,f}$ where $\lambda^{(f)} = (\lambda_1, \ldots, \lambda_k)$ and each $J_{\lambda_i,f}$ is the Jordan block matrix corresponding to f^{λ_i}.

Now we introduce the dual polynomial, denoted $\bar{f}(t)$. If $f(t) \in \mathbb{F}_q[t]$ is irreducible and monic with roots $\alpha, \alpha^q, \ldots, \alpha^{q^{n-1}}$, then we define $\bar{f}(t)$ to be the

polynomial with the inverse roots $\alpha^{-1}, \alpha^{-q}, \ldots, \alpha^{-q^{n-1}}$. If $g \in \mathrm{GL}(n, \mathbb{F}_q)$ has the conjugacy class given by the partitions $\lambda^{(f)}$ corresponding to the monic irreducible polynomials f, then the conjugacy class of g^{-1} must be given by the partitions $\lambda^{(\bar{f})}$ corresponding to the monic irreducible polynomials $\bar{f}$ with the inverse roots.

Now we can define exactly which conjugacy classes are real in $\mathrm{GL}(n, \mathbb{F}_q)$. Note that over $\mathrm{GL}(n, \mathbb{F}_q)$ each $\mathcal{C}_{\lambda_i, f}$ is the companion matrix for f^{λ_i}. Over $\mathrm{GL}(\deg(f)\,|\lambda_i|\,, \bar{\mathbb{F}}_q)$, $\mathcal{C}_{\lambda_i, f}$ is conjugate to $J_{\lambda_i, f}$. Also, $\mathcal{C}^{-1}_{\lambda_i, f}$ is conjugate to $J^{-1}_{\lambda_i, f}$ as well. Now observe that the characteristic polynomial of $J_{\lambda_i, f}$ is f^{λ_i} so the characteristic polynomial of $J^{-1}_{\lambda_i, f}$ must be $\bar{f}^{\lambda_i}$ by examining roots. It follows that $J^{-1}_{\lambda_i, f}$ is conjugate to $J_{\lambda_i, \bar{f}}$. Then, over $\mathrm{GL}(\deg(f)\,|\lambda_i|\,, \bar{\mathbb{F}}_q)$, we know that $J_{\lambda_i, \bar{f}}$ is conjugate to $\mathcal{C}_{\lambda_i, \bar{f}}$, the companion matrix for $\bar{f}^{\lambda_i}$, since they have the same roots. Then $\mathcal{C}_{\lambda_i, f}$ is conjugate to $\mathcal{C}_{\lambda_i, \bar{f}}$ in $\mathrm{GL}(\deg(f)\,|\lambda_i|\,, \bar{\mathbb{F}}_q)$ and thus in $\mathrm{GL}(\deg(f)\,|\lambda_i|\,, \mathbb{F}_q)$. The condition for reality then follows. An element $g \in \mathrm{GL}(n, \mathbb{F}_q)$ is real if and only if g is conjugate in $\mathrm{GL}(n, \mathbb{F}_q)$ to $[\prod_{f \neq \bar{f}} (\mathcal{C}_{\lambda^{(f)}, f} \times \mathcal{C}_{\lambda^{(\bar{f})}, \bar{f}})] \times [\prod_{f = \bar{f}} \mathcal{C}_{\lambda^{(f)}, f}]$. Since g is real, the conjugacy class of g is a real conjugacy class. We end this discussion with a statement of exactly when a conjugacy class in $\mathrm{GL}(n, \mathbb{F}_q)$ is real.

Proposition 3.8. *Given $g \in \mathrm{GL}(n, \mathbb{F}_q)$ is in the conjugacy class parameterized by the list of irreducible polynomials $f \in \mathbb{F}_q[t]$ with associated partitions $\lambda^{(f)}$, g is real if and only if $\lambda^{(f)} = \lambda(\bar{f})$ for each irreducible polynomial f.*

The conjugacy classes in $\mathrm{U}(n, \mathbb{F}_{q^2})$ are defined in an analogous way using U-irreducible polynomials, which we will introduce, in place of these monic irreducibles over $\mathbb{F}_q$, and the real conjugacy classes are also analogous to those in $\mathrm{GL}(n, \mathbb{F}_q)$.
Before we examine the real and strongly real classes in the finite unitary group, however, it is important to state that all real conjugacy classes in $\mathrm{GL}(n, \mathbb{F}_q)$ are also strongly real. Indeed, Wonenburger [10] proved that for fields F with char $F \neq 2$, reality is equivalent to strong reality in $\mathrm{GL}(n, F)$ since an invertible matrix is conjugate to its inverse if and only if it is the product of two involutions. Then Gill and Singh [5] proved that the result is true for characteristic 2 as well. Thus, we have all real classes are strongly real in the finite general linear group.

3.3 Real and Strongly Real Conjugacy Classes of $\mathrm{U}(n, \mathbb{F}_{q^2})$

First we introduce U-irreducible polynomials. These are polynomials in $\mathbb{F}_q[t]$ which are orbits of nonzero elements of $\bar{\mathbb{F}}^{\times}_{q^2}$ under the twisted Frobenius

map defined by $\alpha \mapsto \alpha^{-q}$ for $\alpha \in \bar{\mathbb{F}}_{q^2}^{\times}$. That is, they are of the form $(t-\alpha)(t-\alpha^{-q})(t-\alpha^{q^2})\cdots(t-\alpha^{(-q)^{n-1}})$ where $\alpha \in \bar{\mathbb{F}}_{q^2}^{\times}$. We know from Ennola [3] and Wall [9] how to parameterize the conjugacy classes of $\mathrm{U}(n, \mathbb{F}_{q^2})$. The conjugacy class of any $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ corresponds to lists of powers of U-irreducible polynomials such that the product is the characteristic polynomial for x. These polynomials are not necessarily irreducible, but they are analogous to the irreducible polynomials that correspond to the conjugacy classes of $\mathrm{GL}(n, \mathbb{F}_{q^2})$ and thus we call them U-irreducible. If $f(t) = (t-\alpha)(t-\alpha^{-q})(t-\alpha^{q^2})\cdots(t-\alpha^{(-q)^{n-1}})$, then we define $\bar{f}(t) = (t-\alpha^{-1})(t-\alpha^{q})(t-\alpha^{-q^2})\cdots(t-\alpha^{-(-q)^{n-1}})$, the orbit of α^{-1} under the twisted Frobenius map. For each U-irreducible polynomial f, we assign a partition $\mu^{(f)}$. If $\mu^{(f)}$ has parts $(\mu_1, \mu_2, \ldots, \mu_n)$, then $f^{\mu_1}, f^{\mu_2}, \ldots, f^{\mu_n}$ are elementary divisors of x over $\mathbb{F}_{q^2}[t]$ such that $\sum_f \deg(f)\left|\mu^{(f)}\right| = n$. Then a conjugacy class of $\mathrm{U}(n, \mathbb{F}_{q^2})$ is real exactly when $\mu^{(f)} = \mu^{(\bar{f})}$ for each U-irreducible polynomial f. Note here that the real conjugacy classes in $\mathrm{U}(n, \mathbb{F}_{q^2})$ and $\mathrm{GL}(n, \mathbb{F}_q)$ are parameterized in the same way as observed by Gow [7]. In $\mathrm{GL}(n, \mathbb{F}_q)$, we look at the monic irreducible polynomials $h \in \mathbb{F}_q[t]$, where $\deg(h) = d$, with roots α, α^q, α^{q^2},..., $\alpha^{q^{d-1}} \in \bar{\mathbb{F}}_q[t]$. Then we again have the dual polynomial $\bar{f}$ with the inverse roots α^{-1}, α^{-q},..., $\alpha^{-q^{d-1}} \in \bar{\mathbb{F}}_q[t]$. We assign a partition $\lambda^{(h)}$ to each irreducible polynomial h as explained earlier. A conjugacy class is real exactly when $\lambda^{(h)} = \lambda^{(\bar{h})}$. In the Jordan form we take the direct sum of the Jordan blocks corresponding to h and $\bar{h}$. When we do this, we see that the roots now are α, α^{-1}, α^q, α^{-q}, ..., $\alpha^{q^{d-1}}$, $\alpha^{-q^{d-1}}$, the union of the roots of h and $\bar{h}$. By taking the union of these roots, we can also look at this Jordan block as corresponding to a U-irreducible polynomial f and its dual $\bar{f}$ since the roots of f are $\alpha, \alpha^{-q}, \alpha^{q^2}, \ldots, \alpha^{-q^{d-1}}$ and its dual polynomial $\bar{f}$ has the inverse roots. The union of these roots gives us the same roots as the previous union.

Now we can construct the Jordan block corresponding to each U-irreducible polynomial f, and we call this Jordan block x_f, which is an element of the smaller unitary group $\mathrm{U}(n_f, \mathbb{F}_{q^2})$ where $n_f = \deg(f)\left|\mu^{(f)}\right|$. Then we write x as the direct product of the Jordan blocks of all its U-irreducible divisors so that x is a block diagonal matrix. That is, write $x = \prod_f (x_f)$, where we may may take $x_f \in \mathrm{U}(n_f, \mathbb{F}_{q^2})$. Actually x need only be conjugate to this direct product since we are operating within a conjugacy class.
Before we continue, we will prove two short lemmas that will be useful for our theorem.

Lemma 3.9. *Let $x \in G$ be real where $yxy^{-1} = x^{-1}$ for some $y \in G$. Then $A = \{a \in G | axa^{-1} = x^{-1}\} = yC_G(x)$.*

Proof. First let $z \in A$ so $zxz^{-1} = x^{-1}$. Let $z = yg$ for $y, g \in G$. Then $ygx(yg)^{-1} = x^{-1}$ so $ygxg^{-1}y^{-1} = yxy^{-1}$. Then it follows that $gxg^{-1} = x$ so $gx = xg$. Then $g \in C_G(x)$ and $z \in yC_G(x)$.
Now let $w \in yC_G(x)$. Then $w = yc$ for $c \in C_G(x)$. Then $wxw^{-1} = ycx(yc)^{-1} = ycxc^{-1}y^{-1} = yxcc^{-1}y^{-1} = yxy^{-1} = x^{-1}$ so $w \in A$. □

Lemma 3.10. *An element* $x = (x_i)_{i=1}^n \in \prod_{i=1}^n G_i$ *is strongly real in* $\prod_{i=1}^n G_i$ *if and only if* x_i *is strongly real in* G_i *for each* $i = 1, \ldots, n$.

Proof. First let $x \in \prod_{i=1}^n G_i$ be strongly real in $\prod_{i=1}^n G_i$. Then there exists some $y \in \prod_{i=1}^n G_i$ such that $yxy = x^{-1}$ where $y^2 = 1$. That is,

$$(y_1, y_2, \ldots, y_n)(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1, x_2, \ldots, x_n)^{-1}.$$

Then $(y_1x_1y_1, y_2x_2y_2, \ldots, y_nx_ny_n) = (x_1^{-1}, x_2^{-1}, \ldots, x_n^{-1})$. Therefore we have $y_ix_iy_i = x_i^{-1}$ for $i = 1, \ldots, n$ so x_i is strongly real in G_i for $i = 1, \ldots, n$.
Now assume x_i is strongly real in G_i for each $i = 1, \ldots, n$ so there exists $y_i \in G_i$ such that $y_i^2 = 1$ and $y_ix_iy_i = x_i^{-1}$ for each i. Then let $y \in \prod_{i=1}^n G_i$ be $y = (y_1, y_2, \ldots, y_n)$, it follows that $yxy = x^{-1}$ and thus x is strongly real in $\prod_{i=1}^n G_i$. □

Theorem 3.11. *Conjecture 1.3 holds for any real* $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ *if Conjecture 1.3 holds for any unipotent element in* $\mathrm{U}(n, \mathbb{F}_{q^2})$.

Proof. First we show that if Conjecture 1.3 holds for unipotent elements in $G = \mathrm{U}(n, \mathbb{F}_{q^2})$, then our conjecture holds for negative unipotent elements as well, where by negative unipotent we mean the only elementary divisors are of the form $(t+1)^k$. Now suppose Conjecture 1.3 holds for unipotent elements in G. Then consider the negative unipotent element $x \in G$ where x has elementary divisors only of the form $(t+1)^k$ for various k with multiplicities. Then we have a partition $\mu = \mu^{(t+1)}$ where $|\mu| = n$, and the parts of the partition $\mu_1, \ldots, \mu_r$ correspond to the powers of $(t+1)$ that appear. Then we know x is conjugate to a matrix in Jordan canonical form $J_{\mu^{(t+1)}, t+1}$, which is block diagonal with Jordan blocks corresponding to each elementary divisor. This matrix will have -1 on the diagonal since -1 is the only eigenvalue with multiplicity n. Then consider $-x$. We see that $-x$ will be unipotent since $-J_{\mu^{(t+1)}, t+1}$ will be a block diagonal matrix in Jordan canonical form with 1 on all diagonal entries and thus 1 is the only eigenvalue with multiplicity n. Then $-x$ will have elementary divisors $(t-1)^k$ with the same partition as x. That is, the conjugacy class of $-x$ is given by $\mu = \mu^{(t+1)}$, where μ now corresponds to $t-1$.
Now we show that x is strongly real if and only if $-x$ is strongly real. Let x be strongly real. Then $sxs = x^{-1}$ for $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$ where $s^2 = 1$. Then $(-s)^2 = 1$

so we observe $(-s)(-x)(-s) = -sxs = -x^{-1} = (-x)^{-1}$. Similarly, if we have $-x$ strongly real, then $t(-x)t = (-x)^{-1}$ where $t^2 = 1$. Then $-txt = -x^{-1}$ so $txt = x^{-1}$ and thus x is strongly real. It follows that if x has elementary divisors of the form $(t+1)^k$ for various k with multiplicity we can consider $-x$ instead, which will be unipotent. Thus, if Conjecture 1.3 holds for unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$, then it holds also for negative unipotent elements.

Now we show that Conjecture 1.3 holds for any real x in $G = \mathrm{U}(n, \mathbb{F}_{q^2})$ if it holds for any unipotent element in G. We know that the conjugacy class for x is defined by our partition function μ which sends any U-irreducible polynomial $f \in \mathbb{F}_{q^2}[t]$ to the partition $\mu^{(f)}$ such that $\sum_f \deg(f) \left|\mu^{(f)}\right| = n$ and such that $\mu^{(f)} = \mu^{(\bar{f})}$.

Write the centralizer of x in $\mathrm{U}(n, \mathbb{F}_{q^2})$ as $C_{\mathrm{U}}(x)$. It follows from Ennola [3] and Wall [9] that we have $C_{\mathrm{U}}(x) = \prod_f C_{\mu^{(f)}}(x_f)$ where x is conjugate to $\prod_f (x_f)$ and $x_f \in \mathrm{U}(n_f, \mathbb{F}_{q^2})$ and $\prod_f C_{\mu^{(f)}}(x_f)$ is the centralizer of x_f in the smaller unitary group $\mathrm{U}(n_f, \mathbb{F}_{q^2})$. Here $n_f = \deg(f) \left|\mu^{(f)}\right|$ as defined earlier.

Now we will introduce some new terminology briefly. If x is real, then for each f, $\bar{f}$, if $f \neq \bar{f}$, then define $x_{f,\bar{f}} \in \mathrm{U}(n_f + n_{\bar{f}}, \mathbb{F}_{q^2})$ to be the block diagonal element $(x_f, x_{\bar{f}})$. For simplicity we introduce

$$x_{\tilde{f}} = \begin{cases} x_f & \text{if } f = \bar{f}, \\ x_{f,\bar{f}} & \text{if } f \neq \bar{f}. \end{cases}$$

and

$$n_{\tilde{f}} = \begin{cases} n_f & \text{if } f = \bar{f}, \\ n_{f,\bar{f}} & \text{if } f \neq \bar{f}. \end{cases}$$

Now we have x conjugate to $\prod_f (x_{\tilde{f}}) \in \prod \mathrm{U}(n_{\tilde{f}}, \mathbb{F}_{q^2}) = \prod G_{\tilde{f}}$ which is a subset of $\mathrm{U}(n, \mathbb{F}_{q^2}) = G$. Here $x_{\tilde{f}}$ is real in $G_{\tilde{f}}$, which follows from the parameterization of real classes in $\mathrm{U}(n_{\tilde{f}}, \mathbb{F}_{q^2})$. From Lemma 3.9, we know exactly which elements conjugate x to x^{-1}, given that we know one such element. We know that x is real so for some $y \in G = \mathrm{U}(n, \mathbb{F}_{q^2})$, $yxy^{-1} = x^{-1}$. All other elements which conjugate x to its inverse are in $yC_G(x) = y \prod_{\tilde{f}} C_{G_{\tilde{f}}}(x_{\tilde{f}})$, since

$$C_{G_{\tilde{f}}}(x_{\tilde{f}}) = \begin{cases} C_{G_f}(x_f) & \text{if } f = \bar{f}, \\ C_{G_f}(x_f) C_{G_{\bar{f}}}(x_{\bar{f}}) & \text{if } f \neq \bar{f}. \end{cases}$$

Since $x = \prod_f (x_{\tilde{f}})$ such that $x_{\tilde{f}}$ is real in $G_{\tilde{f}}$, choose y such that $y = \prod_f (y_{\tilde{f}})$ where $y_{\tilde{f}} x_{\tilde{f}} y_{\tilde{f}}^{-1} = x_{\tilde{f}}^{-1}$. Now, any $s \in G = \mathrm{U}(n, \mathbb{F}_{q^2})$ such that $sxs^{-1} = x^{-1}$ is such that $s \in \prod_f y_{\tilde{f}} C_{G_{\tilde{f}}}(x_{\tilde{f}})$. From [6, Proposition 5.2], we know that if $f \neq t+1, t-1$, then $x_{\tilde{f}}$ is strongly real in $G_{\tilde{f}}$. It follows from Lemma 3.10 that x is strongly real if and only if x_{t+1} and x_{t-1} are strongly real in G_{t+1} and G_{t-1}, their respective smaller

unitary groups. Assume that Conjecture 1.3 holds for our unipotent element x_{t-1}. Then x_{t-1} is strongly real if and only if each elementary divisor of x_{t-1} of the form $(t-1)^{2m}$ occurs with even multiplicity. Then since we know that x_{t-1} is strongly real if and only if x_{t+1} is strongly real, it follows that x_{t+1} is strongly real if and only if each elementary divisor of x_{t+1} of the form $(t+1)^{2m}$ occurs with even multiplicity. Thus, it follows that for x real in $\mathrm{U}(n, \mathbb{F}_{q^2})$, x is strongly real if and only if x_{t-1} is strongly real. Hence we need only consider the strongly reality of unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$. □

Chapter 4

The Regular Unipotent Case and Strategy

Now we examine the regular unipotent case, that is, whether or not regular unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$ are strongly real. We actually have the result from Gow and Vinroot[6, Proposition 5.1] that all regular unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$ are not strongly real when n is even and q is odd or when n is odd and q is even. We will show the proof of this proposition given by Gow and Vinroot because it provides a helpful beginning as a method of proof that we will attempt to adapt to our own purposes. We will discuss our strategy after showing the proof following a brief introduction of notation to be used throughout the paper.

In the proof of the following proposition we examine regular unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$. If $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ is regular unipotent, then it has the lone elementary divisor $(t-1)^n$. This divisor corresponds to a Jordan block which corresponds to a choice of basis vectors for V as an $\mathbb{F}_{q^2}$-vector space. That is, we can choose a basis $v_1, \ldots, v_n$ such that $xv_1 = v_1$ and $xv_i = v_{i-1} + v_i$ for $i = 2, \ldots, n$. Furthermore, we can act on a vector $v \in V$ by an involution $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$ and obtain a linear combination of our basis vectors, so $sv = a_1v_1 + a_2v_2 + \cdots + a_nv_n$, for some $a_1, a_2, \ldots, a_n \in \mathbb{F}_{q^2}$.

We now come to the result on regular unipotent elements from [6].

Proposition 4.1. *Let x be a regular unipotent element in $\mathrm{U}(n, \mathbb{F}_{q^2})$. Then x is not strongly real if n is even and q is odd, or if n is odd and q is even. Here x is real in all cases.*

Proof. We only prove the statement for n even and q odd. For the case of n odd and q even, refer to [6, Proposition 5.1]. Let V be a vector space of dimension n

over $\mathbb{F}_{q^2}$ on which x acts, and let $H : V \times V \to \mathbb{F}_{q^2}$ be a non-degenerate Hermitian form preserved by x. We prove this result by induction on n. First consider the base case for when n is even and q is odd. Then let $n = 2$. Then we consider V with a basis comprised of the vectors v_1 and v_2 such that

$$xv_1 = v_1, \quad xv_2 = v_1 + v_2.$$

Also, since x is an isometry of H, we have

$$H(v_1, v_2) = H(xv_1, xv_2) = H(v_1, v_1 + v_2) = H(v_1, v_1) + H(v_1, v_2).$$

which implies that $H(v_1, v_1) = 0$. We assume that x is strongly real in $\mathrm{U}(n, \mathbb{F}_{q^2})$. Let $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be any involution acting on V which inverts x, that is $sxs = x^{-1}$ and $s^2 = 1$. Since $sxsv_1 = x^{-1}v_1$ implies $xsv_1 = sv_1$, we see that x fixes sv_1. However, v_1 spans the unique one-dimensional subspace of V fixed by x so $sv_1 = a_1v_1$ for some scalar $a_1 \in \mathbb{F}_{q^2}$. Then $v_1 = a_1sv_1 = a_1^2v_1$. Then $sv_1 = \pm v_1$ since $a_1^2 = 1$ so $a_1 = \pm 1$. We can assume $sv = v$ since we can replace s with $-s$ if necessary. Also, since $sxsv_2 = x^{-1}v_2$, we obtain $xsv_2 = sv_2 - sv_1$. We write $sv_2 = b_1v_1 + b_2v_2$ so $xsv_2 - sv_2 = -sv_1$ implies $b_2v_1 = -v_1$. Then $b_2 = -1$. Since $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$ is an isometry of H,

$$H(v_1, v_2) = H(sv_1, sv_2) = H(v_1, b_1v_1 - v_2) = H(v_1, b_1v_1) + H(v_1, -v_2) = -H(v_1, v_2).$$

Since q is odd, we observe that $H(v_1, v_2) = 0$. Then $H(v_1, v_1) = H(v_1, v_2) = 0$ which implies that v_1 is in the radical of H which contradicts the fact that H is non-degenerate. Then x is not strongly real in $\mathrm{U}(n, \mathbb{F}_{q^2})$. Now we let $n \geq 4$ and q be odd. We assume that our result holds for spaces of dimension $n - 2$. In this case, we now have n basis vectors, but we still can find vectors v_1 and v_2 in V with

$$xv_1 = v_1, xv_2 = v_1 + v_2.$$

In general, we have a basis $\{v_1, v_2, \ldots, v_n\}$ such that $xv_1 = v_1$ and $xv_i = v_{i-1} + v_i$ for $i = 2, \ldots, n$. As we saw previously, this implies $H(v_1, v_1) = 0$. Let W be the one-dimensional subspace of V spanned by v_1 and let $W^\perp$ be the subspace of V orthogonal to W, that is $H(v_1, w) = 0$ for all $w \in W^\perp$. We observe that W is contained in $W^\perp$ since $H(v_1, v_1) = 0$. Also we have an induced non-degenerate Hermitian form, say $\tilde{H}$, on $W^\perp/W$, which is a vector space of dimension $n-2$ over $\mathbb{F}_{q^2}$ since $\dim W + \dim W^\perp = \dim V$ and $\dim W = 1$. We define $\tilde{H}$ as

$$\tilde{H}(u_1 + W, u_2 + W) = H(u_1, u_2)$$

where u_1, u_2 are in $W^\perp$. We briefly show why $\tilde{H}$ is indeed Hermitian and non-degenerate.
We see that

$$\begin{aligned}
&\tilde{H}(a_1u_1 + W + a_2u_2 + W, a_3u_3 + W + a_4u_4) &=\\
&\tilde{H}(a_1u_1 + a_2u_2 + W, a_3u_3 + a_4u_4 + W) &=\\
&H(a_1u_1 + a_2u_2, a_3u_3 + a_4u_4) &=\\
&H(a_1u_1, a_3u_3) + H(a_2u_2, a_3u_3) + H(a_1u_1, a_4u_4) + H(a_2u_2, a_4u_4) &=\\
&a_1a_3^qH(u_1, u_3) + a_2a_3^qH(u_2, u_3) + a_1a_4^qH(u_1, u_4) + a_2a_4^qH(u_2, u_4) &=\\
&a_1a_3^q\tilde{H}(u_1 + W, u_3 + W) + a_2a_3^q\tilde{H}(u_2 + W, u_3 + W)\\
&\quad + a_1a_4^q\tilde{H}(u_1 + W, u_4 + W) + a_2a_4^q\tilde{H}(u_2 + W, u_4 + W).
\end{aligned}$$

Therefore $\tilde{H}$ is sesquilinear. Furthermore it is Hermitian since

$$\begin{aligned}
\tilde{H}(u_1 + W, u_2 + W) &= H(u_1, u_2)\\
&= \overline{H(u_2, u_1)}\\
&= \overline{\tilde{H}(u_2 + W, u_1 + W)}.
\end{aligned}$$

Now that we have a Hermitian form, we show it is non-degenerate.
Suppose that $\tilde{H}(u + W, v + W) = 0$ for all $u \in W^\perp/W$. Then $H(u, v) = 0$ for all $u \in W^\perp$. Then $v \in (W^\perp)^\perp$. Note that $\dim(W^\perp)^\perp = 1$ where W is contained in $(W^\perp)^\perp$ and $\dim W = 1$ so $W = (W^\perp)^\perp$ and thus $v \in W$ which is what we want since W is our zero element in $W^\perp/W$.
Also x maps W into W and $W^\perp$ into $W^\perp$. Since $xv_1 = v_1$ and any $w \in W$ can be written av_1 for some $a \in \mathbb{F}_{q^2}$, the first statement is true. Now consider any $u \in W^\perp$. Then $H(u, v_1) = 0$. Also $H(u, v_1) = H(xu, xv_1) = H(xu, v_1) = 0$ so $xu \in W^\perp$ as well. It suffices to consider v_1 since any $w \in W$ is a scalar multiple of v_1.
Since x maps W into W and $W^\perp$ into $W^\perp$, x has an induced action as a regular unipotent element, say $\tilde{x}$, on $W^\perp/W$, where it preserves $\tilde{H}$. We define this action to be $\tilde{x}(u+W) = xu+W$. We see that $\tilde{x}$ acts as a regular unipotent element since $\tilde{x}(v_2 + W) = xv_2 + W = v_1 + v_2 + W = v_2 + W$ and for $i = 3, \ldots, n-1$ we have $\tilde{x}(v_i + W) = xv_i + W = v_{i-1} + v_i + W = v_{i-1} + W + v_i + W$.
Now suppose that x is inverted by s, where $s^2 = 1$ and s is an isometry of H. Also, since v_1 is the only basis vector fixed by x and $xsv_1 = sv_1$, sv_1 must be in the span of v_1 so s maps W into W and thus maps $W^\perp$ into $W^\perp$ as well. We see this since $sW = W$ implies $sw = aw$ for some $a \in \mathbb{F}_{q^2}^\times$, any $w \in W$, and, for any $u \in W^\perp$, we have $H(u, w) = H(su, sw) = a^qH(su, w) = 0$ so $su \in W^\perp$. Then we also have an induced action of s on $W^\perp/W$ as an involutory isometry, say $\tilde{s}$, of

$\tilde{H}$, and $\tilde{s}$ inverts the regular unipotent element $\tilde{x}$. Here we define this action to be $\tilde{s}(u+W) = su+W$ for any $u \in W^{\perp}$. We observe that since $sxs = x^{-1}$, we have, for any $u+W \in W^{\perp}/W$,

$$\begin{aligned} sxs(u+W) &= x^{-1}(u+W) \quad \text{so} \\ sxsu+W &= x^{-1}u+W \quad \text{and finally} \\ \tilde{s}\tilde{x}\tilde{s}(u+W) &= \tilde{x}^{-1}(u+W) \end{aligned}$$

which shows that $\tilde{s}\tilde{x}\tilde{s} = \tilde{x}^{-1}$. Since $W^{\perp}/W$ is of dimension $n-2$, the induction hypothesis eliminates the possibility of this occurring so we have a contradiction. Thus s is not an isometry of H and x is not strongly real in $\mathrm{U}(n, \mathbb{F}_{q^2})$. □

We have already shown via Theorem 3.11 that if Conjecture 1.3 holds for any unipotent element in $\mathrm{U}(n, \mathbb{F}_{q^2})$, then it holds for any real $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$. Thus we need only consider the strong reality of unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$ to prove the general case. In order to do this, we will adapt the strategy employed by Gow and Vinroot in the previous proof. Our goal is to first prove which classes are strongly real with only elementary divisors of the form $(t-1)$ and $(t-1)^2$. Then we will adapt their induction method of choosing a subspace W of V and looking at $W^{\perp}$. However, we will not use induction but instead use this method of wisely choosing the correct vectors to span our space W and use $W^{\perp}/W$ and its induced unipotent element, reversing involution, and induced Hermitian form. This enables us to reduce from our initial case where our unipotent element may have any unipotent elementary divisors to a case where we have an induced unipotent element with elementary divisors only of the form $(t-1)$ and $(t-1)^2$. We can then use the same contradiction as in the proof of Proposition 4.1. That is, we assume our initial element is strongly real. If we reduce it to an induced unipotent element in a smaller unitary group and this element is not strongly real because of its elementary divisors, then we have a contradiction since the induced unipotent element should retain strong reality. Then our initial element must not be strongly real.

We will first examine the case of q odd although some results for q even will follow quickly. Then we will examine the case that q is even briefly as well, although we will then have to consider reduction to divisors of the form $(t-1)$,$(t-1)^2$, and $(t-1)^3$.

Chapter 5

Base Case and Reduction

In this chapter, we will be proving our main results, namely the reduction of the elementary divisors of a unipotent element in $\mathrm{U}(n, \mathbb{F}_{q^2})$ and our best current result for the base case when q is odd. Before we prove these results, we must prove several lemmas.

5.1 Useful Lemmas

Lemma 5.1. *If $sv = \lambda v$ for a vector $v \in V$, where $s^2 = 1$ for $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$ and λ is a scalar, then $\lambda = \pm 1$.*

Proof. Let $sv = \lambda v$. Since $s^2 = 1$, we act on each side by s, and $v = s\lambda v = \lambda sv = \lambda^2 v$. Thus $\lambda^2 = 1$ so $\lambda = \pm 1$. □

Lemma 5.2. *Let x be a unipotent element of $\mathrm{U}(n, \mathbb{F}_{q^2})$, where x has $(t-1)^l$ as one of its elementary divisors, and let $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be an involution. Suppose $sxs = x^{-1}$ so x is strongly real. Consider the subspace W of the n-dimensional $\mathbb{F}_{q^2}$-vector space $V = span\{v_1, \ldots, v_n\}$, say $W = span\{v_1, \ldots, v_l\}$ such that x acts on W with elementary divisor $(t-1)^l$.. Choose a basis $\{v_1, \ldots, v_l\}$ of W such that $xv_1 = v_1$ and $xv_i = v_{i-1} + v_i$ for $i = 2, 3, \ldots, l$. Then $xsv_i = \sum_{j=1}^{i} (-1)^{i-j} sv_j$.*

Proof. We will proceed by induction. First let $i = 1$. Then since $sxs = x^{-1}$ and $x^{-1}v_1 = v_1$, we have $sxsv_1 = v_1$ so $xsv_1 = sv_1$. Now let our statement be true for some $i > 1$. Then $xsv_i = \sum_{j=1}^{i} (-1)^{i-j} sv_j$. Then $sxsv_i = x^{-1}v_i = \sum_{j=1}^{i} (-1)^{i-j} v_j$. Also since $x^{-1}xv_{i+1} = v_{i+1}$, we have $x^{-1}(v_i + v_{i+1}) = x^{-1}v_i + x^{-1}v_{i+1} = v_{i+1}$. We substitute and see that $sxsv_{i+1} = x^{-1}v_{i+1} = \sum_{j=1}^{i} (-1)^{i-j+1} v_j + v_{i+1} = \sum_{j=1}^{i+1} (-1)^{i-j+1} v_j$ so $xsv_{i+1} = \sum_{j=1}^{i+1} (-1)^{i+1-j} sv_j$, and by induction we obtain our result. □

Note that when q is even, we have $-1 = 1$ so $xsv_i = \sum_{j=1}^{i} sv_i$.

Before we prove the following lemma, we must first introduce some new notation. Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be a unipotent element. Then x has elementary divisors of the form $(t-1)^l$ for various l. We can choose to order these divisors in descending order by this exponent l. We consider each factor $(t-1)^l$ to generate an l-dimensional subspace of our n-dimensional vector space V in the following way. As an element of $\mathrm{GL}(n, \mathbb{F}_{q^2})$, the elementary divisor $(t-1)^l$ corresponds to a Jordan block, which corresponds to a choice of basis vectors for V as an $\mathbb{F}_{q^2}$-vector space as seen in the case of regular unipotent elements. That is, we have the basis $\{v_1, \ldots, v_l\}$ such that $xv_1 = v_1$ and $xv_i = v_i$ for $i = 2, \ldots, l$. Now we can do this for each elementary divisor. When we look at the list of elementary divisors of x, we have $(t-1)^l$, where $1 \leq l \leq m$, for various l. We say that there are n_l elementary divisors of the form $(t-1)^l$ for specific l. We introduce the notation $v_i^{(l,j)}$ where v_i is the ith vector from the jth appearance of the divisor $(t-1)^l$ in the list of elementary divisors. In this case, i ranges from 1 to l, j ranges from 1 to n_l, and l ranges from 1 to m. Then we choose the basis $\{v_i^{(l,j)} | 1 \leq i \leq l, 1 \leq j \leq n_l, 1 \leq l \leq m\}$ for V, so $xv_1^{(l,j)} = v_1^{(l,j)}$ and $xv_i^{(l,j)} = v_{i-1}^{(l,j)} + v_i^{(l,j)}$ for $i = 2, \ldots, l$, for $1 \leq l \leq m$ and $1 \leq j \leq n_l$. This corresponds to x in Jordan canonical form where x is block diagonal with Jordan blocks corresponding to each divisor along the diagonal.

Lemma 5.3. *Let V be an n-dimensional $\mathbb{F}_{q^2}$ vector space, and let x be a unipotent element in $\mathrm{U}(n, \mathbb{F}_{q^2})$, so x has elementary divisors of the form $(t-1)^l$ for various l between 1 and m with multiplicities n_l. Choose the basis $\{v_i^{(l,j)} | 1 \leq i \leq l, 1 \leq j \leq n_l, 1 \leq l \leq m\}$ for V, so $xv_1^{(l,j)} = v_1^{(l,j)}$ and $xv_i^{(l,j)} = v_{i-1}^{(l,j)} + v_i^{(l,j)}$ for $i = 2, \ldots, l$, for $1 \leq l \leq m$ and $1 \leq j \leq n_l$. Then if $v \in V$ is fixed by x, that is $xv = v$, then $sv = \sum_{l=1}^{m} \sum_{j=1}^{n_l} a_1^{(l,j)} v_1^{(l,j)}$, for $a_1^{(l,j)} \in \mathbb{F}_{q^2}$.*

Proof. We know that $xsv = sv$ since $sxsv = x^{-1}v = v$. Then $xsv - sv = 0$. Let $sv = \sum_{l=1}^{m} \sum_{j=1}^{n_l} \sum_{h=1}^{l} a_h^{(l,j)} v_h^{(l,j)}$, a linear combination of our basis vectors. Then, since $xv_h = v_{h-1} + v_h$ for $h = 2, \ldots, l$, we have

$$xsv = \sum_{l=1}^{m} \left(\sum_{j=1}^{n_l} \left(\sum_{h=1}^{l-1} (a_h^{(l,j)} + a_{h+1}^{(l,j)}) v_h^{(l,j)} \right) + a_l^{(l,j)} v_l^{(l,j)} \right).$$

Now we subtract and obtain

$$\begin{aligned} xsv - sv &= \sum_{l=1}^{m}\left(\sum_{j=1}^{n_l}\left(\sum_{h=1}^{l-1}(a_h^{(l,j)} + a_{h+1}^{(l,j)})v_h^{(l,j)}\right) + a_l^{(l,j)}v_l^{(l,j)}\right) - \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l} a_h^{(l,j)}v_h^{(l,j)} \\ &= \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l-1} a_{h+1}^{(l,j)}v_h^{(l,j)} \qquad (5.1) \\ &= 0. \end{aligned}$$

It follows that $a_{h+1}^{(l,j)} = 0$ for $h = 1, \ldots, l-1$, $1 \leq l \leq m$, and $1 \leq j \leq n_l$. Thus $sv = \sum_{l=1}^{m}\sum_{j=1}^{n_l} a_1^{(l,j)}v_1^{(l,j)}$, a linear combination of the basis vectors fixed by x. □

Lemma 5.4. *Consider the element $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ with a list of elementary divisors all of the form $(t-1)^k$ for some $k = 1, 2, \ldots, m$, where $(t-1)^m$ is the highest power of $(t-1)$ that appears and $(t-1)^k$ appears n_k times for $k = 1, \ldots, m$. Also, let $H : V \times V \to \mathbb{F}_{q^2}$ be the non-degenerate Hermitian form that defines our unitary group. Then, for any (l, j), (r, s), and any $1 \leq h \leq l$, $H(v_{h'}^{(l,j)}, v_i^{(r,s)}) = 0$ for all h', i such that $1 \leq h' \leq h$ and $1 \leq i \leq r - h$.*

Proof. We will proceed by induction on h. First let $h = 1$. Then we must show that $H(v_1^{(l,j)}, v_i^{(r,s)}) = 0$ for all $1 \leq i \leq r-1$. Since x is an isometry of H, we know that, for $2 \leq i \leq r$,

$$\begin{aligned} H(v_1^{(l,j)}, v_i^{(r,s)}) &= H(xv_1^{(l,j)}, xv_i^{(r,s)}) \\ &= H(v_1^{(l,j)}, v_{i-1}^{(r,s)}) + H(v_1^{(l,j)}, v_i^{(r,s)}) \end{aligned}$$

so $H(v_1^{(l,j)}, v_{i-1}^{(r,s)}) = 0$ for $i = 2, \ldots, r$. By shifting indices by 1, we have $H(v_1^{(l,j)}, v_i^{(r,s)}) = 0$ for $1 \leq i \leq r-1$.
Now assume our statement is true for $1 \leq h \leq l-1$. That is, $H(v_{h'}^{(l,j)}, v_i^{(r,s)}) = 0$ for $1 \leq h' \leq h$ and $1 \leq i \leq r-h$. Then we must show that $H(v_{h'}^{(l,j)}, v_i^{(r,s)}) = 0$ for $1 \leq h' \leq h+1$ and $1 \leq i \leq r-h-1$. Since we have our induction hypothesis, it will suffice to show that $H(v_{h+1}^{(l,j)}, v_i^{(r,s)}) = 0$ for $1 \leq i \leq r-h-1$. Since x is an isometry of H, we know that, for $2 \leq i \leq r$,

$$\begin{aligned} H(v_{h+1}^{(l,j)}, v_i^{(r,s)}) &= H(xv_{h+1}^{(l,j)}, xv_i^{(r,s)}) \\ &= H(v_h^{(l,j)}, v_{i-1}^{(r,s)}) + H(v_h^{(l,j)}, v_i^{(r,s)}) + H(v_{h+1}^{(l,j)}, v_{i-1}^{(r,s)}) + H(v_{h+1}^{(l,j)}, v_i^{(r,s)}). \end{aligned}$$

From our induction hypothesis, we know that $H(v_h^{(l,j)}, v_i^{(r,s)}) = 0$ for $1 \leq i \leq r-h$. Then, for $i = 2, \ldots, r-h$, $H(v_h^{(l,j)}, v_{i-1}^{(r,s)}) = 0$ and $H(v_h^{(l,j)}, v_i^{(r,s)}) = 0$. Therefore, we obtain $H(v_{h+1}^{(l,j)}, v_{i-1}^{(r,s)}) = 0$ for $2 \leq i \leq r-h$. Then, shifting indices by 1,

$H(v_{h+1}^{(l,j)}, v_i^{(r,s)}) = 0$ for $1 \leq i \leq r-h-1$. Hence, by induction, $H(v_{h'}^{(l,j)}, v_i^{(r,s)}) = 0$ for $1 \leq h' \leq h$ and $1 \leq i \leq r-h$. □

Lemma 5.5. *Consider the element $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ with a list of elementary divisors all of the form $(t-1)^k$ for some $k = 1, 2, \ldots, m$, where $(t-1)^m$ is the highest power of $(t-1)$ that appears and $(t-1)^k$ appears n_k times for $k = 1, \ldots, m$. Also, let $H : V \times V \to \mathbb{F}_{q^2}$ be the non-degenerate Hermitian form that defines our unitary group. Then, for any (l,j), (r,s), if $r < l$, then $H(v_{r-i+1}^{(l,j)}, v_i^{(r,s)}) = 0$ for some $1 \leq i \leq r$. In particular, $H(v_1^{(l,j)}, v_i^{(r,s)}) = 0$ for all $1 \leq i \leq r$ so $v_1^{(l,j)}$ is orthogonal to all basis vectors corresponding to the divisor $(t-1)^{(r,s)}$.*

Proof. We proceed by induction on i. First let $i = 1$. We must show $H(v_r^{(l,j)}, v_1^{(r,s)}) = 0$. Since $r < l$, we know that $l \geq r+1$. Then we know

$$\begin{aligned} H(v_{r+1}^{(l,j)}, v_1^{(r,s)}) &= H(xv_{r+1}, xv_1^{(r,s)}) \\ &= H(v_r^{(l,j)}, v_1^{(r,s)}) + H(v_{r+1}^{(l,j)}, v_1^{(r,s)}) \end{aligned}$$

so we must have $H(v_r^{(l,j)}, v_1^{(r,s)}) = 0$. Now assume our statement is true for $1 \leq i \leq r-1$. That is, $H(v_{r-i+1}^{(l,j)}, v_i^{(r,s)}) = 0$ for some $1 \leq i \leq r-1$. Then we must show $H(v_{r-(i+1)+1}^{(l,j)}, v_{i+1}^{(r,s)}) = H(v_{r-i}^{(l,j)}, v_{i+1}^{(r,s)}) = 0$. We know that x is an isometry of H, $i+1 > 1$, and $r-i+1 > 1$, so we have

$$\begin{aligned} H(v_{r-i+1}^{(l,j)}, v_{i+1}^{(r,s)}) &= H(xv_{r-i+1}^{(l,j)}, xv_{i+1}^{(r,s)}) \\ &= H(v_{r-i}^{(l,j)}, v_i^{(r,s)}) + H(v_{r-i}^{(l,j)}, v_{i+1}^{(r,s)}) + H(v_{r-i+1}^{(l,j)}, v_i^{(r,s)}) + H(v_{r-i+1}^{(l,j)}, v_{i+1}^{(r,s)}). \end{aligned}$$

We know, from our induction hypothesis, that $H(v_{r-i+1}^{(l,j)}, v_i^{(r,s)}) = 0$. Also, from Lemma 5.4, we know that $H(v_{i'}^{(r,s)}, v_h^{(l,j)}) = 0$ for $1 \leq i' \leq i$, $1 \leq h \leq r-i$, and $1 \leq i \leq r$. Then $H(v_i^{(r,s)}, v_{r-i}^{(l,j)}) = 0$. Since $H(v_{r-i}^{(l,j)}, v_i^{(r,s)}) = \overline{H(v_i^{(r,s)}, v_{r-i}^{(l,j)})}$, we obtain $H(v_{r-i}^{(l,j)}, v_i^{(r,s)}) = 0$. It follows that $H(v_{r-i}^{(l,j)}, v_{i+1}^{(r,s)}) = 0$. Hence, if $r < l$, then $H(v_{r-i+1}^{(l,j)}, v_i^{(r,s)}) = 0$ for $1 \leq i \leq r$. □

Now we introduce some further notation. Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be unipotent with elementary divisors $(t-1)^l$ for various l with $1 \leq l \leq m$. Then we choose our basis $\{v_i^{(l,j)} | 1 \leq i \leq l, 1 \leq j \leq n_l, 1 \leq l \leq m\}$ in V as shown above. We are especially interested in the action of an involution $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$ on our vector space. We can act on our basis vectors by s to obtain a linear combination of all basis vectors, and in this case we are interested usually in the coefficients of the basis vectors that occur under the action of s. In particular, we will typically act by s on one basis vector at a time. For instance, we may choose to act on the ith vector of the j'th elementary divisor of the form $(t-1)^{l'}$. In this case,

we write $sv_i^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l} a_{h,(l',j',i)}^{(l,j)} v_h^{(l,j)}$ where m is the highest power of $(t-1)$ that appears in the elementary divisor decomposition and $a_{h,(l',j',i)}^{(l,j)}$ is the coefficient of $v_h^{(l,j)}$ corresponding to $sv_i^{(l',j')}$. We incorporate the triple sum since our linear combination must include the basis vectors from all elementary divisors of x.

Note that from Equation 5.1 in Lemma 5.3 that, with the use of this notation, if we choose a basis vector from the j'th appearance of the elementary divisors $(t-1)^{l'}$ of x, then $xsv_i^{(l',j')} - sv_i^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l-1} a_{h+1,(l',j',i)}^{(l,j)} v_h^{(l,j)}$.

Lemma 5.6. *Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ have elementary divisors of the form $(t-1)^l$ for $l = 1, \ldots, m$, where m is the highest power of $(t-1)$ appearing and where $(t-1)^l$ appears n_l times. Then, choosing a basis vector from one of the elementary divisors $(t-1)^{l'}$ and acting on it by s, we have $sv_i^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l} a_{h,(l',j',i)}^{(l,j)} v_h^{(l,j)}$. Then, in fact, $sv_i^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{min\{i,l\}} a_{h,(l',j',i)}^{(l,j)} v_h^{(l,j)}$.*

Proof. First we know from Lemma 5.3 that since $xsv_1^{(l',j')} = sv_1^{(l',j')}$,

$$sv_1^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l} a_{1,(l',j',1)}^{(l',j')} v_1^{(l',j')},$$

that is, a linear combination of all basis vectors fixed by x. We can rewrite this as $sv_1^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{min\{1,l\}} a_{h,(l',j',1)}^{(l',j')} v_h^{(l',j')}$ since we are summing just when $h = 1$ as desired. Now assume, using strong induction, that

$$sv_i^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{min\{i,l\}} a_{h,(l',j',i)}^{(l,j)} v_h^{(l,j)}$$

for $i = 1, \ldots, r$. From Lemma 5.2, we have $xsv_{r+1}^{(l',j')} - sv_{r+1}^{(l',j')} = \sum_{\tau=1}^{r}(-1)^{r-t+1} sv_\tau^{(l',j')}$. Then by Equation 5.1, we have $xsv_{r+1}^{(l',j')} - sv_{r+1}^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l-1} a_{h+1,(l',j',r+1)}^{(l,j)} v_h^{(l,j)}$, and, by our induction hypothesis, $sv_\tau^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{\min\{\tau,l\}} a_{h,(l',j',\tau)}^{(l,j)} v_h^{(l,j)}$. Therefore,

$$\sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l-1} a_{h+1,(l',j',r+1)}^{(l,j)} v_h^{(l,j)} = \sum_{\tau=1}^{r}(-1)^{r-\tau+1}\sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{\min\{\tau,l\}} a_{h,(l',j',\tau)}^{(l,j)} v_h^{(l,j)}.$$

We observe that on the right-hand side sum, there are no $v_h^{(l,j)}$ terms where $h > r$. Therefore, all coefficients on the left-hand side of the form $a_{h+1,(l',j',r+1)}^{(l,j)}$ are 0 for

$h > r$. These are coefficients of $sv_{r+1}^{(l',j')}$ which are 0. Thus

$$sv_{r+1}^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{min\{r+1,l\}} a_{h,(l',j',r+1)}^{(l,j)} v_h^{(l,j)}.$$

□

Lemma 5.7. *Consider the unipotent element x in $\mathrm{U}(n,\mathbb{F}_{q^2})$ with elementary divisors of the form $(t-1)^l$ with $1 \leq l \leq m$ so m is the highest power of $(t-1)$ appearing, and $(t-1)^l$ has multiplicity n_l. Then we choose the fixed basis vector $v_1^{(l',j')}$ from one of the elementary divisors $(t-1)^{l'}$. Then $sv_1^{(l',j')}$ is a linear combination of the fixed vectors only from powers of $(t-1)$ greater than or equal to l'. That is, $sv_1^{(l',j')} = \sum_{l=l'}^{m}\sum_{j=1}^{n_l} a_{1,(l',j',1)}^{(l,j)} v_1^{(l,j)}$.*

Proof. From Lemma 5.3 we have that $sv_1^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l} a_{1,(l',j',1)}^{(l,j)} v_1^{(l,j)}$, so it is a linear combination of all fixed vectors. We also have from Equation 5.1, in general, $xsv_i^{(l',j')} - sv_i^{(l',j')} = \sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l-1} a_{h+1,(l',j',i)}^{(l,j)} v_h^{(l,j)}$. We have from Lemma 5.2 that $xsv_i^{(l',j')} = \sum_{\tau=1}^{i}(-1)^{i-t} sv_\tau^{(l',j')}$ so $xsv_i^{(l',j')} - sv_i^{(l',j')} = \sum_{\tau=1}^{i-1}(-1)^{i-t} sv_\tau^{(l',j')}$ so

$$\sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l-1} a_{h+1,(l',j',i)}^{(l,j)} v_h^{(l,j)} = \sum_{\tau=1}^{i-1}(-1)^{i-\tau}\sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{min\{\tau,l\}} a_{h,(l',j',\tau)}^{(l,j)} v_h^{(l,j)},$$

where the left-hand side is $xsv_i^{(l',j')} - sv_i^{(l',j')}$, and the right-hand side is the expansion of $\sum_{\tau=1}^{i-1}(-1)^{i-t} sv_\tau^{(l',j')}$.

Consider $l = i$. On the left-hand side, we sum from $h = 1$ to $h = i-1$ so there will only be one coefficient of $v_{i-1}^{(i,j)}$. On the right-hand side, we sum to $i-1$ as well when $\tau = i-1$. Thus, there is only one coefficient of $v_{i-1}^{(i,j)}$ on the right side as well, for each j. Therefore we obtain the equality $a_{i,(l',j',i)}^{(i,j)} v_{i-1}^{(i,j)} = -a_{i-1,(l',j',i-1)}^{(i,j)} v_{i-1}^{(i,j)}$ so $a_{i,(l',j',i)}^{(i,j)} = -a_{i-1,(l',j',i-1)}^{(i,j)}$ in general. Then we see that $(-1)^{i-1} a_{1,(l',j',1)}^{(i,j)} = (-1)^{i-2} a_{2,(l',j',2)}^{(i,j)} = \cdots = a_{i,(l',j',i)}^{(i,j)}$. We can now consider $xsv_{i+1}^{(l',j')} - sv_{i+1}^{(l',j')} = \sum_{\tau=1}^{i}(-1)^{i+1-\tau} sv_\tau^{(l',j')}$ so

$$\sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{l-1} a_{h+1,(l',j',i+1)}^{(l,j)} v_h^{(l,j)} = \sum_{\tau=1}^{i}(-1)^{i+1-\tau}\sum_{l=1}^{m}\sum_{j=1}^{n_l}\sum_{h=1}^{min\{\tau,l\}} a_{h,(l',j',\tau)}^{(l,j)} v_h^{(l,j)}.$$

Observe that when $l = i$, we only sum to $v_{i-1}^{(i,j)}$ on the left side so $a_{i,(l',j',i)}^{(i,j)} = 0$ because $v_i^{(i,j)}$ only appears on the right-hand side of the equation. It follows that $a_{1,(l',j',1)}^{(i,j)} = 0$ since $(-1)^{i-1} a_{1,(l',j',1)}^{(i,j)} = a_{i,(l',j',i)}^{(i,j)}$. Note here that there is no difference

if q is odd or if q is even since we are showing that these equal 0, so it does not matter if 1 or -1 is the sign of the coefficient.
We can use this method to simplify $sv_1^{(l',j')}$ by discovering which coefficients are 0 when it is written as a linear combination of all fixed vectors. We can perform this method of first examining $xsv_i^{(l',j')} - sv_i^{(l',j')}$ to obtain the equality $a^{(i,j)}_{i,(l',j',i)} = a^{(i,j)}_{i-1,(l',j',i-1)}$ and then examining $xsv_{i+1}^{(l',j')} - sv_{i+1}^{(l',j')}$ to see that $a^{(i,j)}_{i,(l',j',i)} = 0$ for $i = 2, \ldots, l'-1$ since there are l' basis vectors for the space spanned by the vectors $v_i^{(l',j')}$ corresponding to the elementary divisor $(t-1)^{l'}$.
That is, $xsv_2^{(l',j')} - sv_2^{(l',j')} = -sv_1^{(l',j')}$ shows us that $a^{(2,j)}_{2,(l',j',2)} = -a^{(2,j)}_{1,(l',j',1)}$ and the equation $xsv_3^{(l',j')} - sv_3^{(l',j')} = sv_1^{(l',j')} - sv_2^{(l',j')}$ shows that $a^{(2,j)}_{2,(l',j',2)} = 0$ so it follows that $a^{(2,j)}_{1,(l',j',1)} = 0$. We repeat this procedure through $i = l'-1$ and see that $a^{(i,j)}_{i,(l',j',i)} = 0$ for $i = 1, \ldots, l'-1$ and $j = 1, \ldots, n_i$ and thus $a^{(i,j)}_{1,(l',j',1)} = 0$ for the same i, j.
Therefore

$$\begin{aligned} sv_1^{(l',j')} &= \sum_{l=1}^{m}\sum_{j=1}^{n_l} a^{(l,j)}_{1,(l',j',1)} v_1^{(l,j)} \\ &= \sum_{l=l'}^{m}\sum_{j=1}^{n_l} a^{(l,j)}_{1,(l',j',1)} v_1^{(l,j)} \end{aligned}$$

as desired. □

5.2 Reduction of Unipotent Elements

Now we will describe a method of reducing unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$ to unipotents with simpler elementary divisors that we can work with. In general we wish to choose a certain number of vectors that are fixed by x to span W and then examine $W^{\perp}/W$ and its induced Hermitian form, unipotent element, and involution that reverses our unipotent element. This allows us to reduce certain powers of $(t-1)$ two at a time until we eventually get down to the case of $(t-1)^2 \cdots (t-1)^2 (t-1) \cdots (t-1)$ where we have only $(t-1)$ and $(t-1)^2$ appearing with some multiplicity. Since we know that strong reality of an element of $\mathrm{U}(n, \mathbb{F}_{q^2})$ depends only on its unipotent elementary divisors, in the end we conclude that this is the only case we must consider.

Lemma 5.8. *Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be unipotent with elementary divisors of the form $(t-1)^l$ for various l with multiplicity n_l. Let $(t-1)^m$ be the maximum power of $(t-1)$ that appears as an elementary divisor with $m \leq n$. Also let $H : V \times V \to \mathbb{F}_{q^2}$*

be a non-degenerate Hermitian form which is invariant under action of x. Let $W = \text{span}\{v_1^{(l,j)} : l' \leq l \leq m, 1 \leq j \leq n_l\}$ where $1 \leq l' \leq m$. That is, W is the span of the basis vectors fixed by x corresponding to elementary divisors of the form $(t-1)^l$ for $l \geq l'$. Then $xW = W$ and $xW^\perp = W^\perp$.

Proof. Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be as stated above. Let $W = \text{span}\{v_1^{(l,j)} : l' \leq l \leq m, 1 \leq j \leq n_l\}$. Then, from Lemma 5.5, we know that $W^\perp$, the subspace of V containing all vectors orthogonal to W with respect to the Hermitian form H, is the span of all vectors $v_k^{(l,j)}$ where $1 \leq k \leq l$ if $l < l'$ and $1 \leq k \leq l-1$ if $l \geq l'$, $j = 1, \ldots, n_l$. Let $w \in W$. Then w is a linear combination of the chosen vectors which span W, which are all fixed by x. Therefore $xw \in W$. Then $xW = W$. Now let $v \in W^\perp$. Then v is a linear combination of those vectors listed above that span $W^\perp$. For any vector $v_i^{(l,j)}$ for some choice of i, j, l such that the vector is in this list, it is true that $xv_i^{(l,j)} = v_i^{(l,j)} + v_{i-1}^{(l,j)}$ when $i > 1$ or $xv_i^{(l,j)} = v_i^{(l,j)}$ if $i = 1$. Then we observe that these vectors are still in $W^\perp$. Then since v is a linear combination of such vectors, xv will be a linear combination of such vectors as well and thus $xv \in W^\perp$. Then $xW^\perp = W^\perp$ as well. □

Lemma 5.9. *Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be unipotent with elementary divisors of the form $(t-1)^l$ for various l with multiplicity n_l. Let $(t-1)^m$ be the maximum power of $(t-1)$ that appears as an elementary divisor with $m \leq n$. Also let $H : V \times V \to \mathbb{F}_{q^2}$ be a non-degenerate Hermitian form which is invariant under action of x. Let $W = \text{span}\{v_1^{(l,j)} : l' \leq l \leq m, 1 \leq j \leq n_l\}$ where $1 \leq l' \leq m$. That is, W is the span of the basis vectors fixed by x corresponding to elementary divisors of the form $(t-1)^l$ for $l \geq l'$. Also, let x be strongly real in $\mathrm{U}(n, \mathbb{F}_{q^2})$ such that $sxs = x^{-1}$ for some involution $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$. Then $sW = W$ and $sW^\perp = W^\perp$.*

Proof. Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be as stated above. Let $W = \text{span}\{v_1^{(l,j)} : l' \leq l \leq m, 1 \leq j \leq n_l\}$. Then, from Lemma 5.5, we know that $W^\perp$ is the span of all vectors $v_k^{(l,j)}$ where $1 \leq k \leq l$ if $l < l'$ and $1 \leq k \leq l-1$ if $l \geq l'$, $j = 1, \ldots, n_l$. By Lemma 5.7, $sv_1^{(l',j)}$, $j = 1, \ldots, n_{l'}$, will be a linear combination of the fixed vectors from powers of $(t-1)$ greater than or equal to l', that is $sv_1^{(l',j)} = \sum_{l=l'}^{m} \sum_{j=1}^{n_l} a_{1,(l',j)}^{(l,j)} v_1^{(l,j)}$. If we consider $sv_1^{(\tilde{k},j)}$, $j = 1, \ldots, n_{k'}$ where $k' > l'$, then $sv_1^{(k',j)} = \sum_{l=k'}^{m} \sum_{j=1}^{n_l} a_{1,(k',j)}^{(l,j)} v_1^{(l,j)}$. Therefore, $sv_1^{(l,j)} \in W$ for $l \geq l'$, $j = 1, \ldots, n_l$. Since any $w \in W$ is a linear combination of these fixed vectors, $w = \sum_{l=l'}^{m} \sum_{j=1}^{n_l} \lambda_1^{(l,j)} v_1^{(l,j)}$. Then $sw = \sum_{l=l'}^{m} \sum_{j=1}^{n_l} \lambda_1^{(l,j)} sv_1^{(l,j)}$, so $sw \in W$. Thus $sW = W$. Also, from Lemma 5.7, we know that $sv_i^{(k,j')} = \sum_{l=1}^{m} \sum_{j=1}^{n_l} \sum_{h=1}^{min\{i,l\}} a_{h,(k,j',i)}^{(l,j)} v_h^{(l,j)}$, where we consider here $k \geq l'$. We observe that only the basis vectors $v_l^{(l,j)}$ for $l \geq l'$, $j = 1, \ldots, n_l$ are in $V \backslash W^\perp$. However, since we need consider only $sv_i^{(l,j)}$ where $i < l$ in $sW^\perp$, no linear combination will contain any vectors in $V \backslash W^\perp$. Thus $sW^\perp = W^\perp$. □

Theorem 5.10. *Let V be our n-dimensional $\mathbb{F}_{q^2}$-vector space, and let H be the non-degenerate Hermitian form on V that defines our unitary group. If q is odd, and if any unipotent $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ with elementary divisors $\overbrace{(t-1)^2, \ldots, (t-1)^2}^{2m+1 \text{ times}}, (t-1), \ldots, (t-1)$ is not strongly real, then Conjecture 1.3 is true for q odd. If q is even, and if any unipotent $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ with elementary divisors $\overbrace{(t-1)^3, \ldots, (t-1)^3}^{2k+1 \text{ times}}, (t-1)^2, \ldots, (t-1)^2, (t-1), \ldots, (t-1)$ is not strongly real, then Conjecture 1.3 is true for q even.*

Proof. Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be a unipotent element with elementary divisors of the form $(t-1)^l$ for various l with $1 \leq l \leq m$ with multiplicity n_l for $(t-1)^l$. Assume x is strongly real so $sxs = x^{-1}$ with $s^2 = 1$ for some $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$. Then to begin our reduction we choose $W = span\{v_1^{(m,1)}, v_1^{(m,2)}, \ldots, v_1^{(m,n_m)}, \ldots, v_1^{(l',1)}, \ldots, v_1^{(l',n_{l'})}\}$, the span of all fixed vectors of $(t-1)^l$ for $l \geq l'$. We will later discuss how to choose W algorithmically. It is important, however, that if we choose a vector corresponding to a power of $(t-1)^k$, then we must choose the fixed vector from all appearances of $(t-1)^k$. Also, we must then choose the fixed vector from all appearances of powers greater than k. Next, from Lemma 5.4, we know that $W^\perp$, the subspace of V containing all vectors orthogonal to W with respect to the form H, is the span of all vectors $v_{i_1}^{(l,j)}$ for $i_1 = 1, \ldots, l$ when $l < l'$ for $j = 1, \ldots, n_l$ and all vectors $v_{i_2}^{(l,j)}$ for $i_2 = 1, \ldots, l-1$ when $l \geq l'$, $j = 1, \ldots, n_l$. Then we can consider the $W^\perp/W$, a subspace of V with less dimension, which has an induced Hermitian form, say H_1. Here we define $H_1(v+W, u+W) = H(v,u)$ where $v, u \in W^\perp$.
From Lemma 5.8, we know that $xW = W$ and $xW^\perp = W^\perp$. Since x maps W into W and $W^\perp$ into $W^\perp$, x has an induced action as a unipotent element, say x_1 on $W^\perp/W$ where it preserves H_1. By our choice of W and thus $W^\perp$, we observe that x_1 acts as a unipotent element where each power $(t-1)^l$ for $l \geq l'$ in x is now $(t-1)^{l-2}$ in the list of elementary divisors of x_1. That is, by choosing the vector fixed by x corresponding to $(t-1)^l$ for $l \geq l'$ to be one of the spanning elements of W, we reduce the power of these elementary divisors by 2 in the induced unipotent element acting on $W^\perp/W$. If we are down to only elementary divisors of the form $(t-1)^2$, $(t-1)$ for q odd or $(t-1)^3$, $(t-1)^2$, $(t-1)$ for q even, then we can apply the same argument we saw earlier in the proof that regular unipotent elements in $\mathrm{U}(n, \mathbb{F}_{q^2})$ are not strongly real. That is, we know that our involution $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$ maps W into W and maps $W^\perp$ into $W^\perp$ and thus has an induced action on $W/W^\perp$ as an involutory isometry, say s_1, of H_1, which conjugates x_1 to x_1^{-1}. Then if we have reduced to multiplicities of $(t-1)^2$, $(t-1)$ for q odd or $(t-1)^3$, $(t-1)^2$, $(t-1)$ for q even, if x_1 is not strongly real by examining these elementary divisors, we have a contradiction which shows that x must then be not strongly real.

If we have not yet reduced to multiplicities of $(t-1)^2$, $(t-1)$ for q odd or $(t-1)^3$, $(t-1)^2$, $(t-1)$ for q even, then we can continue this process. We now begin with our non-degenerate Hermitian form $H_1 : W^\perp/W \times W^\perp/W \to \mathbb{F}_{q^2}$, our unipotent element x_1, and its reversing involution s_1. Now consider x_1 to have elementary divisors of the form $(t-1)^l$ where $1 \leq l \leq m_0$. First we must choose which powers of elementary divisors we wish to reduce, say all powers of $(t-1)$ greater than or equal to l_0'. Then we choose W_1 as expected. Let $W_1 = span\{v_1^{(m_0,1)}, \ldots, v_1^{(m_0,n_{m_0})}, \ldots, v_1^{(l_0',1)}, \ldots, v_1^{(l_0',n_{l_0'})}\}$. Then we know that $W_1^\perp$ must be the span of vectors $v_{i_1}^{(l,j)}$ for $i_1 = 1, \ldots, l$ when $l < l_0'$, $j = 1, \ldots, n_l$ and $v_{i_2}^{(l,j)}$ for $i_2 = 1, \ldots, l-1$, $j = 1, \ldots, n_l$. Again we have an induced nondegenerate Hermitian form H_2 on $W_1^\perp/W$ defined analogously to H_1. We again have an induced unipotent element acting on $W_1^\perp/W$ which preserves H_1, say x_2, and an induced involution which reverses x_2 and preserves H_1, say s_2 since, for the same reasons as above, $x_1W_1 = W_1$, $x_1W_1^\perp$, $s_1W_1 = W_1$, and $s_1W_1^\perp = W_1^\perp$. Now we see that each power of $(t-1)$ greater than or equal to l_0 is reduced by two in their appearance as elementary divisors of x_2. Now, if x_2 has elementary divisors that are multiplicities of $(t-1)^2$, $(t-1)$ for q odd or $(t-1)^3$, $(t-1)^2$, $(t-1)$ for q even, then we can check again if x_2 is strongly real or not. If it is not strongly real by its elementary divisors, then we have a contradiction, since x_2 is strongly real with $s_2x_2s_2 = x_2^{-1}$.
If we have not yet reduced the elementary divisors of our unipotent element to multiplicities of $(t-1)^2$, $(t-1)$ for q odd or $(t-1)^3$, $(t-1)^2$, $(t-1)$ for q even as elementary divisors of an induced unipotent element in a smaller unitary group, then we can continue this process for a finite number of steps before this reduction will be complete. □

Our general strategy for this reduction will be to first look at the highest even power of $(t-1)$, say $(t-1)^m$. If the multiplicity of $(t-1)^m$ is 1, then we are able to reduce to $(t-1)^2(t-1)\cdots(t-1)$ and obtain that our element is not strongly real as we show later. If not, we can still reduce to $(t-1)^2\cdots(t-1)^2(t-1)\cdots(t-1)$ for some multiplicities of $(t-1)^2$ and $(t-1)$. We do this by first choosing W to be the span of the fixed vectors from odd powers of $(t-1)$ greater than m. Then we reduce these odd powers by 2 by consecutively choosing W and then examining $W^\perp/W$ until we have m as the highest appearing power of $(t-1)$. Then we choose our next subspace W_1 to be the span of the fixed vector from $(t-1)^m$ and the fixed vectors from whatever powers we wish to reduce. That is, if we choose W to be the span of fixed vectors from elementary divisors of the form $(t-1)^k$ where $k > n$ for some $n > 1$, then for all powers $k > n$, we will reduce these powers to $k-2$ in the space $W^\perp/W$. We can continue this process until we reduce to $(t-1)^k$ for $k = 1, 2$.

Here is an example of the process where we have multiplicity one of the highest even power:

Example 5.11. Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ be unipotent with elementary divisors

$$(t-1)^7, (t-1)^7, (t-1)^6, (t-1)^5, (t-1)^5, (t-1)^4, (t-1)^4, (t-1)^2, (t-1)^2, (t-1), (t-1), (t-1).$$

Then first we wish to reduce the odd power of 7 so that our highest even power is the highest power remaining. Here we choose $W = span\{v_1^{(7,1)}, v_1^{(7,2)}\}$. Then $W^\perp$ will be all basis vectors except for $v_7^{(7,1)}$,$v_7^{(7,2)}$ since only $v_7^{(7,1)}$ and $v_7^{(7,2)}$ are not orthogonal to W. Then when we consider, $W^\perp/W$, we have reduced the space by dimension 4 since we mod out by the 2-dimensional space W, and we have two one-dimensional spaces that are in neither W or $W^\perp$. Thus, we have reduced these divisors $(t-1)^7$ to $(t-1)^5$ and we now have

$$(t-1)^6, (t-1)^5, (t-1)^5, (t-1)^5, (t-1)^5, (t-1)^4, (t-1)^4, (t-1)^2, (t-1)^2, (t-1), (t-1), (t-1)$$

for our induced unipotent element acting on $W^\perp/W$ along with an induced non-degenerate Hermitian form and reversing involution of our unipotent element. Our next step, now that we have our highest even power as the highest remaining power, is to keep that divisor as the highest remaining power by choosing our subspace $W_1 = span\{v_1^{(6,1)}, v_1^{(5,1)}, v_1^{(5,2)}, v_1^{(5,3)}, v_1^{(5,4)}, v_1^{(4,1)}, v_1^{(4,2)}\}$. We stop at the last $(t-1)^4$ since there is no $(t-1)^3$ appearing. Thus we can reduce this group of divisors all by power two in one step which is convenient. Here $W_1^\perp$ is the span of all basis vectors except for $v_6^{(6,1)}$,$v_5^{(5,1)}$,$v_5^{(5,2)}$, $v_5^{(5,3)}$, $v_5^{(5,4)}$, $v_4^{(4,1)}$, $v_4^{(4,2)}$. Our construction of $W_1^\perp/W_1$ reduces powers of $(t-1)$ greater than or equal to 4 by 2. Thus we have a new induced non-degenerate Hermitian form, unipotent element, and reversing involution acting on $W_1^\perp/W_1$. Now we have elementary divisors

$$(t-1)^4, (t-1)^3, (t-1)^3, (t-1)^3, (t-1)^3, (t-1)^2, (t-1)^2, (t-1)^2, (t-1)^2, (t-1), (t-1), (t-1).$$

For the next step we choose $W_2 = span\{v_1^{(l,j)} | l \geq 1, j = 1, \ldots, n_l\}$. Therefore $W_2^\perp$ is the span of all basis vectors except for $v_4^{(4,1)}$, $v_3^{(3,j)}$ for $j = 1, 2, 3$, $v_2^{(2,j)}$ for $j = 1, 2, 3, 4$. Then $W_2^\perp/W$ will have again an induced Hermitian form, unipotent element, and reversing involution in a smaller space where our induced unipotent element now has elementary divisors

$$(t-1)^2, (t-1), (t-1), (t-1), (t-1).$$

Our induced unipotent element should be strongly real with our induced reversing involution, but we know that any element with these elementary divisors is not

strongly real by Proposition 5.11 which we state next, so we have a contradiction. Therefore, our initial element must be not strongly real.

5.3 Base Case for q Odd

We have not yet proven whether or not our conjecture holds for any multiplicities of $(t-1)^2$, $(t-1)$. However, we do have the result for when the divisor $(t-1)^2$ appears only once.

Proposition 5.12. *Let x be a real element in $\mathrm{U}(n, \mathbb{F}_{q^2})$ and let V be a an n-dimensional vector space over $\mathbb{F}_{q^2}$ and $H : V \times V \to \mathbb{F}_{q^2}$ a non-degenerate Hermitian form used to define our unitary group. Let x act on V with elementary divisors $(t-1)^2, (t-1), \ldots, (t-1)$ where $(t-1)$ appears $n-2 = n_1$ times. Then x is not strongly real.*

Proof. First, we assume that x is strongly, that is, $sxs = x^{-1}$ for an involution $s \in \mathrm{U}(n, \mathbb{F}_{q^2})$. Since x has these elementary divisors, it is conjugate to $\begin{pmatrix} 1 & 1 & & 0 \\ 0 & 1 & & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$ in $\mathrm{GL}(n, \mathbb{F}_{q^2})$. Therefore we can choose a basis $\{v_1, v_2, \ldots, v_n\}$ such that $xv_1 = v_1$, $xv_2 = v_1 + v_2$, and $xv_i = v_i$ for $i = 3, 4, \ldots, n$. However, we will label these according to their respective elementary divisors as previously mentioned so $xv_1^{(2,1)} = v_1^{(2,1)}$, $xv_2^{(2,1)} = v_1^{(2,1)}$, and $xv_1^{(1,j)} = v_1^{(1,j)}$ for $j = 1, \ldots, n_1$. From Lemma 5.4, we obtain $H(v_1^{(2,1)}, v_2^{(2,1)}) \neq 0$ since H is non-degenerate, and $v_1^{(2,1)}$ is orthogonal to all other basis vectors in V. From Lemma 5.2, we also obtain that $xsv_1^{(2,1)} = sv_1^{(2,1)}$ so $xsv_1^{(2,1)} - sv_1^{(2,1)} = 0$. Then we have $sv_1^{(2,1)} = a_{1,(2,1,1)}^{(2,1)} v_1^{(2,1)} + \sum_{j=1}^{n_1} a_{1,(2,1,1)}^{(1,j)} v_1^{(1,j)}$. Also, $xsv_2^{(2,1)} = sv_2^{(2,1)} - sv_1^{(2,1)}$. Then $xsv_2^{(2,1)} - sv_2^{(2,1)} = -sv_1^{(2,1)}$ so

$$\sum_{l=1}^{2} \sum_{j=1}^{n_l} \sum_{h=1}^{l-1} a_{h+1,(2,1,2)}^{(l,j)} v_h^{(l,j)} = -\sum_{l=1}^{2} \sum_{j=1}^{n_l} a_{1,(2,1,1)}^{(l,j)} v_1^{(l,j)}.$$

We observe that when $l = 1$, the sum on the left-hand side vanishes, so we have $a_{1,(2,1,1)}^{(1,j)} = 0$ for $j = 1, \ldots, n_1$. Hence $sv_1^{(2,1)} = a_{1,(2,1,1)}^{(2,1)} v_1^{(2,1)}$, and, by Lemma 5.1, $sv_1^{(2,1)} = \pm v_1^{(2,1)}$. Also, we see that $a_{2,(2,1,2)}^{(2,1)} = -a_{1,(2,1,1)}^{(2,1)}$ when we let $l = 1$ and

observe the coefficients of $v_1^{(2,1)}$. Since s is unitary,

$$\begin{aligned} H(v_1^{(2,1)}, v_2^{(2,1)}) &= H(sv_1^{(2,1)}, sv_2^{(2,1)}) \\ &= H\left(a_{1,(2,1,1)}^{(2,1)} v_1^{(2,1)}, \sum_{l=1}^{2}\sum_{j=1}^{n_l}\sum_{h=1}^{l} a_{h,(2,1,2)}^{(l,j)} v_h^{(l,j)}\right) \\ &= H(a_{1,(2,1,1)} v_1^{(2,1)}, a_{2,(2,1,2)}^{(2,1)} v_2^{(2,1)}) \\ &= (a_{2,(2,1,2)}^{(2,1)})^q a_{1,(2,1,1)}^{(2,1)} H(v_1^{(2,1)}, v_2^{(2,1)}). \end{aligned}$$

Then $(a_{2,(2,1,2)}^{(2,1)})^q a_{1,(2,1,1)}^{(2,1)} = 1$. However, since $a_{2,(2,1,2)}^{(2,1)} = -a_{1,(2,1,1)}^{(2,1)}$ and $a_{1,(2,1,1)}^{(2,1)} = \pm 1$, we obtain $-1 = 1$ by either substitution, a contradiction. Thus x is not strongly real. □

This statement allows us to state our current result as follows:

Theorem 5.13. *Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$. If the highest even power of the elementary divisor $(t-1)$ appears with multiplicity one, then x is not strongly real.*

Proof. The statement follows from Theorem 5.9 and Proposition 5.11. We can use our reduction such that the highest even power is reduced to power 2 still with multiplicity one, and then we can apply Proposition 5.11. □

5.4 Odd Multiplicity of $(t-1)^2$

Although the previous statement is the best we can do currently, we can consider multiplicities of $(t-1)^2$ greater than one. Consider $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$, q odd, with elementary divisors $\overbrace{(t-1)^2 \cdots (t-1)^2}^{2m+1 \text{ times}}$. That is, we have the elementary divisor $(t-1)^2$ only appearing with odd multiplicity. Let H be our Hermitian form on the vector space V over $\mathbb{F}_{q^2}$. Now let $S = \{W : W$ is a 2-dimensional, non-degenerate, x-invariant subspace of V such that there is a basis w_1, w_2 where $xw_1 = w_1$ and $xw_2 = w_1 + w_2\}$. If S contains an odd number of subspaces W, then we are able to make a statement about the strong reality of x as follows:

Proposition 5.14. *If S contains an odd number of subspaces, then x is not strongly real in $\mathrm{U}(n, \mathbb{F}_{q^2})$, q odd.*

Proof. We will assume that x is strongly real in $\mathrm{U}(n, \mathbb{F}_{q^2})$ so $sxs = x^{-1}$ for some unitary involution s. Then in order to prove this statement, we will first show that s permutes the elements of S. Then we will use the fact that the number of subspaces in S is odd to provide a contradiction.

First we must show that if W is non-degenerate, then sW is also non-degenerate. Since W is non-degenerate, we know that if $H(w, v) = 0$ for all $v \in W$, then $w = 0$. Now assume that sW is degenerate. Then there exists $w' \in sW$, where $w' = sw$ for some $w \in W$, such that $H(w', v') = 0$ for all $v' \in sW$. Now consider any $v \in W$. Then $v = aw_1 + bw_2$, for some $a, b \in \mathbb{F}_{q^2}$ since w_1, w_2 is a basis for W. Also, $sv \in sW$ so $H(w', sv) = 0$ for any $v \in W$. Therefore, since s is an involution, $H(sw, sv) = H(w, v) = 0$ for any $v \in W$. Then W is degenerate, a contradiction. Thus, sW is a non-degenerate subspace of V.
We know that W is x-invariant by definition so $xW = W$. Therefore $x^{-1}W = W$ as well. Then $sxsW = x^{-1}W = W$ so $xsW = sW$. Hence sW is x-invariant as well. Now we need a basis in sW, say u_1, u_2 such that $xu_1 = u_1$ and $xu_2 = u_1 + u_2$. Let us begin with our basis w_1, w_2 in W. We know that $xw_1 = w_1$ so $x^{-1}w_1 = w_1$. Then $sxsw_1 = w_1$ so $xsw_1 = sw_1$. Now recall that $xw_2 = w_1 + w_2$ so $x^{-1}w_2 = w_2 - w_1$. Therefore $sxsw_2 = w_2 - w_1$ so $xsw_2 = sw_2 - sw_1$. Then let our basis be $u_1 = sw_1, u_2 = -sw_2$. Then $xsw_1 = sw_1$ and $x(-sw_2) = sw_1 - sw_2$ as desired. Thus, we obtain that $sW \in S$ so s permutes the elements of S. Also, since the order of s is 2, and the number of elements of S is odd, there exists some $U \in S$ such that $sU = U$. We know then that $sU = U$, $xU = U$, and thus $x^{-1}U = U$. Then $sxsU = U = x^{-1}U$ so $sxs = x^{-1}$. Here we observe that since U is 2-dimensional and x-invariant with a basis u_1, u_2 such that $xu_1 = u_1$ and $xu_2 = u_1 + u_2$, $x|_U$ is conjugate to $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ in $\mathrm{GL}(U)$. Then $x|_u$ has the lone elementary divisor $(t-1)^2$. We have just seen that $x|_u$ is strongly real since $sx|_u s = x|_u^{-1}$, a contradiction since we know that $x|_u$ cannot be strongly real with only the elementary divisor $(t-1)^2$. Thus, $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$ is not strongly real. □

5.5 q even

The results for q even are exactly the same as when q is odd except that the base case is different. That is, we are no longer attempting to reduce to only divisors of the form $(t-1)^2$ and $(t-1)$. Our new goal will be to reduce down to the base case of only elementary divisors of the form $(t-1)^3$, $(t-1)^2$, and $(t-1)$. We will give an example of a reduction.

Example 5.15. Let $x \in \mathrm{U}(n, \mathbb{F}_{q^2})$, q even, with elementary divisors

$$(t-1)^8, (t-1)^8, (t-1)^6, (t-1)^5, (t-1)^5, (t-1)^5, (t-1)^4, (t-1)^3, (t-1)^2, (t-1)^2, (t-1).$$

First we will choose $W = span\{v_1^{(8,1)}, v_1^{(8,2)}, v_1^{(6,1)}\}$ so $W^\perp$ will be the span of all basis vectors except for $v_8^{(8,1)}, v_8^{(8,2)}, v_6^{(6,1)}$. Then by considering the subspace $W^\perp/W$, we

have our induced unipotent element on this space, $\tilde{x}$ with elementary divisors

$$(t-1)^6, (t-1)^6, (t-1)^5, (t-1)^5, (t-1)^5, (t-1)^4, (t-1)^4, (t-1)^3, (t-1)^2, (t-1)^2, (t-1).$$

Now we let $W_1 = span\{v_1^{(6,1)}, v_1^{(6,2)}\}$. Then $W_1^\perp$ is the span of all basis vectors except for $v_6^{(6,1)}$ and $v_6^{(6,2)}$. Then we now can consider our induced unipotent element $\tilde{x_1}$ acting on $W_1^\perp/W_1$ with elementary divisors

$$(t-1)^5, (t-1)^5, (t-1)^5, (t-1)^4, (t-1)^4, (t-1)^4, (t-1)^4, (t-1)^3, (t-1)^2, (t-1)^2, (t-1).$$

Next we choose W_2 to be the span of the fixed vectors from each elementary divisor. Thus, when we consider the space $W_2^\perp/W_2$, we reduce the power of each divisor by 2 and the resulting unipotent element is $\tilde{x_2}$ acting on $W_2^\perp/W_2$ with elementary divisors

$$(t-1)^3, (t-1)^3, (t-1)^3, (t-1)^2, (t-1)^2, (t-1)^2, (t-1)^2, (t-1).$$

Now we have reduced to the base case for q even.

As of yet, however, we have no analogous statement to Proposition 5.11 for when q is even. However, since the reduction can be applied similarly, this base case is all we need to consider.

Chapter 6

Strongly Real Conjugacy Classes of the Symplectic Group

6.1 Embedding $\mathrm{Sp}(2n, \mathbb{F}_q)$ in $\mathrm{U}(2n, \mathbb{F}_{q^2})$

Before we discuss the conjugacy classes of the symplectic group, we will show that it can indeed be embedded inside the unitary group. It is immediate from the definition that the symplectic group is a subgroup of the general linear group, but it is not obvious that it also is a subgroup of the finite unitary group.

Proposition 6.1. *There is an isomorphic copy of* $\mathrm{Sp}(2n, \mathbb{F}_q)$ *embedded in* $\mathrm{U}(2n, \mathbb{F}_{q^2})$.

Proof. We know that $\mathrm{Sp}(2n, \mathbb{F}_q)$ is the group of isometries in V, an $\mathbb{F}_q$-vector space, of a non-degenerate alternating form, say $\langle\ ,\ \rangle : V \times V \to \mathbb{F}_q$. First we show that this form can be extended to a non-degenerate skew-Hermitian form on the $\mathbb{F}_{q^2}$-vector space $V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$, which we obtain here by extending by scalars. In order to show that we can extend our alternating form to a skew-Hermitian form, it suffices to show that for $u, v \in V$, $\langle\ u, v\ \rangle = -\overline{\langle v,\ u\rangle}$. First, since $\langle\ ,\ \rangle$ is an alternating form on V, we know that $\langle u,\ v\rangle = -\langle v,\ u\rangle$. Also, we know that $\langle u,\ v\rangle \in \mathbb{F}_q$ for any $u, v \in V$. Then $\overline{\langle v,\ u\rangle} = \langle v,\ u\rangle^q = \langle v,\ u\rangle$ so $\langle u,\ v\rangle = -\langle v,\ u\rangle = -\overline{\langle v,\ u\rangle}$ as desired.
Now we have extended our alternating form to a skew-Hermitian form $\langle\ ,\ \rangle : V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$. Now we must show that the group of $\mathbb{F}_{q^2}$ transformations preserving this non-degenerate skew-Hermitian form is isomorphic to the group of $\mathbb{F}_{q^2}$ transformations preserving the Hermitian form defined by $H(u, v) = \alpha\langle u,\ v\rangle$ for all $u, v \in V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$, where $\alpha \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$ such that $\bar{\alpha} = \alpha^q = -\alpha$, and $\alpha^2 = -1$. We know such an α exists because $\mathbb{F}_{q^2}$ is a quadratic extension of $\mathbb{F}_q$, and thus

there is some irreducible polynomial in $\mathbb{F}_q[t]$ of the form $t^2 - \beta$. In $\mathbb{F}_{q^2}[t]$, we have $t^2 - \beta = (t - \alpha)(t + \alpha)$ for some $\alpha \in \mathbb{F}_{q^2}$. Since $t^2 - \beta$ is irreducible over $\mathbb{F}_q$, it is given by the orbit of α under the map $\alpha \mapsto \alpha^2$, so $t^2 - \beta = (t - \alpha)(t - \alpha^q)$. Therefore, $\alpha^q = -\alpha$. Now we observe that this is indeed a Hermitian form since $\bar{\alpha} = -\alpha$ so $\overline{H(v,u)} = \overline{\alpha\langle v,\ u\rangle} = (-\alpha)(-\langle u,\ v\rangle) = \alpha\langle u,\ v\rangle = H(u,v)$, and linearity follows from the linearity of $\langle\ ,\ \rangle$.
Now first let τ be an $\mathbb{F}_{q^2}$ transformation preserving our skew-Hermitian form $\langle\ ,\ \rangle$, so $\langle \tau u,\ \tau v\rangle = \langle u,\ v\rangle$ for all $u, v \in V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$. Then $H(\tau u, \tau v) = \alpha\langle \tau u,\ \tau v\rangle = \alpha\langle u,\ v\rangle = H(u,v)$ so τ also preserves our Hermitian form H. Next, let σ preserve our Hermitian form H, so $H(\sigma u, \sigma v) = H(u,v)$ for all $u, v \in V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^2}$. Then $\alpha\langle \sigma u,\ \sigma v\rangle = \alpha\langle u,\ v\rangle$ so $\langle \sigma u,\ \sigma v\rangle = \langle u,\ v\rangle$. Therefore we have an isomorphism from the group of symplectic transformations preserving the non-degenerate alternating form $\langle\ ,\ \rangle$ to a subgroup of the unitary transformations preserving the Hermitian form H. □

6.2 Conjugacy Classes in $\mathrm{Sp}(2n, \mathbb{F}_q)$

We have already introduced the symplectic group $\mathrm{Sp}(2n, \mathbb{F}_q)$, which is a subgroup of both $\mathrm{GL}(2n, \mathbb{F}_q)$ and $\mathrm{U}(2n, \mathbb{F}_{q^2})$. Wall[9] gave a parameterization of the conjugacy classes of the symplectic group. These conjugacy classes are exactly the real conjugacy classes of $\mathrm{GL}(2n, \mathbb{F}_q)$ and $\mathrm{U}(2n, \mathbb{F}_{q^2})$ with some additional constraints on the elementary divisors $(t-1)$, $(t+1)$. Consider $g \in \mathrm{Sp}(2n, \mathbb{F}_q)$ and consider the symplectic matrix $J \in \mathrm{GL}(2n, \mathbb{F}_q)$, that is ${}^tJ = -J$. Since $g \in \mathrm{Sp}(2n, \mathbb{F}_q)$, we have ${}^tgJg = J$. Then ${}^tg = Jg^{-1}J^{-1}$ so ${}^tg$ is conjugate to g^{-1} in $\mathrm{GL}(2n, \mathbb{F}_q)$. Also, by Jordan canonical forms and elementary divisors, ${}^tg$ is conjugate to g in $\mathrm{GL}(2n, \mathbb{F}_q)$. Therefore g is conjugate to g^{-1} in $\mathrm{GL}(2n, \mathbb{F}_q)$ so g is real in $\mathrm{GL}(2n, \mathbb{F}_q)$. Also, g is conjugate to g^{-1} in $\mathrm{U}(2n, \mathbb{F}_{q^2})$ since a conjugacy class in $\mathrm{GL}(2n, \mathbb{F}_{q^2})$ intersects uniquely with $\mathrm{U}(2n, \mathbb{F}_{q^2})$ and we know that g is real in $\mathrm{GL}(2n, \mathbb{F}_{q^2})$ since it is real in $\mathrm{GL}(2n, \mathbb{F}_q)$.

We know now that the conjugacy classes of the symplectic group are the real classes in the general linear and unitary groups. Furthermore, these classes must satisfy another condition. Let the elementary divisors $(t-1)$ and $(t+1)$ be represented by the partitions $\lambda^{(1)}$ and $\lambda^{(-1)}$, respectively. Then for any odd j, $m_j(\lambda^{(1)})$ and $m_j(\lambda^{(-1)})$ must be even, where m_j is the multiplicity of part j in the partition. That is, all odd parts in the partition must appear with even multiplicity. We give an example of two conjugacy classes, one which is in $\mathrm{Sp}(2n, \mathbb{F}_q)$ and one which is not:

Example 6.2. Consider the conjugacy class of $g_1 \in \mathrm{GL}(2n, \mathbb{F}_q)$ with elementary

divisors $(t-1)^3, (t-1)^2, (t-1)^2, (t-1), (t-1), (t-1)$. Then since $(t-1)^3$ and also $(t-1)$ appear with odd multiplicity, this is a conjugacy class in $\mathrm{GL}(10, \mathbb{F}_q)$ but not in $\mathrm{Sp}(10, \mathbb{F}_q)$. That is, we look at the partition $\lambda^{(1)} = (3, 2, 2, 1, 1, 1)$, and it has odd parts with odd multiplicity, so this can not be a conjugacy class in the symplectic group.
Now consider the conjugacy class in $\mathrm{GL}(2n, \mathbb{F}_q)$ given by $(t-1)^3, (t-1)^3, (t-1)^2, (t-1)^2, (t-1), (t-1), (t-1), (t-1)$. Then our partition $\lambda^{(1)} = (3, 3, 2, 2, 1, 1, 1, 1)$. Observe that our odd parts 3 and 1 appear with even multiplicity so this is indeed a conjugacy class in $\mathrm{Sp}(14, \mathbb{F}_q)$.

Also, a real conjugacy class in $\mathrm{GL}(2n, \mathbb{F}_q)$ is not necessarily just one conjugacy class in the smaller symplectic group. It can, in fact, split into several conjugacy classes in $\mathrm{Sp}(2n, \mathbb{F}_q)$. We define a function $\delta : \{2i \in 2\mathbb{Z}_{\geq 1} | m_{2i}(\lambda) \neq 0\} \to \{\pm 1\}$ on the partitions $\lambda^{(1)}$ and $\lambda^{(-1)}$ where we assign each even part size a sign. Then this conjugacy class in $\mathrm{GL}(2n, \mathbb{F}_q)$ will split into 2^l conjugacy classes in $\mathrm{Sp}(2n, \mathbb{F}_q)$ if there are l distinct even parts in the partition. We will give an example:

Example 6.3. Consider the conjugacy class in $\mathrm{GL}(14, \mathbb{F}_q)$ given by elementary divisors $(t-1)^4, (t-1)^3, (t-1)^3, (t-1)^2, (t-1)^2$. Then we have the partition $\lambda^{(1)} = (4, 3, 3, 2, 2)$ We can assign each even part a sign, either positive or negative. Then we have the possible partitions $(4^+, 3, 3, 2^+, 2^+)$, $(4^+, 3, 3, 2^-, 2^-)$, $(4^-, 3, 3, 2^+, 2^+)$, and $(4^-, 3, 3, 2^-, 2^-)$. Thus, this class splits into four conjugacy classes in $\mathrm{Sp}(14, \mathbb{F}_q)$.

6.3 Strongly Real Classes in $\mathrm{Sp}(2n, \mathbb{F}_q)$

Since we know that conjugacy classes in $\mathrm{Sp}(2n, \mathbb{F}_q)$ are also classes in the larger group $\mathrm{U}(2n, \mathbb{F}_{q^2})$, we can use our results on strong reality in the unitary group to get some results in the symplectic group. We note that although the conjugacy classes in the symplectic group will have the assigned sign on the part sizes of even multiplicity in the partitions corresponding to the divisors $(t-1)$ and $(t+1)$, these conjugacy classes will simply correspond to the same conjugacy class in $\mathrm{U}(2n, \mathbb{F}_{q^2})$. Thus, if we know a class is strongly real in $\mathrm{Sp}(2n, \mathbb{F}_q)$, then the corresponding conjugacy class that it splits from in $\mathrm{U}(2n, \mathbb{F}_{q^2})$ is also strongly real. By the contrapositive, if a class is not strongly real in $\mathrm{U}(2n, \mathbb{F}_{q^2})$, then the corresponding classes that this class splits into in $\mathrm{Sp}(2n, \mathbb{F}_q)$ are not strongly real.

Corollary 6.4. *Let q be odd. If the highest even power of the elementary divisor $(t-1)$ appears with multiplicity one in the conjugacy class in* $\mathrm{Sp}(2n, \mathbb{F}_q)$*, then the conjugacy class is not strongly real.*

Proof. This statement follows directly from Theorem 5.9 and Proposition 5.11 since if the conjugacy class in $\mathrm{U}(2n, \mathbb{F}_{q^2})$ is not strongly real, then the conjugacy classes that it splits into in $\mathrm{Sp}(2n, \mathbb{F}_q)$ are not strongly real. □

Furthermore, for the same reason we can state the following:

Corollary 6.5. *Let q be odd. If Conjecture 1.3 is true, then if some even power of the elementary divisor $(t-1)$ appears with odd multiplicity in the conjugacy class in $\mathrm{Sp}(2n, \mathbb{F}_q)$, then the conjugacy class is not strongly real.*

Although this leaves us with work to do in describing the strongly real conjugacy classes of $\mathrm{Sp}(2n, \mathbb{F}_q)$, there are only partial results thus far such as that in Feit and Zuckerman [4], so we can at least begin with this statement following from our work in the finite unitary group.

Bibliography

[1] François Digne and Jean Michel. *Representations of finite groups of Lie type*, volume 21 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1991.

[2] David S. Dummit and Richard M. Foote. *Abstract algebra*. John Wiley & Sons Inc., Hoboken, NJ, third edition, 2004.

[3] Veikko Ennola. On the conjugacy classes of the finite unitary groups. *Ann. Acad. Sci. Fenn. Ser. A I No.*, 313:13, 1962.

[4] Walter Feit and Gregg J. Zuckerman. Reality properties of conjugacy classes in spin groups and symplectic groups. In *Algebraists' homage: papers in ring theory and related topics (New Haven, Conn., 1981)*, volume 13 of *Contemp. Math.*, pages 239–253. Amer. Math. Soc., Providence, R.I., 1982.

[5] Nick Gill and Anupam Singh. Real and strongly real classes in $\mathrm{SL}_n(q)$. *J. Group Theory*, 14(3):437–459, 2011.

[6] Rod Gow and C. Ryan Vinroot. Extending real-valued characters of finite general linear and unitary groups on elements related to regular unipotents. *J. Group Theory*, 11(3):299–331, 2008.

[7] Roderick Gow. Two multiplicity-free permutation representations of the general linear group $\mathrm{GL}(n, q^2)$. *Math. Z.*, 188(1):45–54, 1984.

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

[9] G. E. Wall. On the conjugacy classes in the unitary, symplectic and orthogonal groups. *J. Austral. Math. Soc.*, 3:1–62, 1963.

[10] María J. Wonenburger. Transformations which are products of two involutions. *J. Math. Mech.*, 16:327–338, 1966.