Involutions and regular semisimple elements in finite unitary groups of odd characteristic

Stephen Glasby, Cheryl E. Praeger and Colva M. Roney-Dougal

Abstract. We analyse the complexity of constructing centralisers of strong involutions in unitary groups over finite fields of odd order. Let $t$ be an involution in $\text{GU}_n(q)$, with fixed point space $E_+(t)$ of dimension between $n/3$ and $2n/3$ (a strong involution). For each $g \in \text{GU}_n(q)$ such that $tt^g$ has even order, there is a unique power $z(g)$ of $tt^g$ that is an involution, and $z(g) \in C_{\text{SU}_n(q)}(t)$. We prove that there exists a constant $\kappa > 0$ such that with probability at least $\kappa/\log n$, the restriction $z(g)|_{E_+(t)}$ is a strong involution, and similarly for $z(g)|_{E_-(t)}$. This enables us to prove logarithmic bounds on the number of random conjugates of $t$ required to generate a subgroup of $C_{\text{SU}_n(q)}(t)$ containing the last term of its derived series. This has consequences for the complexity of recognition algorithms for unitary groups in odd characteristic.

1. Introduction

Parker and Wilson showed in 2010 (see [12]) that involution-centraliser methods could be used to solve several computationally difficult problems, and gave complexity analyses for these algorithms in simple Lie type groups in odd characteristic. Central to these approaches are conjugate pairs $(t, tt^g)$ of involutions. If $g$ is a uniformly distributed element of a group $G$, and $y = tt^g$ has odd order $2k+1$, then $z = gy^k$ is an element of $C = C_G(t)$ (this observation dates back to Bray’s paper [2]). Furthermore, if $g$ is random and uniformly distributed in $G$, then $z$ is uniformly distributed in $C$. Parker and Wilson showed that if $G$ is a simple classical group of dimension $n$, then the proportion of $g \in G$ such that $tt^g$ has odd order is bounded below by $cn^{-1}$, for some constant $c$, so that with high probability $O(n)$ random elements $g$ suffice to construct such a random element $z$. Moreover, for infinitely many odd field orders, if $G$ is linear or unitary then the lower bound $cn^{-1}$ cannot be improved (see [12, bottom p. 897] and [1, Theorem 1.2]).

If $y$ has even order, then $y$ can also be used to construct an element $z$ of $C$; here $z$ is the power of $y$ that is an involution. However, these elements $z$ are not uniformly distributed in $C$; instead $z$ is uniformly distributed only within its $C$-conjugacy class.

Date: 30th November 2018.

Key words and phrases. Involution centralisers, recognition algorithms, classical groups, unitary groups, regular semisimple elements, group generation.
(Remark 11.3). In this paper we analyse the centralisers of strong involutions in unitary groups (Definition 1.1). We first analyse the fundamental case of conjugate involution pairs \((t, t^q)\) whose product \(y = tt^q\) is regular semisimple on the underlying vector space. We go on to show that there exists an absolute constant \(D\) such that \(D \log n\) random elements \(g\) suffice to construct a set of involutions that generate a group containing the last term in the derived series of \(C\). Our methods build on those of [14] and [3], but we encounter fundamental new difficulties, as the structure of regular semisimple elements in \(GU_n(q)\) that are “almost irreducible” (in a sense that we shall make precise in Definition 2.5) and conjugate to their inverses is very different from those in \(GL_n(q)\). In future work, we plan to address the symplectic and orthogonal groups. For these families of groups completely different arguments will be required: for example, one may readily compute that in \(Sp_4(3)\) and \(Sp_6(3)\) there are no regular semisimple elements that are inverted by involutions.

**Definition 1.1.** For an involution \(t \in GL_n(q^2)\), we write \(E_+ \) and \(E_-\) to denote its eigenspaces for eigenvalues \(+1\) and \(-1\). We say that such a \(t\) is **strong** if \(n/3 \leq \dim(E_+(t)) \leq 2n/3\).

For \(G\) a group, and \(x \in G\), we write \(\text{inv}(x)\) for \(x^{|x|/2}\) when \(|x|\) is even, and for \(1_G\) when \(|x|\) is odd.

**Definition 1.2.** A random variable \(x\) on a finite group \(G\) is **nearly uniformly distributed** if for all \(g \in G\) the probability \(\mathbb{P}(x = g)\) that \(x\) takes the value \(g \in G\) satisfies

\[
\frac{1}{2|G|} < \mathbb{P}(x = g) < \frac{3}{2|G|}.
\]

Our first main technical theorem is as follows.

**Theorem 1.** There exist positive constants \(\kappa, n_0 \in \mathbb{R}\) such that the following is true. Suppose that \(n \geq n_0\), that \(t\) is a strong involution in \(GU_n(q)\) with \(q\) odd, and that \(g\) is a nearly uniformly distributed random element of \(GU_n(q)\). Let \(z(g) := \text{inv}(tt^q)\), and let \(z(g)_\varepsilon\) be the restriction of \(z(g)\) to the eigenspace \(E_\varepsilon(t)\) \((\varepsilon = +\) or \(-)\). Then

(i) \(z(g)_+\) is a strong involution with probability at least \(\kappa/\log n\); and

(ii) \(z(g)_-\) is a strong involution with probability at least \(\kappa/\log n\).

Our proof shows that the values \(n_0 = 250\) and \(\kappa = 0.0001\) suffice. The comparable values in [3] for the case of special linear groups with nearly uniform random elements would be \(n_0 = 700, \kappa = 0.0001\), and echoing the view expressed there, ‘we believe that these constants are far from best possible’. From Theorem 1, we are able to deduce the following result (see Section 11).

**Theorem 2.** There exist constants \(\lambda, n_1 \in \mathbb{R}\) such that the following is true. Let \(n \geq n_1\), let \(G = GU_n(q)\) with \(q\) odd, let \(t \in G\) be a strong involution, let \(V_+ = E_+(t)\) and let \(V_- = E_-(t)\). Let \(A\) be a sequence of at least \(\lambda \log n\) random elements of \(G\), chosen independently and nearly uniformly, and let \(H = \langle \text{inv}(tt^q) : g \in A\rangle\). Then

\[
\mathbb{P}(H \text{ contains } SU(V_+) \times SU(V_-)) > 0.9(1 - q^{-n/3} - q^{-2n/3}).
\]
One of our motivations for proving the preceding two theorems was an application to computational group theory.

**Theorem 3.** There exists a constant \( \mu \in \mathbb{R} \) such that for all \( n > 2 \) and all odd \( q \), the following holds. There is a Las Vegas algorithm which on input a strong involution \( t \in GU_n(q) \), constructs generators for a subgroup of \( C_{GU_n(q)}(t) \) containing \( (C_{GU_n(q)}(t))^\infty \). It requires \( \mu \log n \) nearly uniformly distributed random elements and succeeds with probability at least 0.9\((1-q^{-n/3} - q^{-2n/3})\).

We focus now on the algorithm of Leedham-Green and O'Brien [9] for constructive recognition of special unitary groups. Let \( \xi \) denote an upper bound on the number of field operations needed to construct an independent nearly uniformly distributed random element of \( SU_n(q) \), and let \( \chi(q) \) be an upper bound on the number of field operations equivalent to a call to a discrete logarithm oracle for \( \mathbb{F}_{q^2} \). Reasoning in exactly the same way as [3, §1.1], the following theorem can be deduced from [9] and Theorem 3.

**Theorem 4.** There is a Las Vegas algorithm that takes as input a subset \( X \) of bounded cardinality in \( S = SU_n(q) \), with \( q \) odd, and returns standard generators for \( S \) as straight line programmes of length \( O(\log^3 n) \) in \( X \). The algorithm has complexity \( O(\log n(\xi + n^2\log n + n^2\log n\log n\log q + \chi(q^2))) \), measured in field operations.

To prove Theorem 1, we carry out an extensive analysis of the products of conjugate involutions in \( GU_n(q) \). Some of our results may be of independent interest, so in the remainder of this section we describe them.

**Definition 1.3.** An \( n \times n \) matrix \( y \) is regular semisimple if its characteristic polynomial \( c_y(X) \) is multiplicity-free.

An involution \( t \in GL_n(q^2) \) has type \((a,b)\) if \( \dim(E_+(t)) = a \) and \( \dim(E_-(t)) = b \). Given \( 0 \leq \alpha < \beta \leq 1 \), an involution \( t \in GL_n(q^2) \) of type \((n_+, n_-)\) is \((\alpha, \beta)\)-balanced if \( \alpha \leq n_+/n \leq \beta \). An involution \( t \in GL_n(q^2) \) of type \( ([n/2], [n/2]) \) is perfectly balanced.

Let \( V = \mathbb{F}_{q^2} \), equipped with a unitary form with Gram matrix \( I_n \). Following [14], we define \( \mathcal{C}(V) \) to be the class of perfectly balanced involutions in \( GL_n(q^2) \), with \( q \) odd, and we define \( \mathcal{C}_U(V) \) to be \( \mathcal{C}(V) \cap GU_n(q) \).

We let
\[
\textbf{I}_U(V) = \textbf{I}_U(n, q) = \{(t, t') \in \mathcal{C}_U(V) \times \mathcal{C}_U(V) \mid y := tt' \text{ is regular semisimple}\},
\]
and let \( \iota_U(n, q) = \iota_U(V) = \frac{|I_U(V)|}{|\mathcal{C}_U(V)|^2} \) be the probability that a random element of \( \mathcal{C}_U(V)^2 \) lies in \( I_U(V) \).

**Theorem 5.** Let \( \iota_U(n, q) \) be as above, with \( q \) odd. If \( n \neq 3 \), then \( \iota_U(n, q) > 0.25 \), whilst \( \iota_U(3, q) > 0.142 \).

**Remark 1.4.** We prove that for \( n \geq 4 \) even, \( \iota_U(n, q) > 0.343 \). We show in Lemma 11.4 that we can derive the probability \( \iota_U(n, q) \) for \( n \) odd from the even-dimensional case, and hence show that for \( n \geq 5 \) odd, \( \iota_U(n, q) > 0.254 \). We prove in Corollary 11.5 that the limits as \( m \to \infty \) of \( \iota_U(2m, q) \) and \( \iota_U(2m + 1, q) \) exist, and determine each limit.
The structure of this paper is as follows. In Section 2 we begin our exploration of the conjugacy classes in $\text{GU}_n(q)$, and of the characteristic polynomials of elements of $\text{GU}_n(q)$. In Section 3 we define a set of ordered pairs of conjugate involutions $(t, t^g)$ such that $\text{inv}(tt^g)|_{E(t)}$ is guaranteed to be a strong involution. Thus to prove Theorem 1 it suffices to show that this set is sufficiently large. In Sections 4, 5 and 6 we classify the $\text{U}^*$-irreducible regular semisimple elements of $\text{GU}_n(q)$ (that is, such elements that are as close to irreducible as possible, see Definition 2.5), determine their centralisers, and count the number of involutions inverting them. In Section 7 we calculate various upper and lower bounds on the number of monic polynomials that correspond to irreducible factors of the characteristic polynomials of these $\text{U}^*$-irreducible regular semisimple elements. In Section 8 we define and analyse our key generating function, $R_U(q, u)$. In Section 9 we factorise $R_U(q, u)$, in order control the dimension of the $-1$-eigenspace of $\text{inv}(tt^g)$, and prove bounds on the coefficients of certain generating functions that refine the information in $R_U(q, u)$. In Section 10 we prove Theorem 1, and finally in Section 11 we prove Theorems 2, 3 and 5.

1.1. Acknowledgements. The work for this paper began whilst the third author was a Cheryl E Praeger Visiting Research Fellow, and the authors are grateful for the hospitality of several academic institutions, including the Universities of St Andrews and Western Australia, and the Hausdorff Research Institute for Mathematics, Bonn. We are grateful for support from Australian Research Council, Discovery Project grants DP160102323 and DP190100450.

2. Preliminaries

In this section we study the conjugacy classes and characteristic polynomials of involutions in $\text{GU}_n(q)$ and of regular semisimple elements $y$ of $\text{GU}_n(q)$ that are products of involutions.

Recall from Definition 1.3 that we let $\text{GU}_n(q)$ act naturally on $V = \mathbb{F}_{q^2}^n$ with $q$ odd, and that unless stated otherwise, we take the sesquilinear form fixed by $\text{GU}_n(q)$ to have the identity matrix $I_n$ as its Gram matrix. Determining conjugacy in $\text{GU}_n(q)$ is straightforward:

**Theorem 2.1.** (Wall, [17, p.34]) Let $g, h \in \text{GU}_n(q)$. If $g$ and $h$ are conjugate in $\text{GL}_n(q^2)$ then they are conjugate in $\text{GU}_n(q)$.

The following corollary is immediate, since for $q$ odd, involutions in $\text{GL}_n(q^2)$ are conjugate if and only if they have the same type.

**Corollary 2.2.** Let $q$ be odd. For each type $(n_+, n_-)$ of involution in $\text{GL}_n(q^2)$, there exists a unique conjugacy class in $\text{GU}_n(q)$ containing involutions of that type. In particular, $C_U(V)$ is a $\text{GU}_n(q)$-conjugacy class.

We define three involutory operations on polynomials over $\mathbb{F}_{q^2}$. Let

$$f(X) := X^n + a_{n-1}X^{n-1} + \cdots + a_0,$$

(2)
where \( a_i \in \mathbb{F}_{q^2} \) for \( 0 \leq i \leq n - 1 \). Let \( \sigma \) be the involutory automorphism \( \sigma : x \mapsto x^q \) of \( \mathbb{F}_{q^2} \). Then we define the \( \sigma \)-\textit{conjugate polynomial} to be

\[
f^\sigma(X) := X^n + a_{n-1}^q X^{n-1} + \cdots + a_0^q.
\]

If \( a_0 \neq 0 \) then we also define the \textit{\( \ast \)-conjugate polynomial} to be

\[
f^\ast(X) := X^n + a_1 a_0^{-1} X^{n-1} + a_2 a_0^{-1} X^{n-2} + \cdots + a_{n-1} a_0^{-1} X + a_0^{-1},
\]

and define

\[
f^\sim(X) := f^{\sigma^T}(X) = f^{*\sigma}(X).
\]

It is clear that the \( \ast \) and \( \sim \) operations are involutions on the set of monic polynomials of degree \( n \) over \( \mathbb{F}_{q^2} \) with nonzero constant term.

By abuse of notation, we also write \( \sigma \) for the automorphism of \( \text{GL}_n(q^2) \) induced by replacing each matrix entry by its image under \( \sigma \). We write \( A^T \) for the transpose of a matrix \( A \), and \( h^\sim = h^\ast \sigma^T \) for \( h \in \text{GL}_n(q^2) \).

Our choice of unitary form means that \( h \in \text{GL}_n(q^2) \) lies in \( \text{GU}_n(q) \) if and only if \( h h^\ast \sigma^T = I \). In other words, we have the following.

**Lemma 2.3.** Let \( h \in \text{GL}_n(q^2) \). Then a conjugate of \( h \) lies in \( \text{GU}_n(q) \) if and only if \( h \) is conjugate to \( h^\sim \).

Notice that that the characteristic polynomial \( g(X) = c_h(X) \) of \( h \in \text{GL}_n(q^2) \) satisfies \( c_{h^\sim}(X) = g^\ast(X) \), and \( c_{h^\sim}(X) = g^\sim(X) \).

**Corollary 2.4.** Let \( y \in \text{GL}_n(q^2) \) be regular semisimple, and let \( g(X) = c_y(X) \).

(i) A conjugate of \( y \) lies in \( \text{GU}_n(q) \) if and only if \( g(X) = g^\sim(X) \).

(ii) If \( y \in \text{GU}_n(q) \) then \( y \) is conjugate in \( \text{GU}_n(q) \) to \( y^{-1} \) if and only if \( g(X) = g^\ast(X) \).

**Proof.** In both parts, one direction is clear, and the other follows from the fact that since \( y \) is regular semisimple, \( g(X) \) is equal to the minimal polynomial \( m_y(X) \), and \( c_y(X) \) is multiplicity-free. The fact that \( y \) and \( y^{-1} \) are conjugate in \( \text{GU}_n(q) \) (rather than just in \( \text{GL}_n(q^2) \)) follows from Theorem 2.1. \( \square \)

**Definition 2.5.** A polynomial over a field \( \mathbb{F} \) is \textit{separable} if it has no repeated roots in the algebraic closure \( \bar{\mathbb{F}} \). We say that a polynomial \( f(X) \in \mathbb{F}_{q^2}[X] \) is \textit{\( U \ast \)-closed} if \( f(X) = f^\sim(X) = f^\ast(X) \). Define \( \Pi(n,q) \) to be the set of separable, degree \( n \), monic, \( U \ast \)-closed polynomials over \( \mathbb{F}_{q^2} \) with no roots 0, 1, \(-1 \). We say that a polynomial \( g(X) \) is \textit{\( U \ast \)-irreducible} if \( g(X) = g^\ast(X) = g^\sim(X) \) and no proper nontrivial divisor \( f(X) \) of \( g(X) \) satisfies \( f(X) = f^\ast(X) = f^\sim(X) \).

The importance of the conjugacy class \( \mathcal{C}(V) \) of perfectly balanced involutions for studying regular semisimple elements is illustrated by the following result. Part (i) follows from [14, Lemma 3.1(a) and Table 1], Part (ii) is [14, Lemma 3.1(c)], and Part (iii) follows from [14, Lemma 3.1(b)(i)].

**Lemma 2.6 ([14, Lemma 3.1]).** Let \( t, y \in \text{GL}_n(q^2) \) with \( q \) odd, such that \( y \) is regular semisimple, and \( t \) is an involution inverting \( y \). Let \( t' = ty \).
(i) If $\gcd(c_y(X), X^2 - 1) = 1$, then all involutions inverting $y$ lie in $C(V)$ and $n$ is even.
(ii) If $t, t' \in \GL_n(q^2)$ are conjugate in $\GL_n(q^2)$ then either $t, t' \in C(V)$ or $-t, -t' \in C(V)$.
(iii) If $t, t' \in C(V)$ and $n$ is even, then $\gcd(c_y(X), X^2 - 1) = 1$.

For $n = 2m$, we define the following set, recalling that $C_U(V) = C(V) \cap GU_n(q)$:

$$\Delta_U(V) = \Delta_U(2m, q) := \left\{(t, y) \mid t \in C_U(V), y \in GU(V), y^t = y^{-1}, y \text{ regular semisimple, and } c_y(X) \text{ coprime to } X^2 - 1 \right\}.$$

This set is analogous to the set $RI(V)$ defined in \cite[Equation (3)]{14}. Recall Equation (1) defining $I_U(V)$, and Definition 2.5 of $\Pi_U(n, q)$. We now show the link between these sets.

**Lemma 2.7.** With respect to a fixed unitary form, $\Delta_U(n, q)$ is equal to the set

$$\{(t, y) \mid t \in GU_n(q), \ y \in SU_n(q), \ t^2 = 1, \ y^t = y^{-1}, c_y(X) \in \Pi_U(n, q)\}.$$

When $n$ is even, $|\Delta_U(n, q)| = |I_U(n, q)|$.

**Proof.** Let $S$ denote the displayed set. We show first that $S \subseteq \Delta_U(n, q)$, so let $(t, y) \in S$. Then $t$ inverts $y$, and our assumption that $c_y(X) \in \Pi_U(n, q)$ implies that $y$ is regular semisimple and $\gcd(c_y(X), X^2 - 1) = 1$. Hence it follows from Lemma 2.6 that $t \in C_U(V)$. Therefore $(t, y) \in \Delta_U(n, q)$.

Let $(t, y) \in \Delta_U(n, q)$. Since $y^t = y^{-1}$, with $y$ regular semisimple and $c_y(X)$ coprime to $X^2 - 1$, all involutions in $GU_n(q)$ inverting $y$ are in $C_U(V)$ by Lemma 2.6. Let $t' = ty$. Then $t'$ also inverts $y$, so by Lemma 2.6 $t' \in C(V)$. Hence, by Theorem 2.1 the involutions $t$ and $t'$ are conjugate in $GU_n(q)$. Then $y = tt'$ is a product of two conjugate involutions in $GU_n(q)$, and so $y \in SU_n(q)$. Therefore $(t, y) \in S$.

For the final claim, consider the map $\theta: (t, t') \mapsto (t, tt') = (t, y)$ from $I_U(V)$ to $C_U(V) \times GU(V)$. It is clear that $\theta$ is injective, and $c_y(X)$ is coprime to $X^2 - 1$ by Lemma 2.6(iii), so the image of $\theta$ is a subset of $\Delta_U(V)$. Hence $|I_U(V)| \leq |\Delta_U(V)|$. It follows from \cite[Lemma 4.1(a)]{14} that $\Delta_U(V) \subseteq \text{Im}(\theta)$, so these two sets have equal sizes.

## 3. Pairs of involutions yielding strong involutions

In this section, we characterise a certain set of ordered pairs of involutions $(t, t^g)$ from $GU_n(q)$ whose product $y = tt^g$ is such that $\text{inv}(y)|_{E_+(t)}$ is strong. Recall Definition 1.3 of the type of an involution, and that by Corollary 2.2 the types naturally parametrise the conjugacy classes of involutions in $GU_n(q)$. First we make a simple observation about subspaces of $E_+(t)$.

**Lemma 3.1.** Let $t \in GU_n(q)$ be an involution and let $U$ be a subspace of $E_+(t)$ acting on the natural formed space $V$ for $GU_n(q)$. Then $U^\perp$ is $t$-invariant, and further if $U$ is non-degenerate then also $U^\perp$ is non-degenerate and $U \cap U^\perp = 0$.

**Proof.** Let $u \in U$ and $w \in U^\perp$. Then, evaluating the form on $u$ and $w^t$ gives $(u, w^t) = (u^t, w)$ (since the form is $t$-invariant and $t^2 = 1$), and this is equal to zero since $w^t \in U$. Thus $(U^\perp)^t \subseteq U^\perp$ and we conclude that $(U^\perp)^t = U^\perp$. Finally, if $U$ is non-degenerate then $U \cap U^\perp = 0$ and thus also $U^\perp$ is non-degenerate.

\qed
DEFINITION 3.2. Let $K_{U,s}$ be the GU$_n(q)$-conjugacy class of involutions of type $(s, n-s)$, and fix $0 \leq \alpha < \beta \leq 1$. Define $L_U(n, s, q; \alpha, \beta)$ to be the set of pairs $(t, t') \in K_{U,s} \times K_{U,s}$ such that

(i) $V_1 := E_+(t) \cap E_+(t')$ is a non-degenerate subspace of the natural formed space $V$ for GU$_n(q)$, and has dimension $h = 2s-n$, (so, by Lemma 3.1, $V_2 := V_1^\perp$ is non-degenerate and $(t, t')$-invariant of dimension $n-h = 2(n-s)$);

(ii) $(t|V_2, t'|V_2) \in \Delta_U(n-h, q)$ and $\text{inv}(tt'|V_2)$ is $(\alpha, \beta)$-balanced.

LEMMA 3.3. Let $(t, t') \in L_U(n, s, q; \alpha, \beta)$, and let $V, V_1$ and $V_2$ be as in Definition 3.2. If $W$ is a $(t, t')$-invariant subspace of $V_2$, then $\dim W$ is even, and the involutions $t|_W$ and $t'|_W$ are both perfectly balanced.

PROOF. Lemma 2.7 shows that the characteristic polynomial for $tt'|V_2$ lies in $\Pi_U(2(n-s), q)$, and in particular it is coprime to $X^2 - 1$. Thus also, by Definition 2.5, the characteristic polynomial for $tt'|W$ lies in $\Pi_U(r, q)$, where $r = \dim(W)$, and so by Lemma 2.6, $r$ is even and $t|_W$ and $t'|_W$ lie in $C_U(W)$ (hence are perfectly balanced). \hfill \square

LEMMA 3.4. Let $s$ satisfy $2n/3 \geq s \geq n/2$, let $h = 2s-n$, let $\alpha := \max \left\{0, 1 - \frac{2s}{3(n-s)}\right\}$ and let $\beta := 1 - \frac{s}{3(n-s)}$. Then $\alpha < \beta$. Choose $(t, t') \in L_U(n, s, q; \alpha, \beta)$, and let $V_1$ and $V_2$ be as in Definition 3.2. Let $z = \text{inv}(tt')$. Let $V_2^+ := V_2 \cap E_+(z)$ and $V_2^- := E_-(z)$.

Then the following hold.

(i) Each entry in the table below is the dimension of the intersection of the subspaces at the heads of the row and column of the entry, and $k_+ + k_- = (n-h)/2 = n-s$.

| $V_1$ | $E_+(t)$ | $E_-(t)$ | $V$ |
|-------|---------|---------|-----|
| $V_2^+$ | $k_+$ | $k_+$ | $2k_+$ |
| $V_2^-$ | $k_-$ | $k_-$ | $2k_-$ |
| $V$ | $s$ | $n-s$ | $n$ |

(ii) $z|_{E_+(t)}$ is $(1/3, 2/3)$-balanced.

PROOF. It is clear from the definitions of $\alpha$ and $\beta$ that $0 \leq \alpha \leq 1/3$ and $1/3 \leq \beta \leq 2/3$, and that if $\alpha = 1/3$ then $\beta > 1/3$ so $\alpha < \beta$.

The first and last rows of the table in Part (i) are clear, so we need only prove the middle two rows.

Since $t$ is conjugate in GU$_n(q)$ to a diagonal matrix, and our standard unitary form is the identity matrix, the spaces $E_+(t)$ are non-degenerate, and $V = E_+(t) \perp E_-(t)$, so $E_-(t) = E_+(t)^\perp$. For the same reason $E_-(z) = E_+(z)^\perp$, so $V = E_+(z) \perp E_-(z)$.

By definition $V_1$ is fixed pointwise by $t$ and $t'$ and hence also by $z$, so that $E_+(z)$ contains both $V_1$ and $V_2^+$. Since $V_2^+ \subseteq V_2 = V_1^\perp$ we have $V_1 \perp V_2^+ \subseteq E_+(z)$. Since $V = V_1 \perp V_2$, an arbitrary element $v \in E_+(z)$ is of the form $v = v_1 + v_2$ for some $v_i \in V_i$ ($i = 1, 2$). Thus $v = vz = v_1z + v_2z = v_1 + v_2z$ whence $v_2 = v_2z \in V_2^+$. This yields $E_+(z) = V_1 \perp V_2^+$.
and hence also $V_{2-} = E_{-}(z) = E_{+}(z)^{1/2} \leq V_{1} = V_{2}$.

Let $D = (t, t')$. By Lemma 3.1, $V_{2}$ is $D$-invariant, and by definition $D$ centralises $z$. Hence $V_{2+}$ and $V_{2-}$ are $D$-invariant subspaces of $V_{2}$. It follows from Lemma 3.3 that, for $\varepsilon = \pm$, $V_{2\varepsilon}$ has even dimension, say $2k_{\varepsilon}$, and that $\dim(E_{+}(t) \cap V_{2\varepsilon}) = \dim(E_{-}(t) \cap V_{2\varepsilon}) = \frac{1}{2} \dim(V_{2\varepsilon}) = k_{\varepsilon}$. This proves the proof of Part (i).

It remains to prove Part (ii). Notice first that by Definition 3.2 the element $z|_{V_{2}}$ is $(\alpha, \beta)$-balanced, so we can bound $\alpha \leq \frac{2k_{1}}{n-h} = \frac{k_{1}}{n-s} \leq \beta$. Now consider $z' := z|_{E_{+}(t)}$, and notice that $E_{+}(z') = E_{+}(z) \cap E_{+}(t) = V_{1} \perp (V_{2+} \cap E_{+}(t))$ which by Part (i) has dimension $h + k_{+}$.

Since $\dim E_{+}(t) = s$, the element $z'$ is $(1/3, 2/3)$-balanced if and only if

$$1/3 \leq (h + k_{+})/s \leq 2/3.$$

Since $n/2 \leq s \leq 2n/3$ and $h = 2s-n$, we have $0 \leq h \leq n/3$. By Part (i), $k_{+} + k_{-} = n-s$, so $h + k_{+} + k_{-} = s$, and so $\frac{h+k_{+}}{s} = 1 - \frac{k_{-}}{s}$. From $\alpha \leq k_{+}/(n-s) \leq \beta$, we now deduce that

$$\frac{s}{3(n-s)} = 1 - \beta \leq 1 - \frac{k_{+}}{n-s} = \frac{k_{-}}{n-s} \leq 1 - \alpha \leq \frac{2s}{3(n-s)}.$$

Hence $\frac{s}{3} \leq k_{-} \leq \frac{2s}{3}$, which in turn implies that $\frac{1}{3} \leq 1 - \frac{k_{-}}{s} \leq \frac{2}{3}$, as required. $\square$

4. $U\ast$-irreducible polynomials

Recall Definition 2.5 of a $U\ast$-irreducible polynomial. In this section we classify the $U\ast$-irreducible polynomials, and determine the 2-part-orders of their roots (that is, the 2-parts of their orders). Recall the three involutory operations on polynomials that we defined in Section 2.

**Lemma 4.1.** Let $f(X) \in \mathbb{F}_{q}^{2}[X]$ be monic, irreducible, and of degree $\deg f = m$.

(i) If $f^{\ast}(X) = f(X)$ then either $f(X)$ is $X + 1$ or $X - 1$ or $m$ is even.

(ii) If $f^{\ast}(X) = f(X)$ then $m$ is odd.

(iii) If $f(X) \neq X \pm 1$ then at least one of $f^{\ast}(X), f^{\ast}(X)$ does not equal $f(X)$.

(iv) If $f(X) \neq X \pm 1$ and $f(X) = f^{-}(X)$ then $m$ is odd.

**Proof.** Parts (i) and (ii) are proved in [4, Lemma 1.3.15(c)] and [4, Lemma 1.3.11(b)], respectively. Part (iii) follows immediately from the Parts (i) and (ii), so we consider Part (iv). Suppose that $f(X) = f^{\ast}(X) \neq X \pm 1$. Since at least one of $f^{\ast}(X), f^{\ast}(X)$ is not equal to $f(X)$, whilst $f^{-}(X) = f^{\ast}(X) = f(X)$, we deduce that $f^{\ast}(X) = f^{\ast}(X) \neq f(X)$. Let $\zeta \in \mathbb{F}_{q^{2m}}$ be a root of $f$, so that $f(X) = m_{\mathbb{F}_{q^{2}}}(\zeta)$. Then the set of roots of $f^{\ast}$ is \{ξ, λξ, ηξ, . . . , ξq2m−1\} and the set of roots of $f^{\ast}$ is \{ξ−1, ξ−q2, . . . , ξ−q2m−2\}. Since these sets are equal, there exists an i such that $\zeta_{i} = \zeta^{q^{2i+1}}$, and this implies that $\zeta^{q^{2i+1}} = 1$, and hence that $\zeta \in \mathbb{F}_{q^{2i+2}} = \mathbb{F}_{q^{2i+1}}$, an odd degree extension of $\mathbb{F}_{q^{2}}$. $\square$

**Definition 4.2.** For a monic irreducible polynomial $f(X)$, we let $\omega(f)$ denote the order of one (and hence all) of its roots. Similarly we write $\omega(g)$ for the order of one (and hence all) of the roots of a $U\ast$-irreducible polynomial $g(X)$. We write $n_{2}$ for the 2-part of an integer $n$, and let $\omega_{2}(f)$ denote the 2-part of $\omega(f)$. A monic polynomial $g(X) \in \mathbb{F}_{q^{2}}[X]$ is said to be $U\ast$-closed if $g(X) = g^{\ast}(X) = g^{\ast}(X)$ (and hence also $g(X) = g^{\ast}(X)$).
We distinguish five possibilities for irreducible factors \( f(X) \) of \( c_y(X) \), where \( y \in \text{GU}_n(q) \) is regular semisimple, and conjugate to its inverse.

**Proposition 4.3.** Let \( y \in \text{GU}_n(q) \) be regular semisimple, and let \( g(X) = c_y(X) \in \mathbb{F}_q[X] \). Let \( f(X) \) be an irreducible factor of \( g(X) \), of degree \( m \). If \( y \) is conjugate to \( y^{-1} \) in \( \text{GU}_n(q) \), then \( g(X) \) is \( U \) is closed, and \( f(X) \) satisfies precisely one of the following:

**Case A.** \( f(X) = f^*(X) \neq f^\sigma(X) \). Thus \( f^\sim(X) = f^\sigma(X) \neq f(X) \), \( f(X)f^\sim(X) \mid c_y(X) \), and \( m \) is even, and \( \omega(f) \mid (q^m + 1) \).

**Case B.** \( f(X) = f^*(X) \neq f^\sigma(X) \). Thus \( f^\sim(X) = f^\sigma(X) \neq f(X) \), \( f(X)f^\sim(X) \mid c_y(X) \), and \( m \) is odd, and \( \omega(f) \mid (q^m - 1) \).

**Case C.** \( f(X) \neq f^*(X) \neq f^\sigma(X) \). Thus \( f^\sim(X) = f(X), \ f(X)f^\sim(X) \mid c_y(X), \ m \) is odd, and \( \omega(f) \mid (q^m - 1) \).

**Case D.** \( \{f(X), f^*(X), f^\sigma(X), f^\sim(X)\} = 4, \ f(X)f^*(X)f^\sigma(X)f^\sim(X) \mid c_y(X), \ \text{and} \ \omega(f) \mid (q^{2m} - 1) \).

**Case E.** \( f(X) = X \pm 1 \).

**Proof.** Since \( y \) is conjugate to \( y^{-1} \), we have \( g(X) = g^*(X) \), and by Corollary 2.4, \( g(X) = g^\sim(X) \). Thus \( g^*(X) = g^\sim(X) = g^\sigma(X) \), and hence also \( g(X) = g^\sigma(X) \), so \( g(X) \) is \( U \) is closed.

Since \( g(X) = g^*(X) \), the polynomial \( f^*(X) \) is an irreducible factor of \( g(X) \), and either \( f(X) = f^*(X) \) or \( f(X)f^*(X) \) divides \( g(X) \). Furthermore, since \( g(X) = g^\sim(X) \), the polynomial \( f^\sim(X) \) is an irreducible factor of \( g(X) \), and either \( f(X) = f^\sim(X) \) or \( f(X)f^\sim(X) \) divides \( g(X) \).

If \( f(X) = f^*(X) = f^\sigma(X) \) then, by Lemma 4.1, \( m = 1 \) and \( f(X) = X \pm 1 \), and we are in Case E. Assume now that \( \{f(X), f^*(X), f^\sim(X)\} \geq 2 \). Then it is easy to see that equalities between the polynomials, \( f(X), f^*(X), f^\sigma(X), f^\sim(X) \), and the divisibility concerning \( c_y(X) \), satisfy the conditions of precisely one of Cases A to D.

It remains to prove the claims about the parity of \( m \) and \( \omega(f) \). Let \( \zeta \) be a root of \( f \). In Case A, \( m \) is even by Lemma 4.1(i), and since \( f(X) = f^*(X) \), the set of roots of \( f(X) \) in \( \mathbb{F}_{q^{2m}} \) satisfy

\[
\{\zeta, \zeta^q, \ldots, \zeta^{q^{2m}-2}\} = \{\zeta^{-1}, \zeta^{-q}, \ldots, \zeta^{-q^{2m-2}}\}.
\]

Thus \( \zeta^{-1} = \zeta^{q^i} \) for some \( i \) with \( 0 < i \leq m - 1 \), and so \( \zeta^{q^{2i+1}} = 1 \), from which we deduce that \( \zeta \in \mathbb{F}_{q^i} \cap \mathbb{F}_{q^{2m}} = \mathbb{F}_{q^{\lfloor i+m/2 \rfloor}} \). If \( i \neq m/2 \) then \( 4(i, m/2) < 2m \), contradicting the irreducibility of \( f \). Hence \( q^{2i+1} = 1 \), as required.

Similarly, in Case B, the degree \( m \) is odd by Lemma 4.1(ii), and we deduce from \( f(X) = f^\sigma(X) \) with \( m \) odd that \( \zeta^{q^{2i+1}} = 1 \) for some \( i \) with \( 0 < i \leq m - 1 \), and hence that \( 2i + 1 = m \). In Case C we have \( m \) odd by Lemma 4.1(iv), and we use \( f(X) = f^\sigma(X) \) to reach a similar conclusion. For Case D, we shall see in Section 5 a construction of elements \( y \) that in no way depends on the parity of \( m \).

**Remark 4.4.** We shall eventually see that almost all irreducible polynomials lie in Case D, independent of the parity of \( m \).

**Remark 4.5.** Observe that Case E is equivalent to \( f(X) = f^*(X) = f^\sigma(X) \neq X \). Hence if \( \deg f > 1 \), then the hypotheses for cases A, B, C can be abbreviated to \( f(X) =
f^*(X), f(X) = f^\sigma(X), and f(X) = f^~(X), respectively. Indeed, f(X) = f^~(X) holds in Cases C and E only.

**Definition 4.6.** We shall refer to a U*-irreducible polynomial (not equal to X ± 1) as being in Case A, B, C or D, according to which of the above cases one (and hence all) of its irreducible factors belong.

**Definition 4.7.** Let \( N(q^2, r) \) denote the number of monic irreducible \( f(X) \in \mathbb{F}_{q^2}[X] \) of degree \( r \) with \( \gcd(f(X), X) = 1 \).

**Lemma 4.8 ([3, Lemma 2.11]).** Let \( \mathcal{P}_{r,q^2} \) be the set of monic irreducible polynomials \( f(X) \) of degree \( r \) over \( \mathbb{F}_{q^2} \) (\( q \) odd) with nonzero roots (so \( |\mathcal{P}_{r,q^2}| = N(q^2, r) \)). Then

(i) \( \omega_2(f) \leq (q^{2r} - 1)_2 \) for all \( f(X) \in \mathcal{P}_{r,q^2} \), and

(ii) \( \omega_2(f) = (q^{2r} - 1)_2 \) for at least \( \frac{1}{2}N(q^2, r) \) of the \( f(X) \in \mathcal{P}_{r,q^2} \).

If \( r = 2^b \) then \( \omega_2(f) = (q^{2r} - 1)_2 \) for exactly \( \frac{q^{2r} - 1}{2r} \) of the \( f(X) \in \mathcal{P}_{r,q^2} \).

**Definition 4.9.** Let \( \mathcal{D}_{4r} \) denote the set of all U*-irreducible polynomials of type D of degree \( 4r \) over \( \mathbb{F}_{q^2} \) (so that each irreducible factor has degree r). Let \( \mathcal{D}_{4r}^- \) be the subset of \( \mathcal{D}_{4r} \) consisting of those polynomials \( g \) with \( \omega_2(g) = (q^{2r} - 1)_2 = r_2(q^2 - 1)_2 \). Let \( N_\mathcal{U}^-(q, 4r) \) be the number of monic U*-irreducible polynomials \( g \) of degree \( 4r \) over \( \mathbb{F}_{q^2} \) such that \( \omega_2(f) = (q^{2r} - 1)_2 \).

**Lemma 4.10.** Let \( \Gamma \) denote the set of U*-irreducible polynomials in Cases A, B and C. Let \( r = 2^{b-1}m \), where \( b \geq 1 \) and \( m \) is odd. Then

(i) for each \( g(X) \in \Gamma \), \( \omega_2(g) < (q^2 - 1)_2 \).

(ii) for each \( g(X) \in \mathcal{D}_{4r} \), \( \omega_2(g) = \omega_2(f) \leq (q^{2r} - 1)_2 \), and at least \( \frac{1}{2}N(q^2, r) \) of the polynomials \( g(X) \in \mathcal{D}_{4r} \) have \( \omega_2(g) = (q^{2r} - 1)_2 \).

(iii) \( N_\mathcal{U}^-(q, 4r) = |\mathcal{D}_{4r}^-| \geq \frac{1}{8}N(q^2, r) \), with equality if \( r = 1 \); and if \( r = 2^{b-1} \) (that is, \( m = 1 \)) then \( N_\mathcal{U}^-(q, 4r) = (q^{2r} - 1)/8r \).

**Proof.** (i) This is immediately from Proposition 4.3 (for Case C, notice that \( r \) is odd and \( \omega(g) \mid (q^r + 1) \), hence \( \omega_2(g) \mid \frac{1}{2}(q^{2r} - 1)_2 = \frac{1}{2}(q^2 - 1)_2 \)).

(ii) Let \( g(X) \in \mathcal{D}_{4r} \). Then \( \omega_2(g) \mid (q^{2r} - 1)_2 \), by Proposition 4.3. By Lemma 4.8, \( \omega_2(f) = (q^{2r} - 1)_2 \) for at least \( \frac{1}{2}N(q^2, r) \) of the monic irreducibles in \( \mathcal{P}_{r,q^2} \) and these irreducibles have roots of greater 2-power order than those that correspond to irreducible factors of polynomials of type A, B or C, so the result follows.

(iii) The claim that \( |\mathcal{D}_{4r}^-| = N_\mathcal{U}^-(q, 4r) \) follows from Part (i), and the bound \( |N_\mathcal{U}^-(q, 4r)| \geq \frac{1}{8}N(q^2, r) \) follows from Part (ii).

Let \( r = 1 \). The set \( \mathcal{D}_{4}^- \) consists of U*-irreducible polynomials \( f(X)f^*(X)f^~(X)f^\sigma(X) \), with each factor of degree 1, over \( \mathbb{F}_{q^2}^* \), such that each root \( \zeta \) of \( f(X) \) has 2-power order \( (q^2 - 1)_2 \). Let \( \xi \) be any element of \( \mathbb{F}_{q^2}^* \) of maximal 2-power order. Then \( \xi \neq \xi^q, \xi \neq \xi^{-q} \) and \( \xi \neq \xi^{-q} \). Hence \( f(X) = X - \xi \) satisfies \( \{|f(X), f^\sigma(X), f^*(X), f^~(X)| = 4 \} \), and so \( f(X) \) is an irreducible polynomial of type D. There are \( (q^2 - 1)/2 \) elements of maximal 2-power order in \( \mathbb{F}_{q^2}^* \) (every nonsquare element), and we take them four at a time to make U*-irreducible polynomials, so \( |\mathcal{D}_{4}^-| = \frac{1}{8}(q^2 - 1) \).
Now consider \( r = 2^{2r-1} > 1 \). By Lemma 4.8, there are \((q^{2r} - 1)/(2r)\) degree \( r \) monic irreducibles \( f(X) \) over \( \mathbb{F}_{q^2} \) such that \( \omega_2(f) = (q^{2r} - 1)_2 \). Then Part (i) implies that each such \( f(X) \) corresponds to a \( U^* \)-irreducible polynomial \( g(X) \) of type \( D \), yielding exactly \((q^{2r} - 1)/(8r)\) such \( g(X) \). By Part (ii), each of these \( g(X) \) satisfies \( \omega_2(g) = (q^{2r} - 1)_2 \), and hence each such \( g(X) \) lies in \( \mathcal{D}_{4r} \). Conversely each polynomial in \( \mathcal{D}_{4r} \) is of this form. Hence \(|\mathcal{D}_{4r}| = (q^{2r} - 1)/(8r)\).

5. Centralisers and normalisers of \( U^* \)-irreducible, regular semisimple elements

In this section we investigate the centralisers and normalisers of elements of \( GU_n(q) \) that are regular semisimple, \( U^* \)-irreducible, and conjugate in \( GU_n(q) \) to their inverse. We also count the number of involutions in \( GU_n(q) \) that invert them. We work our way through the cases identified in Proposition 4.3.

The field \( \mathbb{F}_{q^{2m}} \) may be regarded as an \( m \)-dimensional vector space over \( \mathbb{F}_{q^2} \), and from this point of view the multiplicative group of \( \mathbb{F}_{q^{2m}} \) is a cyclic subgroup of \( GL_m(q^2) \) of order \( q^{2m} - 1 \) acting regularly on the nonzero vectors. There is a single conjugacy class of such subgroups of \( GL_m(q^2) \), and they are called Singer subgroups; their generators are Singer cycles. Thus if \( \langle z \rangle \cong C_{q^{2m-1}} \) is a Singer subgroup in \( GL_m(q^2) \) then we may identify the underlying vector space \( \mathbb{F}_{q^{2m}}^m \) with the additive group of the field \( \mathbb{F}_{q^{2m}} \), and \( \langle z \rangle \) with the multiplicative group \( \mathbb{F}_{q^{2m}}^* \), so that the Singer cycle \( z \) corresponds to multiplication by a primitive element \( \zeta \). Moreover, \( N_{GL_m(q^2)}(\langle z \rangle) = \langle z, s \rangle \cong C_{q^{2m-1}} \rtimes C_m \cong \Gamma L_1(\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2}) \), with \( s : z \mapsto q^2z \) corresponding to the field automorphism \( \phi : \zeta \mapsto \zeta q^2 \) of \( \mathbb{F}_{q^{2m}} \) over \( \mathbb{F}_{q^2} \) (see [5, Satz II.7.3]).

5.1. Singer subgroups and regular semisimple elements. In this subsection we change our unitary form, so that we can work with matrices written relative to a decomposition

\[
V = W_0 \oplus W_0^* \quad \text{where } W_0 \text{ and } W_0^* \text{ are totally isotropic subspaces.}
\]

Choose an ordered basis \( \langle v_1, \ldots, v_{2m} \rangle \) for \( V \) such that \( W_0 := \langle v_1, \ldots, v_m \rangle \) and \( W_0^* := \langle v_{m+1}, \ldots, v_{2m} \rangle \). For our analysis in this subsection it is convenient to choose the Gram matrix \( J \) of the unitary form to be

\[
J = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}.
\]

Denote by \( GU(J) \cong GU_{2m}(q) \) the matrix group \( \{ h \in GL_{2m}(q^2) \mid hJh^{\sigma T} = J \} \) (where \( T \) denotes matrix transpose). Consider the monomorphism

\[
\alpha : GL_m(q^2) \rightarrow GL_{2m}(q^2) \quad \text{defined by } a \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-\sigma T} \end{pmatrix}.
\]

To see that \( \alpha(a) \in GU(J) \), we show \( \alpha(a)J\alpha(a^{\sigma T}) = J \), or equivalently \( \alpha(a)^J = \alpha(a^{-\sigma T}) \):

\[
J^{-1}\alpha(a)J = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix} \begin{pmatrix} a & 0 \\ 0 & a^{\sigma T} \end{pmatrix} \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix} = \begin{pmatrix} a^{-\sigma T} & 0 \\ 0 & a \end{pmatrix} = \alpha(a^{\sigma T}).
\]
Thus the automorphism $a \mapsto a^{-\sigma T}$ of $GL_m(q^2)$ induces the automorphism $\alpha(a) \mapsto \alpha(a)^J$ on the image of $\alpha$.

5.2. Cases A and B: $|\{f, f^\sigma, f^*, f^\sim\}| = 2$, with $f(X) \neq f^\sim(X)$. To assist with our analysis of Cases A and B of Proposition 4.3, we first consider the more general situation where $y \in GU_{2m}(q)$ is a regular semisimple element with characteristic polynomial $f(X)f^\sim(X)$, where $f(X)$ is irreducible. We later add the condition that $y$ is conjugate to its inverse. We can then write $V = W \oplus W^\sim = \mathbb{F}^m_{q^2} \oplus \mathbb{F}^m_{q^2}$, where the restrictions $y|_W$ and $y|_W^\sim$ to $W$ and $W^\sim$ have characteristic polynomials $f(X)$ and $f^\sim(X)$, respectively. It follows from a result of Huppert [6,7] (see also [11, Lemma 2.4]) that the subspaces $W$ and $W^\sim$ are totally isotropic.

Before proceeding with our analysis we make a few general remarks.

Remark 5.1. Let $a \in GL_m(q)$. Then $a$ is conjugate in $GL_m(q)$ to its transpose. In fact, by a result of A. Voss [16] (see also [15, Theorem 1] or Kaplansky’s book [8, Theorem 66]), there is a symmetric matrix $c \in GL_m(q)$ which conjugates $a$ to its transpose, that is $c = c^T$ and $c^{-1}ac = a^T$.

Let $a \in GL_m(q)$ be irreducible, with characteristic polynomial $f(X)$. If $a' \in GL_m(q)$ is also irreducible and $\zeta^\ell$ is a root of its characteristic polynomial for some $\ell$, then $a'$ also has characteristic polynomial $f(X)$, and consequently $a'$ is conjugate to $a$ in $GL_m(q)$.

Lemma 5.2. Let $V = W_0 \oplus W_0^\sim$, with $W_0$ totally isotropic. Let $J$ be the Gram matrix of the form on $V$, as in (5), and let $\alpha$ be as in (6). Let $z \in GL_m(q^2)$ be a Singer cycle for $GL_m(q^2)$, and let $s \in N_{GL_m(q^2)}(z)$ be such that $z^s = z^{q^2}$.

(i) Let $H := \alpha(GL_m(q^2))$. Then $H$ is the stabiliser in $GU(V)$ of $W_0$ and $W_0^\sim$. The stabiliser of the decomposition $V = W_0 \oplus W_0^\sim$ is $\text{Stab}_{GU(J)}(W_0 \oplus W_0^\sim) = H : \langle J \rangle$.

(ii) Let $Z := \alpha(z)$. Then $C_{GU(J)}(Z) = \langle Z \rangle \cong C_{q^{2m-1}}$, and $N := N_{GU(J)}(\langle Z \rangle) = \langle Z, B \rangle \cong C_{q^{2m-1}}C_2m$, where $B = \alpha(b)J$ for some $b \in GL_m(q^2)$ such that $b^{-1}zb = z^{q^2T}$. Moreover, $Z^B = Z^{-q}$ and $B^2 = \alpha((b^{-1}T)^s) = \alpha(z^\ell s)$ for some $\ell \in \mathbb{Z}$.

(iii) Let $y \in GL_{2m}(q^2)$ be a regular semisimple element with characteristic polynomial $f(X)f^\sim(X)$, for some irreducible polynomial $f(X)$. Then some conjugate of $y$ lies in $\langle Z \rangle \leq GU(J)$, and has centraliser $\langle Z \rangle$, and normaliser $N$, in $GU(J)$.

Proof. (i) The fact that $H \leq GU(J)$ is immediate from (7). The spaces $W_0$ and $W_0^\sim$ are non-isomorphic irreducible $\mathbb{F}_{q^2}H$-submodules of $V$. Let $\hat{H} := \text{Stab}_{GU(J)}(W_0, W_0^\sim)$. Then $H \subseteq \hat{H}$. The restriction $\hat{H}|_{W_0} = H|_{W_0} \cong GL_m(q^2)$, and the subgroup $K$ of $\hat{H}$ fixing $W_0$ pointwise must fix the hyperplane $w^\perp \cap W_0^\sim$ of $W_0^\sim$ for each non-zero $w \in W_0$. Thus $K$ induces a subgroup of scalar matrices on $W_0^\sim$, and since $K \subseteq GU(J)$, this subgroup $K$ is trivial. It follows that $\hat{H} = H$. Finally each element of $\text{Stab}_{GU(J)}(W_0 \oplus W_0^\sim)$ either fixes setwise, or interchanges, the subspaces $W_0$ and $W_0^\sim$, and it is straightforward to check that $J \in GU(J)$ and interchanges these two subspaces. Hence $\text{Stab}_{GU(J)}(W_0 \oplus W_0^\sim) = H : \langle J \rangle$.

(ii) The spaces $W_0$ and $W_0^\sim$ are also non-isomorphic irreducible $\mathbb{F}_{q^2}\langle Z \rangle$-modules, so $C_{GU_{2m}(q)}(Z)$ fixes each of $W_0, W_0^\sim$ setwise, and so is contained in their stabiliser $H$, by Part (i). Since
$C_{\text{GL}_m(q^2)}(z) = \langle z \rangle \cong C_{q^{2m}-1}$ (see [5, Satz II.7.3]), it follows that $C_{\text{GU}_{2m}(q)}(Z) = \langle Z \rangle$. To prove the second assertion we note that since $N$ normalises $\langle Z \rangle$, the group $N$ must preserve the decomposition $V = W_0 \oplus W_0^\perp$. Thus $N \leq H : \langle J \rangle$, by Part (i). Also $N \cap H$ is the image under $\alpha$ of $N_{\text{GL}_m(q^2)}(\langle z \rangle)$, and this is $\langle \alpha(z), \alpha(s) \rangle$ (again see [5, Satz II.7.3]). Now $N \cap H$ has index at most 2 in $N$, and we shall construct an element $B \in N \setminus (N \cap H)$.

Let $f(X) = c_z(X)$, and let $\zeta$ be a root of $f(X)$. Then the roots of $f(X)$ are $\zeta^{2^i}$ for $0 \leq i \leq m - 1$. Since $|z| = q^{2m} - 1$, the element $z^\sigma$ is irreducible and one of its roots is $\zeta^\sigma$. Similarly $z^{q^\sigma}$ is irreducible and one of its roots is $(\zeta^\sigma)^\sigma = \zeta^q$. Hence, by Remark 5.1, $z$ is conjugate in $\text{GL}_m(q^2)$ to $z^{q^\sigma}$ which, in turn is conjugate to $z^{q^\sigma T}$. Let $b \in \text{GL}_m(q^2)$ be such that $b^{-1}zb = z^{q^\sigma T}$, and let $B := \alpha(b)J$. Then, using (7),

$$Z^B = (\alpha(z)^{\alpha(b)})^B = \alpha(z^b)^J = \alpha(z^{q^\sigma T})^J = \alpha((z^{q^\sigma T})^{-\sigma T}) = \alpha(z^{-q}) = Z^{-q}.$$  

In particular $B$ normalises $\langle Z \rangle$ and interchanges $W_0$ and $W_0^\perp$. Thus $N = \langle Z, \alpha(s), B \rangle$. A straightforward computation shows that $B^2$ and $\alpha(s)$ both conjugate $Z$ to $Z^\sigma$, so $B^2\alpha(s)^{-1} \in C_{\text{GU}(J)}(Z) = \langle Z \rangle$. Hence $N = \langle Z, B \rangle$, and $B^2 = \alpha(z^s)$ for some integer $\ell$. Another easy computation yields $B^2 = (\alpha(b)J)^2 = \alpha(b^{-1} - \sigma T)$, so $b^{-1} - \sigma T = z^{\ell}s$.

(iii) The fact that $y$ is conjugate to an element of $\text{GU}_{2m}(q)$, and hence to an element of $\text{GU}(J)$, is immediate from Corollary 2.4. The primary decomposition of $V$ with respect to $y$, as discussed before the statement, is $V = W \oplus W^\perp$ such that both $W$ and $W^\perp$ are totally isotropic, and the restrictions of $y$ to $W$ and $W^\perp$ are irreducible with characteristic polynomials $f(X)$ and $f^\perp(X)$, respectively. Since $\text{GU}(J)$ is transitive on ordered pairs of disjoint totally isotropic $m$-dimensional subspaces, replacing $y$ by a conjugate, if necessary, we may assume that $W = W_0$ and $W^\perp = W_0^\perp$.

Then $y$ fixes both $W_0$ and $W_0^\perp$ setwise, and hence $y = \alpha(y_0)$ for some $y_0 \in \text{GL}_m(q^2)$, by Part (ii). From the definition of $\alpha(y_0)$, we have $y_0 := y|_{W_0}$. It follows from [5, Satz II.7.3] that there is an element $c \in \text{GL}_m(q^2)$ such that $y_0 \in \langle z \rangle$ and $N_{\text{GL}_m(q^2)}(\langle y_0 \rangle)^c = N_{\text{GL}_m(q^2)}(\langle z \rangle) = \langle z, s \rangle$. Thus, replacing $y$ by its conjugate $y^{\alpha(c)}$, we have $C_{\text{GU}_{2m}(q)}(y) = C_{\text{GU}_{2m}(q)}(Z) = \langle Z \rangle$ and $N_{\text{GU}_{2m}(q)}(\langle y \rangle) \cap H = \langle Z, \alpha(s) \rangle$. Since $N_{\text{GU}_{2m}(q)}(\langle y \rangle)$ normalises $C_{\text{GU}_{2m}(q)}(y) = \langle Z \rangle$, it is contained in $N$, and since the element $B = \alpha(b)J$ normalises the cyclic group $\langle Z \rangle$, it also normalises the subgroup $\langle y \rangle$. Thus $N_{\text{GU}_{2m}(q)}(\langle y \rangle) = N$.

As a corollary we count the number of involutions which invert an element $y$ as in Lemma 5.2(iii).

**Corollary 5.3.** Let $y \in \text{GL}_{2m}(q^2)$ be regular semisimple, with $U^\ast$-irreducible characteristic polynomial $g(X) = f(X)f^\perp(X)$, where $f(X)$ is irreducible and $f(X) \neq f^\perp(X)$. Then up to conjugacy $y \in \text{GU}_{2m}(q)$, and some element of $\text{GU}_{2m}(q)$ inverts this conjugate of $y$ if and only if one of the following holds.

(i) Case $A$ holds for $f(X)$. In this case exactly $q^m + 1$ involutions invert $y$.

(ii) Case $B$ holds for $f(X)$. In this case exactly $q^m - 1$ involutions invert $y$.

**Proof.** Note that $f(X) \neq X \pm 1$ since $f(X) \neq f^\perp(X)$, and hence, in particular, $|y| > 2$. Let $z$, $W_0$ and $N = \langle Z, B \rangle$ be as in Lemma 5.2. By Lemma 5.2, we may assume up to conjugacy that $y = \alpha(z^i)$ for some $i \in \{1, \ldots, q^{2m} - 2\}$ such that $z^i$ is
irreducible on $W_0$, and any element of $\text{GU}_{2m}(q)$ that inverts $y$, if such exists, must lie in $N$. If $n, n'$ are two elements inverting $y$, then $n'n^{-1}$ centralises $y$ and hence, by Lemma 5.2(iii), $n' = \alpha(z')n$, for some $i$. Moreover, if $n$ inverts $y$ then certainly $\alpha(z')n$ also inverts $y$ for each $i$. Hence either $0$ or $|z| = q^{2m} - 1$ elements invert $y$. We show first that such inverting elements exist, in both cases, and then we count the number of them which are involutions.

It follows from Lemma 5.2(ii) that any inverting element $n \in \text{GU}_{2m}(q)$ is of the form $n = \alpha(z^j)B^k \in N$ for some $j, k$ such that $0 \leq j \leq q^{2m} - 2$ and $1 \leq k \leq 2m - 1$. Note that $k \neq 0$ since $|y| > 2$ implies that $n$ does not centralise $y$. Recall from Lemma 5.2(ii) that $Z^B = Z^{-q}$, so that $y^B = y^{-q}$.

Suppose first that $k$ is even. Then

$$y^{-1} = n^{-1}yn = y^q$$

and so $z'^q = z^{-i}$, which is equivalent to $z^{i(q^k+1)} = 1$. This implies that $z^i \in \mathbb{F}_{q^k} \cap \mathbb{F}_{q^{2m}} = \mathbb{F}_{q^{2(k,m)}}$ (identifying $z$ with an element of $\mathbb{F}_{q^{2m}}$). However, $z^i$ acts irreducibly on $\mathbb{F}_q$, so $z^i$ lies in no proper subfield of $\mathbb{F}_{q^{2m}}$ that contains $\mathbb{F}_q$. Hence $k = m$, and in particular $m$ is even (since $k$ is assumed to be even), and we are in Case $A$ by Proposition 4.3. Here $|y| = |z^i|$ divides $q^m + 1$, and hence $n = \alpha(z^j)B^m$ inverts $y$ for each $j \in \{0, \ldots, q^{2m} - 2\}$.

Now suppose that $k$ is odd. Then

$$y^{-1} = n^{-1}yn = y^{-q}$$

and so $z^{i(q^k-1)} = 1$, whence $z^i \in \mathbb{F}_{q^k} \cap \mathbb{F}_{q^{2m}} = \mathbb{F}_{q^{2(k,m)}} \subset \mathbb{F}_{q^{2(k,m)}}$ since $k$ is odd. As in the previous case, $z^i$ lies in no proper subfield of $\mathbb{F}_{q^{2m}}$ containing $\mathbb{F}_q$. Hence $(k, m) = m$, so again $k = m$. Thus $m$ is odd (since $k$ is odd), and we are in Case $B$ by Proposition 4.3. Here $|y| = |z^i|$ divides $q^m - 1$, and hence $n = \alpha(z^j)B^m$ inverts $y$, for each $j \in \{0, \ldots, q^{2m} - 2\}$.

We now count the inverting involutions in each case. First observe that, by Lemma 5.2(ii), $B^2 = \alpha(z^zs)$ for some $\ell \in \{0, \ldots, q^{2m} - 2\}$, where $s^{-1}zs = z^q$, with $z^{q^m-1} = 1$ and $s^m = 1$. Hence

$$B^{2m} = \alpha(z^zs)^m = \alpha((z^zs)^{m-1}sz^{\ell q}) = \cdots = \alpha(z^{\ell(q^m-1)/(q^2-1)})$$

(8)

Case $A$: Each inverting element is of the form $n = \alpha(z^j)B^m$, for some $j \in \{0, \ldots, q^{2m} - 2\}$, and $m$ is even. Such an element $n$ is an involution if and only if

$$1 = n^2 = \alpha(z^j)B^m \alpha(z^j)B^m = \alpha(z^j)\alpha(z^{j(q^m)})B^2m = \alpha(z^{j(q^m+1)})B^{2m}.$$ 

Hence, by (8), $n^2 = 1$ if and only if $q^{2m} - 1$ divides $j(q^m + 1) + \ell \frac{q^{2m}-1}{q^2-1}$. Since $m$ is even, this holds if and only if $q^m - 1$ divides $j + \ell \frac{q^{2m}-1}{q^2-1}$. In particular $j = j'q_{m-1}(q^2-1)$ (there are $(q^m + 1)(q^2-1)$ integers $j$ with this property in $\{1, \ldots, q^{2m} - 2\}$), and in addition $q^2 - 1$ divides $j' + \ell$. Thus we have exactly $q^m + 1$ possibilities for $j$, and hence there are exactly $q^m + 1$ involutions which invert $y$.

Case $B$: Each inverting element is of the form $n = \alpha(z^j)B^m$, for some $j \in \{0, \ldots, q^{2m} - 2\}$, and $m$ is odd. Such an element $n$ is an involution if and only if

$$1 = n^2 = \alpha(z^j)B^m \alpha(z^j)B^m = \alpha(z^j)\alpha(z^{-jq^m})B^2m = \alpha(z^{-j(q^m-1)})B^{2m}.$$
Thus, by (8), \( n^2 = 1 \) if and only if \( q^{2m} - 1 \) divides \(-j(q^m - 1) + \ell q^{2m-1} \). In particular we require \( q^m - 1 \) to divide \( \ell q^{2m-1} \), or equivalently, \( \ell q^{m+1} \) must be an integer. Given this condition, \( n^2 = 1 \) if and only if \( q^m + 1 \) divides \(-j + \ell q^{m+1} \). As \( j \) runs through \( \{0, \ldots, q^{2m} - 2\} \), there are exactly \( q^m - 1 \) values with this property. Thus there are either 0 or \( q^m - 1 \) inverting involutions. To prove the latter holds, we construct an inverting involution.

We have \( m \) odd and \( f(X) = f^\sigma(X) \), so that all of the coefficients of \( f(X) \) lie in \( \mathbb{F}_q \), and hence all of its roots lie in \( \mathbb{F}_{q^m} \). This means that some conjugate of \( z^i \) by an element of \( \text{GL}_m(q^2) \) lies in \( \text{GL}_m(q) \) (the subgroup of \( \text{GL}_m(q^2) \) of matrices with entries in \( \mathbb{F}_q \)). We may therefore conjugate \( y = \alpha(z^i) \) by an element of \( \alpha(\text{GL}_m(q^2)) \subseteq \text{GU}_{2m}(q) \) (see (6)) and obtain an element in \( \alpha(\text{GL}_m(q)) \). Let us replace \( y \) by this element so that \( y = \alpha(z^i) \) with \( z^i \in \text{GL}_m(q) \). By Remark 5.1, there is a symmetric matrix \( c \in \text{GL}_m(q) \) which conjugates \( z^i \) to its transpose, that is, \( c = c^T \) and \( c^{-1} z^i c = (z^i)^T \). Note that \((z^i)^T = (z^1)^\sigma T \) and \( c^\sigma T = c \), since \( z^i, c \in \text{GL}_m(q) \) and \( c = c^T \). Therefore \( c^\sigma(z^i)^{-\sigma} c^\sigma T = (c^{-1} z^{-i})^T = z^{-i} \), and it follows from (6) that \( \alpha(c)^{-1} y \alpha(c) \) is the block diagonal matrix \( \alpha(z^T) \) with diagonal components \( z^T, z^{-i} \). Thus \( C := \alpha(c).J \) conjugates \( y \) to \( \alpha(z^{-i}) = y^{-1} \). Moreover \( J \alpha(c) J = \alpha(c^{-\sigma T}) = \alpha(c^{-1}) \), and hence \( C^2 = \alpha(c) J \alpha(c) J = \alpha(c) \alpha(c^{-1}) = 1 \), that is, \( C \) is an involution inverting \( y \).

5.3. Case C: \(|\{f(X), f^\sigma(X), f^*(X), f^{\sim}(X)\}| = 2, f = f^{\sim} \). Here we consider a regular semisimple element \( y \in \text{GU}_{2m}(q) \) with \( U^* \)-irreducible characteristic polynomial
\[
c_y(X) = f(X) f^*(X),
\]
where \( f(X) = f^{\sim}(X) \) has degree \( m \). So \( y \) is in Case C of Proposition 4.3, and in particular \( m \) is odd. The primary decomposition of \( V \) as an \( \mathbb{F}_{q^2}(y) \)-module is \( V = U \oplus U^* \), where the restrictions \( y_1 := y|_U \) and \( y_2 := y|_{U^*} \) have characteristic polynomials \( f(X) \) and \( f^*(X) \), respectively. Then (for example see \( [6, 7] \)) each of \( U \) and \( U^* \) is non-degenerate, so \( U^* = U^\perp \). For the analysis in this subsection it is convenient to work with matrices with respect to an ordered basis \( \{v_1, \ldots, v_{2m}\} \) where \( U = \langle v_1, \ldots, v_m \rangle \) and \( U^* = \langle v_{m+1}, \ldots, v_{2m} \rangle \), and with the Gram matrix \( J = I_{2m} \). The stabiliser in \( \text{GU}_{2m}(q) \) of the subspace \( U \) (and hence also of \( U^* = U^\perp \)) is then \( H := \text{Stab}_{\text{GU}_{2m}(q)}(U) = \text{GU}(U) \times \text{GU}(U^*) \cong \text{GU}_{m}(q) \times \text{GU}_{m}(q) \). It is convenient to write elements of \( H \) as pairs \( (h, h^\prime) \) with \( h, h^\prime \in \text{GU}_{m}(q) \). The stabiliser in \( \text{GU}_{2m}(q) \) of the decomposition \( V = U \perp U^* \) is \( H := H \cdot \langle \tau \rangle \), where \( \tau : (h, h^\prime) \mapsto (h^\prime, h) \) for \( (h, h^\prime) \in H \).

By \([5, \text{Satz II.7.3}]\), we may replace \( y \) by a conjugate in \( H \) such that \( y_1 \) and \( y_2 \) are contained in the same Singer subgroup \( \langle z \rangle \cong C_{q^m+1} \) of \( \text{GU}_m(q) \), and moreover, such that \( y_2 \) is equal to \( y_1^{-1} \).

**Lemma 5.4.** Let \( y \in \text{GL}_{2m}(q^2) \) be regular semisimple, with \( c_y(X) \) a \( U^* \)-irreducible polynomial in Case C. Then up to conjugacy, \( y \in \text{GU}_m(q) \), \( m \) is odd, and with the notation from the previous two paragraphs
\[
\begin{align*}
(i) \quad & N_{\text{GU}_{2m}(q)}(\langle z \rangle \times \langle z \rangle) = \langle z, \phi \rangle \circ \langle \tau \rangle \cong \Gamma U_1(q^m) \rtimes C_2, \text{ where } \phi : z^i \mapsto z^{iq^2}; \\
(ii) \quad & y \in C_{\text{GU}_{2m}(q)}(\langle y \rangle) \subseteq H, \text{ and is equal to } \langle z \rangle \times \langle z \rangle \cong C_{q^m+1}^2;
\end{align*}
\]
(iii) \( y \) is inverted by precisely \( q^m + 1 \) involutions in \( \text{GU}_2m(q) \).

**Proof.** First note that by Corollary 2.4, up to conjugacy \( y \in \text{GU}_2m(q) \), and then by our discussion before the lemma, we can assume that \( y = (y_1, y_1^{-1}) \in H \). (i) Let \( C := \langle z \rangle \times \langle z \rangle \). Then the only proper non-trivial \( \mathbb{F}_q \)-submodules are \( U \) and \( U^* \), and so \( C \leq H \) and \( N_{\text{GU}_2m(q)}(C) \leq H \). Now the normaliser of \( \langle z \rangle \) in \( \text{GU}_m(q) \) is \( N_1 := \langle z, \phi \rangle \), and so \( N_{\text{GU}_2m(q)}(C) = N_1 \cap C \).

(ii) As observed above, \( U \) and \( U^* \) are non-isomorphic \( \mathbb{F}_q \)-submodules, and we may assume that \( y = (y_1, y_1^{-1}) \). Hence \( C_{\text{GU}_2m(q)}(\langle y \rangle) \leq H \). Moreover, since \( y_1 \) is irreducible on \( U \), its centraliser in \( \text{GU}_m(q) \) is \( \langle z \rangle \), and hence \( C_{\text{GU}_2m(q)}(\langle y \rangle) = C \).

(iii) Since \( y = (y_1, y_1^{-1}) \), the involutory map \( \tau \) conjugates \( y \) to \( y^{-1} \). It follows that the elements which conjugate \( y \) to \( y^{-1} \) are precisely the elements of the coset \( C \tau \). These elements are of the form \( (z_1, z_2) \tau \), for some \( z_1, z_2 \in \langle z \rangle \), and are involutions if and only if \( z_2 = z_1^{-1} \). Thus there are precisely \( |z| = q^m + 1 \) involutions which invert \( y \). \( \square \)

### 5.4. Case D: \( |\{f(X), f^\sigma(X), f^*(X), f^{\tau}(X)\}| = 4 \)

We now consider a regular semisimple element \( y \in \text{GU}_4m(q) \) with \( U^* \)-irreducible characteristic polynomial

\[ c_y(X) = f(X)f^{\tau}(X)f^*(X)f^{\sigma}(X), \]

where \( f(X) \) has degree \( m \), so that \( y \) is in Case D of Proposition 4.3. The primary decomposition of \( V \) as an \( \mathbb{F}_q \)-module is \( V = U \oplus U^{\sim} \oplus U^* \oplus U^\sigma \), where the restrictions \( y|_U, y|_{U^{\sim}}, y|_{U^*}, y|_{U^\sigma} \) have characteristic polynomials \( f(X), f^{\sim}(X), f^*(X), \) and \( f^{\sigma}(X) \), respectively. Hence these four \( m \)-dimensional subspaces are pairwise non-isomorphic \( \mathbb{F}_q \)-submodules, and so the centraliser \( C := C_{\text{GU}_4m(q)}(y) \) lies in the stabiliser \( H = \text{Stab}_{\text{GU}_4m(q)}(U, U^{\sim}, U^*, U^\sigma). \)

Let \( W := U \oplus U^{\sim} \) and \( W^* := U^* \oplus U^\sigma \). Then the characteristic polynomials of \( y|_W \) and \( y|_{W^*} \) are both \( \sim \)-invariant, namely \( g(X) := f(X)f^{\sim}(X) \) and \( g^*(X) := f^*(X)f^{\sigma}(X) \). Thus both \( W \) and \( W^* \) are non-degenerate, and \( V = W \perp W^* \). Moreover on considering \( y|_W, y|_{W^*} \) as in Subsection 5.2, we see by Lemma 5.2 that each of the four subspaces \( U, U^{\sim}, U^*, U^\sigma \) is totally isotropic.

For the analysis in this subsection it is convenient to work with matrices with respect to an ordered basis \( (v_1, \ldots, v_{4m}) \) of \( V \), where \( U = \langle v_1, \ldots, v_m \rangle, U^{\sim} = \langle v_{m+1}, \ldots, v_{2m} \rangle, U^* = \langle v_{3m+1}, \ldots, v_{3m} \rangle, \) and \( U^\sigma = \langle v_{3m+1}, \ldots, v_{4m} \rangle \), and with the Gram matrix

\[ J = \begin{pmatrix} 0 & I_m & 0 & 0 \\ I_m & 0 & 0 & 0 \\ 0 & 0 & I_m & 0 \\ 0 & 0 & I_m & 0 \end{pmatrix}. \]

Then, by Lemma 5.2, the stabiliser \( H \) of the four \( m \)-dimensional subspaces is

\[ H = \left\{ \begin{pmatrix} \alpha(a) & 0 \\ 0 & \alpha(b) \end{pmatrix} \mid a, b \in \text{GL}_m(q^2) \right\} \]
where the matrices $\alpha(a), \alpha(b) \in \text{GU}_{2m}(q)$ are as defined in (6). We note that $\text{GU}_{4m}(q)$ contains the element
\[
\tau := \begin{pmatrix} 0 & I_{2m} \\ I_{2m} & 0 \end{pmatrix} \in \text{GL}_m(q^2)^2,
\]
which interchanges the subspaces $W$ and $W^*$ and normalises $H$. We often write elements of $H$ as pairs $(\alpha(a), \alpha(b))$ with $a, b \in \text{GL}_m(q^2)$. Since $y_1 := y|_V \in \text{GL}_m(q^2)$ is irreducible, it is contained in a Singer subgroup $z \in \text{GL}_m(q^2)$, and it follows from Lemma 5.2 that $y|_W = \alpha(y_1)$ and $C_{\text{GU}(W)}(y|_W) = \langle Z \rangle$, where $Z := \alpha(z)$. Also, since $y|_{W^*}, y|_{W}$ have characteristic polynomials $f^*(X), f^\sigma(X) = (f^\sim(X))^*$, we may replace $y$ by a conjugate in $H$ so that $y|_{W^*} = \alpha(y_1^{-1})$. Thus we may assume that $y = (\alpha(y_1), \alpha(y_1^{-1}))$.

**Lemma 5.5.** Let $y \in \text{GL}_{4m}(q^2)$ be regular semisimple, with $c_y(X)$ a U*-irreducible polynomial in Case D. Then, up to conjugacy, and with the notation from the preceding paragraphs,

(i) $y = (\alpha(y_1), \alpha(y_1^{-1})) \in \text{GU}_{4m}(q)$, where $y_1 \in \text{GL}_m(q^2)$, with characteristic polynomial $f(X)$, $y_1$ is contained in a Singer subgroup $\langle z \rangle$, and $C := C_{\text{GU}_{4m}(q)}(y) = \langle Z \rangle \times \langle Z \rangle \cong C_2^{q^{2m} - 1}$, where $Z = \alpha(z)$;

(ii) $N_{\text{GU}_{4m}(q)}(C) = N \triangleright \langle Z, B \rangle \triangleright \langle \tau \rangle$, with $N, B$, as in Lemma 5.2;

(iii) $y$ is inverted by precisely $q^{2m} - 1$ involutions in $\text{GU}_{4m}(q)$

(iv) The integer $m$ can be even or odd. Let $m = 2^{b-1}r$ with $b \geq 1$ and $r$ odd. Then $|y|_2 \leq 2^{b-1}(q^2 - 2)_2$, and equality can be attained in this bound.

**Proof.** (i) The assertions about $y$ follow from Corollary 2.4, and the discussion above. The structure of $C$ follows from Lemma 5.2 applied to $y|_W = \alpha(y_1)$ and $y|_{W^*} = \alpha(y_1^{-1})$.

(ii) The normaliser $N_{\text{GU}(W)}(\langle y|_W \rangle)) = N \triangleright \langle Z, B \rangle$, as in Lemma 5.2, and $N_{\text{GU}_{4m}(q)}(C)$ is therefore equal to $N \triangleright \langle \tau \rangle$.

(iii) The element $\tau$ is an involution which inverts $y = (y_1, y_1^{-1})$, and hence, if $x \in \text{GU}(V)$ inverts $y$, then $x$ lies in the coset $C\tau$ of the centraliser $C$ of $y$, so $x = (\alpha(z_1), \alpha(z_2))\tau$, for some $z_1, z_2 \in \langle z \rangle$. The condition $x^2 = 1$ is equivalent to $z_2 = z_1^{-1}$. Thus there are precisely $q^{2m} - 1$ involutions inverting $y$.

(iv) The order of $y$ is equal to $|y_1|$, which is a divisor of $q^{2m} - 1$. Now $(q^{2m} - 1)_2 = (q^{2r} - 1)_2 = 2^{b-1}(q - 2)_2$. To see that equality may be attained in the bound, notice that we may set $y_1 = z$, so that $|y| = q^{2m} - 1$: in this case the roots of $f(X) = c_y(X)$ are of the form $\{\zeta, \zeta^q, \ldots, \zeta^{q^{2m-2}}\}$, where $\zeta$ has multiplicative order $q^{2m} - 1$, so $f(X) \notin \{f^*(X), f^\sigma(X), f^\sim(X)\}$, as required. This also shows that $m$ may be even or odd.

6. Involutions inverting regular semisimple elements

Having considered the regular semisimple elements whose characteristic polynomials are U*-irreducible, we now consider the general case.

Let $y$ be a regular semisimple element of $G = \text{GU}_n(q)$ with $q$ odd, and suppose that $y^t = y^{-1}$ for some involution $t \in G$. Let $g(X) := c_y(X)$. Then each of $X - 1$ and $X + 1$ may divide $g(X)$ with multiplicity at most one, so $g(X) = g_0(X)(X - 1)^{\delta_1}(X + 1)^{\delta_2}$ where $\delta_1, \delta_2 \in \{0, 1\}$ and $g_0(X)$ is coprime to $X^2 - 1$ and multiplicity-free.
Definition 6.1. We define \( \mathcal{A} \subset \mathbb{F}_{q^2}[X] \) to contain one irreducible factor of each \( U^* \)-irreducible polynomial \( g(X) \) in Case A. Similarly, we define \( \mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_{q^2}[X] \) to contain one irreducible factor of each \( U^* \)-irreducible polynomial from Cases B, C, and D, respectively. For a \( U^* \)-closed polynomial \( g(X) \), we shall write \( \mathcal{A}_g \) to denote the set of irreducible factors of \( g \) that lie in \( \mathcal{A} \), and similarly for the other classes.

Then \( g_0(X) \) may be written as

\[
(9) \quad \left( \prod_{f \in \mathcal{A}_g} f(X)f^*(X) \right) \left( \prod_{f \in \mathcal{B}_g} f(X)f^*(X) \right) \left( \prod_{f \in \mathcal{C}_g} f(X)f^*(X) \right) \left( \prod_{f \in \mathcal{D}_g} f(X)f^*(X) \right).
\]

We consider the primary decomposition of \( V \) as an \( \mathbb{F}_{q^2}(y) \)-module, equipped with our unitary form, and combine the two summands corresponding to \( \{ f(X), f^*(X) \} \) in Case A, the two summands corresponding to \( \{ f(X), f^*(X) \} \) in Cases B and C, and the four summands corresponding to \( \{ f(X), f^*(X), f^*(X), f^*(X) \} \) in Case D, to obtain the following uniquely determined \( y \)-invariant direct sum decomposition of \( V \):

\[
(10) \quad V = \bigoplus_{f \in \mathcal{A}_g} V_f \oplus \bigoplus_{f \in \mathcal{B}_g} V_f \oplus \bigoplus_{f \in \mathcal{C}_g} V_f \oplus \bigoplus_{f \in \mathcal{D}_g} V_f \oplus V_{\pm}.
\]

such that

(A) for each \( f \in \mathcal{A}_g \), the restriction \( y_f = y|_{V_f} \in \text{GU}(V_f) \) has characteristic polynomial \( f(X)f^*(X) \), with \( f(X) = f^*(X) \neq f^*(X) = f^*(X) \);

(B) for each \( f \in \mathcal{B}_g \), the restriction \( y_f = y|_{V_f} \in \text{GU}(V_f) \) has characteristic polynomial \( f(X)f^*(X) \), with \( f(X) = f^*(X) \neq f^*(X) = f^*(X) \);

(C) for each \( f \in \mathcal{C}_g \), the restriction \( y_f = y|_{V_f} \in \text{GU}(V_f) \) has characteristic polynomial \( f(X)f^*(X) \), with \( f(X) = f^*(X) \neq f^*(X) = f^*(X) \);

(D) for each \( f \in \mathcal{D}_g \), the restriction \( y_f = y|_{V_f} \in \text{GU}(V_f) \) has characteristic polynomial \( f(X)f^*(X)f^*(X)f^*(X) \), with all four polynomials pairwise distinct;

(E) \( \dim V_{\pm} \in \{0, 1, 2\} \); if \( \dim V_{\pm} = 1 \) then \( y|_{V_{\pm}} \) has characteristic polynomial \( X + 1 \) or \( X - 1 \); if \( \dim V_{\pm} = 2 \), then \( V_{\pm} = V_+ \oplus V_- \), and \( y|_{V_+}, y|_{V_-} \) has characteristic polynomial \( X - 1, X + 1 \), respectively.

Lemma 6.2. Let \( y \in \text{GU}(g) = \text{GU}(V) \) (with \( q \) odd), where \( y \) is regular semisimple and conjugate in \( \text{GU}(q) \) to \( y^{-1} \), with characteristic polynomial \( g(X) = c_y(X) = g_0(X)(X - 1)^{\delta_+}(X + 1)^{\delta_-} \) with \( \delta_+, \delta_- \in \{0, 1\} \) and \( g_0(X) \) as in (9). Then

(i) Each non-zero summand in (10) is a non-degenerate unitary space, and distinct summands are orthogonal.

(ii) The centraliser order \( |C_{\text{GU}(V)}(y)| \) is equal to

\[
\left( \prod_{f \in \mathcal{A}_g \cup \mathcal{B}_g} (q^{2\deg f} - 1) \right) \left( \prod_{f \in \mathcal{C}_g} (q^{\deg f} + 1)^2 \right) \left( \prod_{f \in \mathcal{D}_g} (q^{2\deg f} - 1)^2 \right) (q + 1)^{\delta_+ + \delta_-}.
\]
(iii) The number of involutions in $GU(V)$ (see Definition 1.3) that invert $y$ is equal to
\[
\prod_{f \in A_q} (q^{\deg f} - 1) \prod_{f \in B_q} (q^{\deg f} + 1) \prod_{f \in C_q} (q^{\deg f} + 1) \prod_{f \in D_q} (q^{2 \deg f} - 1) \varepsilon(y),
\]
where $\varepsilon(y) = 2$ if $X^2 - 1$ divides $g(X)$, and $\varepsilon(y) = 1$ otherwise.
(iv) If $n = 2m$ is even, and $g(X)$ is coprime to $X^2 - 1$, then the number of pairs $(t, y') \in \Delta U(V)$ (as defined in (4)) such that $y'$ has characteristic polynomial $g(X)$ is
\[
\frac{|GU_{2m}(q)|}{\left(\prod_{f \in A_q} (q^{\deg f} - 1) \prod_{f \in B_q} (q^{\deg f} + 1) \prod_{f \in C_q} (q^{\deg f} + 1) \prod_{f \in D_q} (q^{2 \deg f} - 1)\right)}.
\]

**Proof.** (i) Each space in the primary decomposition of $V$ as an $\mathbb{F}_{q^2}(y)$ module is either non-degenerate or totally singular. It follows from our analysis in Section 5 that the spaces corresponding to a $U^*$-irreducible summand always span a non-degenerate space. Let $U, W$ be distinct such summands, corresponding to $U^*$-irreducible polynomials $h(X), h'(X)$ respectively. Let $h(X) = \sum_{i=0}^r a_i X^i$ where $r = \deg(h)$, each $a_i \in \mathbb{F}_{q^2}$, and $a_r = 1$. Then $h, h'$ are coprime, and so $uh(y) = \sum_{i=0}^r a_i y^i = 0$, for each $u \in U$, while $h(y)|_W$ is a bijection. Then, for all $u \in U, w \in W$, writing $(u, w)$ for the value of the form on these vectors, we have
\[
0 = (uh(y), w) = \sum_{i=0}^r a_i (uy^i, w) = \sum_{i=0}^r a_i (u, wy^{-i}) = (u, \sum_{i=0}^r a_i w y^{-i}) = (u, wh^{\sim}(y)y^{-r})
\]
Since $h$ is $U^*$-irreducible, $h^{\sim}(X) = h(X)$, and hence $wh^{\sim}(y)y^{-r}$ ranges over all of $W$ as $w$ does. It follows that $W \subseteq U^\perp$.

Parts (ii) and (iii) follow from the remarks above on applying Lemmas 5.2, 5.4, 5.5 and Corollary 5.3. For (iv), recall that the number of these pairs is equal to the number $|GU_n(q)|/|C_{GU_n(q)}(y)|$ of conjugates of $y$ times the number of $t \in C_U(V)$ inverting $y$. By Lemma 2.6(i) if $g(X) = g_0(X)$ then all involutions inverting $y$ lie in $C(V)$, since $n$ is even. Thus all involutions in $GU_n(q)$ that invert $y$ lie in $C_U(V)$, and hence Part (iv) follows from Parts (ii) and (iii). \qed

7. Formulae for the number of $U^*$-irreducible polynomials in each Case

Recall the division of $U^*$-irreducible polynomials into Cases A to E from Proposition 4.3. In this section we count the number of polynomials with irreducible factors of degree $r$, in each case.

First we present some standard counts of polynomials. Let $\text{Irr}(r, \mathbb{F}_q)$ denote the set of monic irreducible polynomials over $\mathbb{F}_q$ of degree $r$. Recall definition 4.7 of $N(q, r)$. We define the following quantities as in [4, pp. 23–26]:
\[
N^\sim(q, r) = \text{number of } f \in \text{Irr}(r, \mathbb{F}_q) \text{ with } f^\sim = f \text{ (over } \mathbb{F}_{q^2} \text{ not } \mathbb{F}_q).
\]
\[
N^*(q, r) = \text{number of } f \in \text{Irr}(r, \mathbb{F}_q) \text{ with } f^* = f.
\]
\[
M^*(q, r) = \text{number of subsets } \{f, f^*\} \text{ with } f \in \text{Irr}(r, \mathbb{F}_q) \text{ and } f^* \neq f.
\]
Observe that \( N(q, r) = |\text{Irr}(r, \mathbb{F}_q)| \) if \( r > 1 \) and \( N(q, 1) = q - 1 \): we do not count the polynomial \( f(X) = X \) as the matrices we consider are invertible.

The Möbius \( \mu \) function is defined on \( \mathbb{Z}_{>0} \), and takes values as follows:

\[
\mu(n) = \begin{cases} 
(-1)^k & \text{if } n \text{ is a product of } k \text{ distinct primes} \\
0 & \text{if } n \text{ is not square-free.}
\end{cases}
\]

Proofs of the following formulae can be found in Lemmas 1.3.10(a), 1.3.12(a), 1.3.16(a), and 1.3.16(b) of [4].

**Theorem 7.1.** Let \( r \geq 1 \) and let \( q \) be an odd prime power. Then

\[
N(q, r) = \begin{cases} 
\frac{1}{r} \sum_{d|r} \mu(d)(q^{r/d} - 1) & \text{if } r = 1, \\
q - 1 & \text{if } r > 1;
\end{cases}
\]

\[
N^\sim(q, r) = \begin{cases} 
q + 1 & \text{if } r = 1, \\
0 & \text{if } r \text{ is even}, \\
N(q, r) & \text{if } r > 1 \text{ is odd}.
\end{cases}
\]

\[
N^*(q, r) = \begin{cases} 
2 & \text{if } r = 1, \\
\frac{1}{r} \sum_{d|r, d \text{ odd}} \mu(d)(q^{r/(2d)} - 1) & \text{if } r \text{ is even}, \\
0 & \text{if } r > 1 \text{ is odd};
\end{cases}
\]

\[
M^*(q, r) = \begin{cases} 
\frac{1}{2}(q - 3) & \text{if } r = 1, \\
\frac{1}{2}(N(q, r) - N^*(q, r)) & \text{if } r \text{ is even}, \\
\frac{1}{2}N(q, r) & \text{if } r > 1 \text{ is odd}.
\end{cases}
\]

We now prove some bounds on these quantities.

**Lemma 7.2.** Let \( q \) be an odd prime power, set \( \xi = q/(q - 1) \), and let \( r \geq 1 \). If \( r \geq 2 \) then let \( p_1 < p_2 < \cdots < p_t \) be the prime divisors of \( r \) listed in increasing order.

(i) \( q^r - 2q^{r/2} < q^r - \xi q^{r/p_1} < rN(q, r) \leq q^r - 1 \), and \( N(q, r) > 0.956(q^r - 1)/r \) for \( r \geq 5 \).

(ii) \( N(q, r + 1) \geq N(q, r) \).

(iii) Let \( r \) be even. If \( t = 2 \) then \( rN^*(q, r) = q^{r/2} - q^{r/(2p_2)} \), whilst if \( t > 2 \) then

\[
q^{r/2} - q^{r/(2p_2)} - \xi q^{r/(2p_3)} < rN^*(q, r) < q^{r/2} - q^{r/(2p_2)} - \frac{q - 2}{q - 1}q^{r/(2p_3)}.
\]

**Proof.** (i) The upper bound, and the claim for \( r \geq 5 \), are [3, Lemma 2.9(ii)]. If \( r = 1 \) then the result is trivial. If \( r = p_1^t \) is a prime power then \( rN(q, r) = q^r - q^{r/p_1} \), and the result follows since \( \xi > 1 \). Hence assume that \( t \geq 2 \). Then

\[
rN(q, r) = q^r - q^{r/p_1} + \delta
\]
where \( \delta = \sum_{d|r, d > p_1} \mu(d)q^{r/d} \), so that
\[
|\delta| < \sum_{d|r, d > p_1} q^{r/d} < q^{r/p_1} \sum_{i=1}^{\infty} q^{-i} = q^{r/p_1} \left( \frac{1}{1 - \frac{1}{q}} - 1 \right) = q^{r/p_1}(\xi - 1).
\]
The result follows.

(ii) This is [3, Lemma 2.9(iii)].

(iii) Let \( r = 2^b k \) where \( b \geq 1 \) and \( k > 1 \) is odd. Then from Theorem 7.1 we get
\[
rN^*(q, r) = \sum_{d|k, d \text{ odd}} \mu(d)q^{r/(2d)} - \sum_{d|k} \mu(d) = \sum_{d|k} \mu(d)q^{r/(2d)},
\]
since \( k > 1 \) implies that \( \sum_{d|k} \mu(d) = 0 \). If \( r = 2 \), then the result now follows, so assume that \( t \geq 3 \). Then similarly to the proof of Part (i)
\[
q^{r/2} - q^{r/(2p_2)} - q^{r/(2p_3)} \left( 1 + \sum_{i=1}^{\infty} q^{-i} \right) < rN^*(q, r) < q^{r/2} - q^{r/(2p_2)} - q^{r/(2p_3)} \left( 1 - \sum_{i=1}^{\infty} q^{-i} \right)
\]
and so
\[
q^{r/2} - q^{r/(2p_2)} - \xi q^{r/(2p_3)} < rN^*(q, r) < q^{r/2} - q^{r/(2p_2)} - (2 - \xi)q^{r/(2p_3)},
\]
as required. \( \square \)

**Lemma 7.3.** Let \( q \) be an odd prime power and \( r \) a positive integer. Then
\[
\frac{1}{2} \left( N^*(q^2, 2r) + M^*(q^2, r) - N^*(q, r) \right) = \begin{cases} N(q, 2r) - \frac{3}{2} & \text{if } r = 1, \\ N(q, 2r) & \text{if } r > 1. \end{cases}
\]

**Proof.** Suppose first that \( r = 1 \). By [4, Corollary 1.3.16], \( N^*(q^2, 2) + M^*(q^2, 1) = \frac{q^2-1}{2} + \frac{q^2-3}{2} = q^2 - 2 \). Since \( N^*(q, 1) = q + 1 \) and \( N(q, 2) = \frac{q^2-q}{2} \), the \( r = 1 \) case follows. Now suppose that \( r > 1 \). Then, by [14, Lemma 5.1], \( N^*(q^2, 2r) + M^*(q^2, r) = N(q^2, r) \), and it follows from [4, Corollary 1.3.13] and its proof that \( \frac{1}{2}(N(q^2, r) - N^*(q, r)) = N(q, 2r) \) (note this also holds for \( r \) even since then \( N^*(q, r) = 0 \)). \( \square \)

**Definition 7.4.** We define \( A(q, r) \) to be the number of \( U^* \)-irreducible polynomials in Case A of degree \( 2r \) over \( \mathbb{F}_{q^2} \) (so that the irreducible factors have degree \( r \)). Similarly, we define \( B(q, r) \) and \( C(q, r) \) to be the number of \( U^* \)-irreducible polynomials in Cases B and C of degree \( 2r \), and \( D(q, r) \) to be the number of \( U^* \)-irreducible polynomials in Case D of degree \( 4r \). Recall Definition 4.9: it is immediate that \( |\mathcal{D}_{4r}| = D(q, r) \).
Lemma 7.5. Let $r \geq 1$ and let $q$ be an odd prime power. Then

\[
A(q, r) = \begin{cases} 
\frac{1}{2}N^*(q^2, 1) - 1 = 0 & \text{if } r = 1, \\
\frac{1}{2}N^*(q^2, r) & \text{if } r > 1;
\end{cases}
\]

\[
B(q, r) = \begin{cases} 
\frac{1}{2}N^\sim(q, 1) - 2 = \frac{1}{2}(q - 3) & \text{if } r = 1, \\
\frac{1}{2}N^\sim(q, r) & \text{if } r > 1;
\end{cases}
\]

\[
C(q, r) = \begin{cases} 
\frac{1}{2}N^\sim(q, 1) - 1 = \frac{1}{2}(q - 1) & \text{if } r = 1, \\
\frac{1}{2}N^\sim(q, r) & \text{if } r > 1;
\end{cases}
\]

\[
D(q, r) = \begin{cases} 
\frac{1}{2}(M^*(q^2, 1) - N^\sim(q, 1)) + \frac{3}{2} = \frac{1}{4}(q - 1)^2 & \text{if } r = 1, \\
\frac{1}{2}(M^*(q^2, r) - N^\sim(q, r)) & \text{if } r > 1.
\end{cases}
\]

Proof. In each case, the equivalence of the two statements for $r = 1$ follows immediately from Theorem 7.1.

In each of the following cases, we first count the number of polynomials $f \in \text{Irr}(r, \mathbb{F}_{q^2})$ satisfying the case conditions, and then deduce the number of $\text{U}_\ast$-irreducible polynomials of the relevant degree.

Case A. By Proposition 4.3, in this case $f = f^* \neq f^\circ$, and if $f$ exists then $r$ is even. Therefore $A(q, 1) = 0$, and if $r > 1$ and $r$ is odd, then $A(q, r) = \frac{1}{2}N^*(q^2, r) = 0$. Suppose that $r$ is even. By Lemma 4.1, $r$ even implies that $f \neq f^\circ$, and hence in this case $A(q, r)$ is the number of pairs $\{f, f^\circ\} \subset \text{Irr}(r, \mathbb{F}_{q^2})$ satisfying $f = f^*$, namely $A(q, r) = \frac{1}{2}N^*(q^2, r)$.

Case B. By Proposition 4.3, in this case $f = f^\circ \neq f^*$, and if $f$ exists then $r$ is odd. Thus if $r$ is even then $B(q, r) = 0 = \frac{1}{2}N^\sim(q, r)$. Suppose that $r = 1$ so $f(X) = X - \zeta$, for some $\zeta \in \mathbb{F}_{q^2}$. Since $f \neq f^*$, the polynomial $f$ is not $X \pm 1$ or $X$, and so the root $\zeta \not\in \{0, \pm 1\}$. Moreover, since $f = f^\circ$, we have $\zeta = \zeta^\circ$ so $\zeta \in \mathbb{F}_q \setminus \{0, \pm 1\}$. Note that, for each such $\zeta$, the polynomial $f \neq f^*$ since $\zeta \neq \zeta^{-1}$. Thus there are $q - 3$ possibilities for $\zeta$, so the number of pairs $\{f, f^\circ\}$ is $B(q, 1) = \frac{1}{2}(q - 3)$. Suppose now that $r > 1$ and $r$ is odd. Then $f \neq f^\circ$ by Lemma 4.1, and hence in this case $B(q, r)$ is the number of pairs $\{f, f^*\} \subset \text{Irr}(r, \mathbb{F}_{q^2})$ satisfying $f = f^\circ$, namely $B(q, r) = \frac{1}{2}N(q, r)$.

Case C. By Proposition 4.3, in this case $f \neq f^* = f^\circ$ (so $f = f^\sim$), and if $f$ exists then $r$ is odd. Thus if $r$ is even then $C(q, r) = 0 = \frac{1}{2}N^\sim(q, r)$. Suppose that $r = 1$ so $f(X) = X - \zeta$, for some $\zeta \in \mathbb{F}_{q^2}$. Since $f^* = f^\circ \neq f$, the root satisfies $\zeta^{-1} = \zeta^\circ \neq \zeta$, so $\zeta^{q+1} = 1$ and $\zeta^2 \neq 1$, whence $\zeta \neq \pm 1$. Thus there are $q - 1$ possibilities for $\zeta$, and the number of pairs $\{f, f^\circ\}$ is $C(q, r) = \frac{1}{2}(q - 1)$. Suppose now that $r > 1$ and $r$ is odd. Then $f \neq f^\circ$ by Lemma 4.1, and hence $C(q, r)$ is the number of pairs $\{f, f^*\} \subset \text{Irr}(r, \mathbb{F}_{q^2})$ satisfying $f = f^\sim$, namely $C(q, r) = \frac{1}{2}N^\sim(q, r)$.

Case D. In this case the irreducible polynomials $f, f^\circ, f^*, f^\sim$ are pairwise distinct. First suppose that $r = 1$, so $f(X) = X - \zeta$, for some $\zeta \in \mathbb{F}_{q^2}$. The conditions $f \neq f^\sim$ and $f \neq f^*$ are equivalent to $\zeta^{q+1} \neq 1$ and $\zeta^{q-1} \neq 1$, respectively. These two conditions together imply
that \( f, f^\sigma, f^*, f^\sim \) are pairwise distinct, and hence

\[
D(q, 1) = \frac{1}{4}((q^2 - 1) - (q + 1) - (q - 1) + 2) = \frac{1}{4}(q - 1)^2.
\]

Suppose now that \( r > 1 \). We will prove that \( B(q, r) + C(q, r) + 2D(q, r) = M^*(q^2, r) \). Solving for \( D(q, r) \) then gives the desired result. The number of pairs \( \{f, f^*\} \subseteq \operatorname{Irr}(r, \mathbb{F}_{q^2}) \) satisfying \( f \neq f^* \) is, by definition, \( M^*(q^2, r) \). We enumerate these pairs by a different argument. We showed under ‘Case B’ and ‘Case C’ above that the numbers of such pairs for which \( f^\sigma = f \), or \( f^\sigma = f^* \), is \( B(q, r) \) or \( C(q, r) \), respectively. For the remaining pairs the polynomials \( f, f^*, f^\sigma \) are pairwise distinct, giving a set \( \{f, f^*, f^\sigma, f^\sim\} \) of size four: there are \( D(q, r) \) such subsets and each corresponds to two pairs, namely \( \{f, f^*\} \) and \( \{f^\sigma, f^\sim\} \).

The following is an immediate corollary of Theorem 7.1 and Lemma 7.5.

**Corollary 7.6.** Let \( q \) be an odd prime power. Then

\[
D(q, r) = \begin{cases} 
\frac{1}{4}(N(q^2, r) - N^*(q^2, r)) & \text{if } r \text{ is even}, \\
\frac{1}{4}N(q^2, r) - \frac{1}{2}N(q, r) & \text{if } r > 1 \text{ is odd}.
\end{cases}
\]

We now prove bounds on these polynomial counts that will be useful later.

**Lemma 7.7.** Let \( q \) be an odd prime power, and let \( r \geq 1 \). If \( r > 1 \), then let the distinct prime divisors of \( r \) be \( p_1 < p_2 < \ldots < p_k \).

1. If \( r = 2^b \) for \( b \geq 0 \) then \( D(q, r) = \frac{1}{4r}(q^r - 1)^2 \).
2. If \( r = 3 \), then \( 4rD(q, r) = q^6 - 2q^5 - q^2 + 2q < q^{2r} - q^r + \frac{q+1}{q}q^{r/3} \). For all other \( r \), we can bound

\[
q^{2r} - 2q^r - \frac{1}{q^2 - 1}q^r \leq 4rD(q, r) \leq q^{2r} - q^r + \frac{q+1}{q}q^{r/3} < q^{2r} - 1.
\]

3. For all \( r \geq 1 \), we have \( 4rD(q, r) = (q^{2r} - 1) - \eta(q, r)(q^r - 1) \), where \( 0 < 1 - 2q^{-2r/3} < \eta(q, r) < 2.2 \).

**Proof.** (1) The result for \( r = 1 \) is immediate from Lemma 7.5. Otherwise, by Corollary 7.6, we have \( D(q, r) = \frac{1}{4}N(q^2, r) - \frac{1}{4}N^*(q^2, r) \). Then using Theorem 7.1 and the fact that \( r = 2^b > 1 \), we deduce that \( D(q, r) = \frac{1}{4r}(q^{2r} - q^r) - \frac{1}{4r}(q^r - 1) = \frac{1}{4r}(q^r - 1)^2 \), as required.

(ii) By Part (i) we may assume that \( r \) is not a 2-power, and in particular that \( r \geq 3 \). Before commencing the main part of the proof, notice first that if \( q^{2r} - q^r + \frac{q+1}{q}q^{r/3} \geq q^{2r} - 1 \) then \( q^r - 1 \leq \frac{q+1}{q}q^{r/3} < 2q^{r/3} \), so \( (q^r - 1)^3 < 8q^r \), which is impossible, since \( q \geq 3 \) and \( r \geq 3 \). Thus the last inequality holds.

Suppose first that \( r \) is even, and hence is divisible by at least two primes. Then by Corollary 7.6, \( D(q, r) = \frac{1}{4}(N(q^2, r) - N^*(q^2, r)) \). Using the bounds from Lemma 7.2(i)(iii), we deduce that

\[
4rD(q, r) > (q^{2r} - \frac{q^2}{q^2 - 1}q^r) - (q^r - q^{r/p_2}) > q^{2r} - \frac{2q^2 - 1}{q^2 - 1}q^r = q^{2r} - 2q^r - \frac{1}{q^2 - 1}q^r,
\]
and (using the fact that \( r/p_3 \leq r/p_2 - 2 \) if \( p_3 \) exists)

\[
4rD(q, r) < (q^{2r} - 1) - (q^r - (1 + \frac{1}{q})q^{r/p_2}) < q^{2r} - q^r + \frac{q + 1}{q}q^{r/3}.
\]

Suppose now that \( r > 1 \) is odd, so that \( D(q, r) = \frac{1}{2}N(q^2, r) - \frac{1}{2}N(q, r) \), by Corollary 7.6. If \( r \) is an odd prime then \( rN(q^r, r) = q^{fr} - q^r \) and so \( 4rD(q, r) = (q^{2r} - q^r) - 2(q^r - q) = q^{2r} - 2q^r - q^2 + 2q \). This is less than the required upper bound for all odd primes, is greater than \( q^{2r} - 2q^r - q^r/(q^2 - 1) \) for \( r > 3 \), and is precisely the stated value when \( r = 3 \).

If \( r \) is composite (so \( r \geq 9 \)), then Lemma 7.2(i) gives

\[
4rD(q, r) > (q^{2r} - \frac{q^2}{q^2 - 1}q^{2r/p_1}) - 2(q^r - 1) > q^{2r} - 2q^r - \frac{q^2}{q^2 - 1}q^{2r/3}
\]

and since \( 2r/3 + 2 < r \) this is greater than \( q^{2r} - 2q^r - \frac{1}{q^2 - 1}q^r \). Also (setting \( \xi = q/(q + 1) \))

\[
4rD(q, r) < (q^{2r} - 1) - 2(q^r - \xi q^{r/p_1}) < q^{2r} - 2q^r + 2\xi q^{r/3} < q^{2r} - q^r + \frac{q + 1}{q}q^{r/3}.
\]

(iii) Set \( 4rD(q, r) = (q^{2r} - 1) - \eta(q, r)(q^r - 1) \), and let \( \eta = \eta(q, r) \). When \( r \) is a power of 2, the result follows easily from Part (i) (in fact here \( \eta = 2 \)), so assume that \( r \) is not a power of 2. The upper bound in Part (ii) yields that for all such \( r \),

\[
-1 - \eta(q^r - 1) \leq q^r + \frac{q + 1}{q}q^{r/3}.
\]

Rearranging this gives

\[
\eta \geq 1 - \frac{q + 1}{q} \cdot \frac{q^{r/3}}{q^r - 1},
\]

and we must show that

\[
\frac{q + 1}{q} \cdot \frac{q^{r/3}}{q^r - 1} < \frac{2}{q^{2r/3}}.
\]

For all \( r \geq 3 \) and \( q \geq 3 \), it is clear that \( q^{r-1} < q^r - 2 \), and so \( q^r + q^{r-1} < 2q^r - 2 \). Hence \( (q + 1)q^r = q^{r+1} + q^r = q(q^r + q^{r-1}) < q(2q^r - 2) = 2q(q^r - 1) \). Thus

\[
\frac{q + 1}{q} \cdot \frac{q^r}{q^r - 1} < 2,
\]

from which the claimed lower bound on \( \eta \) follows.

For \( r \) an odd prime we have \( 4rD(q, r) = q^{2r} - 2q^r - q^2 + 2q = q^{2r} - 1 - (2q^r + q^2 - 2q - 1) \) which gives \( \eta(q, r) = 2 + \frac{(q-1)^2}{q^r - 1} \) so \( 2 < \eta(q, r) \leq 2 \frac{2}{13} < 2.2 \). In all other cases the lower bound in Part (ii) yields

\[
\eta(q^r - 1) = q^{2r} - 1 - 4rD(q, r) \leq -1 + 2q^r + \frac{1}{q^2 - 1}q^r = 2(q^r - 1) + \frac{q^r - 1 + q^2}{q^2 - 1}
\]
so (since \( r > 2 \) and \( q \geq 3 \))
\[
\eta \leq 2 + \frac{1}{q^2 - 1} + \frac{q^2}{(q^r - 1)(q^2 - 1)} = 2 + \frac{1}{q^2 - 1} + \frac{1}{q^r - 1} + \frac{1}{(q^r - 1)(q^2 - 1)}
\]
\[
\leq 2 + 1/8 + 1/26 + 1/(8 \times 26) < 2.1683.
\]

\[\square\]

**Lemma 7.8.** Let \( q \geq 5 \) be odd, and \( r \geq 1 \). Then
\[
(i) \frac{D(q, r)}{q^{2r} - 1} \geq \frac{D(3, r)}{3^{2r} - 1}; \quad (ii) \frac{N^*(q^r, r)}{q^r - 1} \geq \frac{N^*(3^r, r)}{3^r - 1} \text{ for } r > 1; \quad (iii) \frac{N^-(q, r)}{q^r - 1} \geq \frac{N^-(3, r)}{3^r - 1}.
\]

**Proof.** (i) For \( r \) a power of 2, we have \( D(q, r) = \frac{1}{4r} (q^r - 1)^2 \) by Lemma 7.7(i). Hence
\[
\frac{D(q, r)}{q^{2r} - 1} = \frac{q^r - 1}{4r(q^r + 1)}
\]
is increasing with \( q \), so Part (i) holds for such \( r \). When \( r = 3 \),
\[
\frac{D(q, 3)}{q^6 - 1} = \frac{q^6 - 2q^3 - q^2 + 2q}{12(q^6 - 1)}
\]
which is increasing with \( q \), so Part (i) holds here too. Now suppose that \( r \geq 5 \). Using Lemma 7.7(ii),
\[
4r \frac{D(q, r)}{q^{2r} - 1} \geq \frac{q^{2r} - 2q^r - \frac{1}{q^2 - 1}q^r}{q^{2r} - 1} = 1 - \frac{2q^r + \frac{1}{q^2 - 1}q^r - 1}{q^{2r} - 1} \geq 1 - \frac{49q^r}{4(q^{2r} - 1)};
\]
Using Lemma 7.7(ii) again we get
\[
4r \frac{D(3, r)}{3^{2r} - 1} \leq \frac{3^{2r} - 3^r + \frac{4}{3}3^{r/3}}{3^{2r} - 1} = 1 - \frac{3^r - \frac{4}{3}3^{r/3} - 1}{3^{2r} - 1} \leq 1 - \frac{1}{2 \cdot 3^r}.
\]

Since \( q \geq 5 \) and \( r \geq 5 \), one may verify that \( 2q^r \geq 9 \cdot 3^r + 2 \). Hence \( 2q^{2r} \geq 9 \cdot 3^r q^r + 2 \), and so \( 2(q^{2r} - 1) \geq 9 \cdot 3^r q^r \). Hence \( \frac{1}{2 \cdot 3^r} \geq \frac{9q^r}{4(q^{2r} - 1)} \), and so the result follows.

(ii) Recall the formulae for \( N^*(q, r) \) from Theorem 7.1. The result is immediate if \( r \) is odd, or if \( r \) is a power of 2, so let \( r = 2^b \cdot k \), where \( k \) is odd. If \( k = p^a \) is a prime power, then
\[
rN^*(q^2, r) = q^r - q^{r/p} \text{ and the result can be verified by direct calculation.}
\]
Let \( p_2 \) and \( p_3 \) be the two smallest odd primes dividing \( r \), then from Lemma 7.2(ii) we see that
\[
rN^*(q^2, r) \geq q^r - q^{r/p_2} - \frac{5}{4}q^{r/p_3}
\]
and
\[
rN^*(3^2, r) \leq 3^r - 3^{r/p_2} - \frac{1}{2}3^{r/p_3}.
\]
Assume, by way of contradiction, that
\[
(3^r - 1)(q^r - q^{r/p_2} - \frac{5}{4}q^{r/p_3}) < (q^r - 1)(3^r - 3^{r/p_2} - \frac{1}{2}3^{r/p_3})
\]
then
\[ q^r (3^{r/p_2} + \frac{1}{2} 3^{r/p_3} - 1) - 3^r (q^{r/p_2} + \frac{5}{4} q^{r/p_3} - 1) + (q^{r/p_2} - 3^{r/p_2}) + (\frac{5}{4} q^{r/p_3} - \frac{1}{2} 3^{r/p_3}) < 0 \]
and so in particular
\[ q^r (3^{r/p_2} + \frac{1}{2} 3^{r/p_3} - 1) - 3^r (q^{r/p_2} + \frac{5}{4} q^{r/p_3} - 1) < 0. \]
Dividing by \((3q)^{r/p_2}\), this implies that
\[ q^{r-r/p_2} - 2 \cdot 3^{r-r/p_2} < 0, \]
a contradiction. Hence the result holds for all \(r\) and \(q\).

(iii) The arguments here are similar to the previous two parts. Recall the formulae for \(N^\sim(q, r)\) from Theorem 7.1. In particular, the result is immediate if \(r\) is even or \(r = 1\), so assume that \(r > 1\) is odd, so that \(N^\sim(q, r) = N(q, r)\).

If \(r = p_1^a\) for some odd prime \(p_1\), then \(rN(q, r) = q^r - q^{r/p_1}\), and a straightforward calculation shows that
\[ \frac{q^r - q^{r/p_1}}{q^r + 1} \geq \frac{3^r - 3^{r/p_1}}{3^r + 1}. \]
Let \(r\) be divisible by at least two distinct primes, \(p_1 < p_2\). Then just as in (11) we can deduce that \(rN(q, r) = q^r - q^{r/p_1} - \delta q^{r/p_2}\), where \(2 - \frac{q}{q-1} < \delta < \frac{q}{q-1}\). Hence
\[ \frac{rN(q, r)}{q^r + 1} > \frac{q^r - q^{r/p_1}}{q^r + 1} - \frac{\delta q^{r/p_2}}{q^r + 1} \]
whilst
\[ \frac{rN(q, 3)}{3^r + 1} < \frac{3^r - 3^{r/p_1}}{3^r + 1} - \frac{\frac{1}{3} 3^{r/p_2}}{3^r + 1} \]
Since we already know that the bound holds when \(r\) is a prime power, it suffices to show that
\[ \frac{3^{r/p_2}}{3^r + 1} > \frac{q^{r/p_2}}{q^r + 1}, \]
and in turn to show this it suffices to show that \(3^{r/p_2}q^r > 6q^{r/p_2}3^r\). Dividing by \((3q)^{r/p_2}\), and noting that \(r \geq 15\) and \(p_2 \geq 5\), gives the result. \(\square\)

8. The generating function \(R_u(q, u)\)

In this section, we define a key generating function, analyse its convergence and bound its coefficients.
8.1. Introducing $R_{U}(q, u)$. Recall the definition of $\Delta_{U}(2n, q)$ from (4).

**Definition 8.1.** We shall consider the ‘weighted proportions’

$$r_{U}(2n, q) := \frac{|\Delta_{U}(2n, q)|}{|GU_{2n}(q)|}$$

for $n \geq 1$, letting $r_{U}(0, q) = 1$,

and define the generating function

$$R_{U}(q, u) = \sum_{n=0}^{\infty} r_{U}(2n, q)u^{n}.$$

Recall Cases A to D from Proposition 4.3, and that we use these cases to describe $U^{*}$-irreducible polynomials. Recall also Definition 6.1.

Let $U_{n}$ denote the set of all monic $U^{*}$-closed polynomials $g(X)$ of degree $2n$ such that $\gcd(g, X^{2} - 1) = 1$. It follows from Lemma 6.2(iv) that, for $n \geq 1$, $r_{U}(2n, q)$ is the sum over all $g(X) = c_{y}(X) \in U_{n}$ of the expression

$$1 \left( \prod_{f \in A_{y}} (q^{\deg f} - 1) \right) \left( \prod_{f \in B_{y} \cup C_{y}} (q^{\deg f} + 1) \right) \left( \prod_{f \in D_{y}} (q^{2\deg f} - 1) \right).$$

Thus the generating function $R_{U}(q, u)$ can be expressed as

$$\sum_{n=0}^{\infty} \left( \sum_{g \in U_{n}} \frac{u^{m}}{\left( \prod_{f \in A_{y}} (q^{\deg f} - 1) \right) \left( \prod_{f \in B_{y} \cup C_{y}} (q^{\deg f} + 1) \right) \left( \prod_{f \in D_{y}} (q^{2\deg f} - 1) \right)} \right).$$

**Theorem 8.2.** $R_{U}(q, u)$ is equal as a complex function to $S_{0}(q, u)S(q, u)$, where

$$S_{0}(q, u) = (1 + \frac{u}{q - 1})^{-1}(1 + \frac{u}{q + 1})^{-3}$$

and $S(q, u)$ is the infinite product

$$(1 + \frac{u^{2}}{q^{2} - 1})^{3/2} \prod_{r \geq 1} \left( 1 + \frac{u^{r}}{q^{r} - 1} \right)^{1/2} N^{*}(q^{2}, r) \prod_{r \geq 1} \left( 1 + \frac{u^{r}}{q^{r} + 1} \right)^{N^{*}(q, r)} \prod_{r \geq 1} \left( 1 + \frac{u^{2r}}{q^{2r} - 1} \right)^{N^{*}(q, r)}.\,$$

Furthermore, the function $R_{U}(q, u) = S_{0}(q, u)S(q, u)$ is absolutely and uniformly convergent on the open disc $|u| < 1$.

**Proof.** Let

$$R'(q, u) = \prod_{f \in A} \left( 1 + \frac{u^{\deg f}}{q^{\deg f} - 1} \right) \prod_{f \in B \cup C} \left( 1 + \frac{u^{\deg f}}{q^{\deg f} + 1} \right) \prod_{f \in D} \left( 1 + \frac{u^{2\deg f}}{q^{2\deg f} - 1} \right).$$

Then computing the coefficient of $u^{n}$ for each $n$ shows that $R'(q, u)$ is equal to $R_{U}(q, u)$.

The contribution of each term of this infinite product depends only on the degree of the corresponding irreducible polynomial $f$, and so $R'(q, u)$ is equal, as a complex function,
to

\begin{equation}
R''_U(q, u) = \prod_{r \text{ even}} \left(1 + \frac{u^r}{q^r - 1}\right)^{A(q,r)} \prod_{r \text{ odd}} \left(1 + \frac{u^r}{q^r + 1}\right)^{B(q,r)+C(q,r)} \prod_{r \text{ all}} \left(1 + \frac{u^{2r}}{q^{2r} - 1}\right)^{D(q,r)}.
\end{equation}

Substituting the values from Lemma 7.5 into the above expression for \(R''_U(q, u)\), and noting from Theorem 7.1 that \(N^*(q, r) = 0\) for \(r > 1\) odd, whilst \(N^-(q, r) = 0\) for \(r\) even, shows that \(R''(q, u) = S_0(q, u)S(q, u)\).

We now consider convergence of \(S(q, u)\). By \([4, \text{Corollary 1.3.2}]\), \(\prod_{r \geq 1} (1 + \frac{u^r}{q^r - 1})^{\frac{1}{2}N^*(q^2, r)}\) is absolutely and uniformly convergent if and only if \(\sum_{r \geq 1} \frac{1}{2}N^*(q^2, r)\frac{|u^r|}{q^r - 1}\) is absolutely and uniformly convergent. Now, by \([4, \text{Lemma 1.3.16(a)}]\), \(N^*(q^2, r) = r^{-1}q^r + O(q^{r/3})\) when \(r\) is even, and is equal to 0 when \(r \geq 3\) is odd, so \(\sum_{r \geq 1} N^*(q^2, r)\frac{|u^r|}{q^r - 1}\) is absolutely and uniformly convergent for \(|u| < 1\).

Similarly, for \(\prod_{r \geq 1} (1 + \frac{u^{2r}}{q^{2r} - 1})^{\frac{1}{2}N^-(q^2, r)}\) we consider the sum \(\sum_{r \geq 1} N^-(q, r)\frac{|u|^r}{q^r + 1}\). By \([4, \text{Lemma 1.3.12(a)}]\), \(N^-(q, r) = r^{-1}q^r - O(q^{r/3})\) when \(r\) is odd, and is equal to 0 when \(r\) is even, so as before this term is absolutely and uniformly convergent for \(|u| < 1\).

For \(\prod_{r \geq 1} (1 + \frac{u^{2r}}{q^{2r} - 1})^{\frac{1}{2}M^*(q^2, r) - \frac{1}{2}N^-(q, r)}\), we use the same arguments: by Lemma 7.5 this exponent is equal to \(D(q, r)\) for \(r > 1\), and then Lemma 7.7(iii) gives bounds on \(D(q, r)\) that guarantee absolute and uniform convergence for \(|u| < 1\). \(\square\)

Next we prove that \(\lim_{n \to \infty} r_U(2n, q)\) exists.

**Theorem 8.3.** The limit \(\lim_{n \to \infty} r_U(2n, q)\) exists and is equal to

\(\frac{1 - \frac{1}{q}}{(1 + \frac{1}{q})} \prod_{r \text{ odd}} \left(1 - \frac{2}{q^r(q^r + 1)}\right)^{N(q, r)}\).

**Proof.** Consider the expression \(R(q, u) = S_0(q, u)S(q, u)\) from Theorem 8.2. We use the fact that \(N^*(q^2, r) = 0\) for \(r > 1\) odd, by Theorem 7.1, to see that

\(\prod_{r \geq 1} \left(1 + \frac{u^r}{q^r - 1}\right)^{\frac{1}{2}N^*(q, r)} = \left(1 + \frac{u}{q - 1}\right) \prod_{s \geq 1} \left(1 + \frac{u^{2s}}{q^{2s} - 1}\right)^{\frac{1}{2}N^*(q^2, 2s)}\).

Similarly, since \(N^-(q, 1) = N(q, 1) + 2\) and \(N^-(q, r) = 0\) for \(r\) even, by Theorem 7.1,

\(\prod_{r \geq 1} \left(1 + \frac{u^r}{q^r + 1}\right)^{N^-(q, r)} = \left(1 + \frac{u}{q + 1}\right)^2 \prod_{r \geq 1 \text{ odd}} \left(1 + \frac{u^r}{q^r + 1}\right)^{N(q, r)}\).

Substituting these into our expression for \(R_U(q, u)\) (and noting that since \(R_U(q, u)\) is uniformly convergent, we can rearrange infinite products, gives

\(R_U(q, u) = \frac{(1 + \frac{u^2}{q-1})^{3/2}}{1 + \frac{u}{q+1}} \prod_{r \geq 1} \left(1 + \frac{u^{2r}}{q^{2r} - 1}\right)^{\frac{1}{2}(N^*(q^2, 2r) + M^*(q^2, r) - N^-(q, r))} \prod_{r \geq 1 \text{ odd}} \left(1 + \frac{u^r}{q^r + 1}\right)^{N(q, r)}\).
Rewriting the exponents in the first infinite product in \( R_\U(q, u) \) using Lemma 7.3 gives
\[
R_\U(q, u) = \left(1 + \frac{u}{q+1}\right)^{-1} \prod_{r \geq 1} \left(1 + \frac{u^{2r}}{q^{2r} - 1}\right)^{N(q, 2r)} \prod_{r \geq 1 \text{ odd}} \left(1 + \frac{u^r}{q^r + 1}\right)^{N(q, r)}
\]
\[
= \left(1 + \frac{u}{q+1}\right)^{-1} \prod_{r \geq 2 \text{ even}} \left(1 + \frac{u^r}{q^r - 1}\right)^{N(q, r)} \prod_{r \geq 1 \text{ odd}} \left(1 + \frac{u^r}{q^r + 1}\right)^{N(q, r)}
\]
\begin{equation}
(14) \quad R_\U(q, u) = \left(1 + \frac{u}{q+1}\right)^{-1} \prod_{r \geq 1} \left(1 + \frac{u^r}{q^r - (-1)^r}\right)^{N(q, r)}.
\end{equation}

We have shown in Theorem 8.2 that this expression converges for \(|u| < 1\). By [4, Lemma 1.3.10(b)] with \( u \) replaced with \( u/q \), the following equality holds for \(|u| < 1\),
\[
\frac{1-u/q}{1-u} \prod_{r \geq 1} \left(1 - \frac{u^r}{q^r}\right)^{N(q, r)} = 1.
\]

Multiplying our expression for \( R_\U(q, u) \) by this gives that for \(|u| < 1\)
\begin{equation}
(15) \quad R_\U(q, u) = \left(1 - \frac{u}{q+1}\right) \prod_{r \geq 1} \left(1 + \frac{u^r}{q^r - (-1)^r}\right)^{N(q, r)}.
\end{equation}

Now consider the final expression above for \( R_\U(q, u) \). By [4, Corollary 1.3.2, and Lemma 1.3.10(a)], the function \( R_\U(q, u) \) has a simple pole at \( u = 1 \) and is of the form \((1-u)^{-1} H(u)\) where

\[
H(u) = \frac{1-u}{(1-u)(1+\frac{u}{q+1})} \prod_{r \geq 1} \left(1 - \frac{u^r}{q^r - (-1)^r}\right)^{N(q, r)}.
\]

Using the bound \( N(q, r) < \frac{1}{r} q^r \) from Lemma 7.2(i), and [4, Corollary 1.3.2], we see that \( H(u) \) is analytic in the disc \(|u| < \sqrt{q}\). Thus by [4, Lemma 1.3.3], the coefficients \( \lim_{m \to \infty} r_\U(2m, q) = H(1) \), and the result follows.

### 8.2. Bounds on \( r_\U(2n, q) \)

In this subsection, we shall prove various upper and lower bounds on the values of \( r_\U(2n, q) \).

**Notation 8.4.** If \( f(z) := \sum_{n \geq 0} f_n z^n \) is a power series, we write \([z^n] f(z)\) to denote the coefficient \( f_n \) of \( z^n \). Moreover, if \( g(z) := \sum_{n \geq 0} g_n z^n \), then we write
\[
f(z) \ll g(z) \quad \text{if} \quad f_n \leq g_n \text{ for all } n.
\]

**Definition 8.5.** Recalling the final expression for \( R_\U(q, u) \) from (15), we let \( R_\U(q, u) = A_\U(q, u) B_\U(q, u) \), where
\[
A_\U(q, u) := \frac{1-u}{(1-u)(1+\frac{u}{q+1})}, \quad B_\U(q, u) := \prod_{r \geq 1} \left(1 - \frac{u^r (u^r - (-1)^r)}{q^r (q^r - (-1)^r)}\right)^{N(q, r)}.
\]
Let $A_u(q, u) = \sum_{n \geq 0} a_n u^n$ and $B_u(q, u) = \sum_{n \geq 0} b_n u^n$.

We shall bound $r_u(2n, q)$ by bounding first $a_n$ and then $b_n$.

**Lemma 8.6.** Let $q$ be odd, and let $A_u(q, u)$ be as in Definition 8.5. Then for all $n \geq 1$,

$$a_n = \frac{q^2 - 1}{q^2 + 2q} + c_n, \text{ where } c_n := (-1)^n \frac{2q + 1}{q(q + 2)(q + 1)^n}.$$  

**Proof.** It is straightforward to check that

$$A_u(q, u) = \frac{1 - 1/q^2}{1 + 2/q} \cdot \frac{1}{1 - u} + \frac{2q + 1}{q(q + 2)} \cdot \frac{1}{1 + u/(q + 1)}.$$  

The result follows. \hfill \Box

We now bound the coefficients $b_n$, which will take a little more work.

**Lemma 8.7.** Let $q$ be odd, and let $B_u(q, u)$ be as in Definition 8.5. For all $n$, we can bound

$$|b_n| \leq \beta q^{-n/2} \text{ where } \beta := q/(q - 1).$$

In particular, $B_u(q, u)$ is absolutely convergent for all $|u| < q^{1/2}$.

**Proof.** First we claim that for $r \geq 1$ and $n \geq 0$,

$$|u^n| \left| 1 - \frac{u^r(u^r - (-1)^r)}{q^r(q^r - (-1)^r)} \right|^{N(q, r)} \leq [u^r N] \left( 1 + \frac{u^r(u^r + 1)}{q^r(q^r - 1)} \right)^{N(q, r)}.$$

To see this, let $N := N(q, r)$. Then we calculate that

$$\left( 1 - \frac{u^r(u^r + 1)}{q^r(q^r + 1)} \right)^N = \sum_{j=0}^{N} (-1)^j \binom{N}{j} \left( \frac{u^r}{q^r(q^r + 1)} \right)^j = \sum_{j=0}^{N} \sum_{k=0}^{j} (-1)^j \binom{N}{j} \binom{j}{k} \frac{u^{r(j+k)}}{(q^r(q^r + 1))^j}.$$  

Hence

$$\left| 1 - \frac{u^r(u^r + 1)}{q^r(q^r + 1)} \right|^N \leq \sum_{n=0}^{2N} \left( \sum_{n/2 \leq j \leq n} \left( \binom{N}{j} \binom{j}{n-j} \frac{1}{(q^r(q^r + 1))^j} \right) u^n \right.$$

$$= \left( 1 + \frac{u^r(u^r + 1)}{q^r(q^r - 1)} \right)^N \ll \left( 1 + \frac{u^r(u^r + 1)}{q^r(q^r - 1)} \right)^N.$$

Similarly, one may show that (see also [3, p433])

$$\left| 1 - \frac{u^r(u^r - 1)}{q^r(q^r - 1)} \right|^N \ll \left( 1 + \frac{u^r(u^r + 1)}{q^r(q^r - 1)} \right)^N.$$  

Substituting these bounds for the terms with $r$ odd and $r$ even on the left hand side of (16) yields the right hand side.
Now, from Definition 8.5, we deduce from (16) that
\[
|B_U|(q, u) \ll \prod_{r \geq 1} \left| \left( 1 - \frac{u^r(u^r - (-1)^r)}{q^r(q^r - (-1)^r)} \right)^{N(q,r)} \right| \ll \prod_{r \geq 1} \left( 1 + \frac{u^r(u^r + 1)}{q^r(q^r - 1)} \right)^{N(q,r)}.
\]

Comparing the expression for $B_U(q, u)$ with that for $B(q, u)$ in [3, Equation (8)], we can reason just as in the proof of Lemma 4.1 in [3, top of p434] that the bound in Equation (10) from [3] is valid for $|B_U(q, u)|$. This is precisely the bound in the current lemma.

The convergence claims are clear. □

**Theorem 8.8.** Let $q$ be an odd prime power, let $B_U(q, u)$ be as in Definition 8.5, and let $\alpha = \frac{q^2-1}{q^2+2q}$. Then $B_U(q, 1) = \sum_{n \geq 0} b_n$ converges and $\lim_{n \to \infty} r_U(2n, q) = \alpha B_U(q, 1)$. Furthermore

\[
\epsilon_n := |r_U(2n, q) - \alpha B_U(q, 1)| < \frac{\alpha q^{1/2} + 2}{q^{(n-1)/2}(q-1)(q^{1/2} - 1)} = O(q^{-(n-1)/2}).
\]

**Proof.** By Definition 8.5, the coefficient $r_U(2n, q) = \sum_{k=0}^{n} a_{n-k}b_k$. By Lemma 8.7, the series $B_U(q, u)$ converges for $|u| < q^{1/2}$, so $B_U(q, 1) = \sum_{n \geq 0} b_n$ converges. As in Lemma 8.6, we can write $a_n = \alpha + c_n$. Hence

\[
(17) \quad r_U(2n, q) - \alpha B_U(q, 1) = \sum_{k=0}^{n} (\alpha + c_{n-k})b_k - \alpha \sum_{k=0}^{n} b_k = \sum_{k=0}^{n} c_{n-k}b_k - \alpha \sum_{k>n} b_k.
\]

We bound the terms on the right side of (17) as follows. Since $\frac{2q+1}{q(q+2)} < \frac{2}{q+1}$, we have

\[
|c_n| = \frac{2q+1}{q(q+2)(q+1)^n} < \frac{2}{(q+1)^{n+1}} < \frac{2}{q^{n+1}}.
\]

Hence by Lemma 8.7,

\[
\left| \sum_{k=0}^{n} c_k b_{n-k} \right| < \left| \sum_{k=0}^{n} \frac{2\beta}{q^{k+1}q^{(n-k)/2}} \right| = \frac{2\beta}{q^{n+1}(q^{n/2} + 1)} < \frac{2\beta}{q^{n/2}(1 - q^{-1/2})} = \frac{2\beta}{q^{(n+1)/2}(q^{1/2} - 1)}.
\]

Similarly, from Lemma 8.7, we deduce that

\[
\left| \alpha \sum_{k>n} b_k \right| < \alpha \sum_{k>n} \beta q^{-k/2} = \frac{\alpha \beta}{q^{n/2}(1 - q^{-1/2})} = \frac{\alpha \beta q^{1/2}}{q^{(n+1)/2}(q^{1/2} + 1)}.
\]

Substituting the previous two displayed equations into (17), and then substituting $\beta = \frac{q}{q+1}$, gives

\[
|r_U(2n, q) - \alpha B_U(q, 1)| < \frac{(\alpha q^{1/2} + 2)\beta}{q^{n+1/2}(q^{1/2} - 1)} = \frac{\alpha q^{1/2} + 2}{q^{(n-1)/2}(q - 1)(q^{1/2} - 1)}.
\]

Therefore $r_U(2n, q) \to \alpha B_U(q, 1)$ as $n \to \infty$ as claimed. □

Before proving explicit bounds on the limit of $r_U(2n, q)$, and bound its convergence, we record a technical lemma.
Lemma 8.9. Let \( a, b \in \mathbb{R}_{>0} \) such that \( b > 1 \) and \( ab < 1 \). Then \( (1 - a)^b \geq 1 - ab \).

Proof. Taking logs, it suffices to show that \( b \log(1 - a) \geq \log(1 - ab) \). We use the infinite series expansion \( \log(1 - x) = - \sum_{n=1}^{\infty} x^n / n \), valid for \( 0 < x < 1 \). Notice that

\[
b \log(1 - a) = -b \sum_{i \geq 1} \frac{a^i}{i} = -ab - a^2b \left( \frac{1}{2} + \frac{a}{3} + \cdots \right)
\]

whilst

\[
\log(1 - ab) = - \sum_{i \geq 1} \frac{a^ib^i}{i} = -ab - a^2b \left( \frac{b}{2} + \frac{ab^2}{3} + \cdots \right)
\]

Since \( b > 1 \), it follows that \( \frac{a^{i+2}}{i+2} > \frac{a^i}{i+2} \) for all \( i \), from which the result follows. \( \square \)

Theorem 8.10. Let \( q \) be an odd prime power, let \( \mu = \frac{q^2-1}{q^2+2q} \left( 1 - \frac{2}{q(q+1)} \right)^{q-1} \), let \( \delta = 1 - \frac{3}{4q^4} \), and let \( \varepsilon_n \) be as in Theorem 8.8. Then

\[
\mu \delta - \varepsilon_n < r_{U}(2n, q) < \mu + \varepsilon_n
\]

In particular, \( r_{U}(2, 3) = 0.25 \), and \( 0.3433 < r_{U}(2n, 3) < 0.3795 \) for \( n \geq 2 \).

Proof. We showed in Theorem 8.8 that \( \lim_{n \to \infty} r_{U}(2n, q) = \alpha B_{U}(q, 1) \), so we first prove bounds on \( B_{U}(q, 1) \). It follows from Definition 8.5 that

\[
B_{U}(q, 1) = \prod_{r \geq 1 \text{ odd}} \left( 1 - \frac{2}{q^r(q^r+1)} \right)^{N(q,r)}.
\]

By Theorem 7.1, the \( r = 1 \) term in this product is \( \gamma := (1 - \frac{2}{q(q+1)})^{q-1} \) and this provides an upper bound for \( B_{U}(q, 1) \), since all terms are less than 1. For a lower bound note that

\[
1 - \frac{2}{q^r(q^r+1)} > 1 - \frac{2}{q^2}, \quad \text{and} \quad N(q, r) \leq q^r/r \text{ by Lemma 7.2(i)}. \]

Hence

\[
B_{U}(q, 1) = \prod_{r \text{ odd}} \left( 1 - \frac{2}{q^r(q^r+1)} \right)^{N(q,r)} = \gamma \prod_{r \geq 3 \text{ odd}} \left( 1 - \frac{2}{q^r(q^r+1)} \right)^{N(q,r)}
\]

\[
\geq \gamma \prod_{r \geq 3 \text{ odd}} \left( 1 - \frac{2}{q^{2r}} \right)^{q^r/r}
\]

Now, we apply Lemma 8.9 with \( a = 2q^{-2r} \) and \( b = q^r/r \) to see that \( (1 - \frac{2}{q^{2r}})^{q^r/r} \geq 1 - \frac{2q^r}{rq^{2r}} = 1 - \frac{2}{rq^{r}} \) and hence

\[
B_{U}(q, 1) \geq \gamma \prod_{r \geq 3 \text{ odd}} \left( 1 - \frac{2}{rq^{r}} \right).
\]

An easy induction on \( r \) then shows that

\[
B_{U}(q, 1) \geq \gamma \left( 1 - \sum_{r \geq 3 \text{ odd}} \frac{2}{rq^{r}} \right).
\]
However,

$$\sum_{r \geq 3 \text{ odd}} \frac{2}{rq^r} < \sum_{r \geq 3 \text{ odd}} \frac{2}{3q^r} \sum_{r \geq 0 \text{ even}} \frac{1}{q^r} = \frac{2}{3q^3} \sum_{s \geq 0} \frac{1}{q^{2s}} = \frac{2}{3q^3} \frac{1}{1-q^{-2}} \leq \frac{3}{4q^3}$$

and so $\gamma > B_U(q,1) > \gamma \left(1 - \frac{3}{4q^2}\right)$. Setting $\delta = 1 - \frac{3}{4q^2}$ and $\mu = \alpha \gamma = \frac{q^2-1}{q(q+1)} \left(1 - \frac{2}{q(q+1)}\right)^{q-1}$ gives

$$\mu \delta < \alpha B_U(q,1) < \mu$$

and the main claim follows immediately from Theorem 8.8. When $q = 3$, we have $\alpha = \frac{8}{15}$ and $\gamma = \frac{25}{36}$, so that $\mu = \alpha \gamma = 10/27$. We also find that $\delta = \frac{35}{36}$. Putting these bounds together yields

(18) \hspace{1cm} 0.3601 < \alpha B_U(3,1) < 0.3704.

Finally, we estimate $r_U(2n,3)$ for $n \geq 3$. We compute the values of $r_U(2n,q)$ directly for $n \leq 20$, using the expression for $R_U(q,u)$ given in (14), and we find that $r_U(0,q)$ and $r_U(2,q)$ are as given, and that for $n \geq 2$ we can bound $0.3433 < r_U(2n,q) < 0.3795$. Assume therefore that $n \geq 21$. Theorem 8.8 gives

$$|r_U(2n,q) - \alpha B_U(3,1)| \leq \varepsilon_n = \frac{\alpha q^{1/2} + 2}{q^{(n-1)/2}(q-1)(q^{1/2} - 1)}.$$ 

Substituting $q = 3$ and simplifying we get

$$|r_U(2n,3) - \alpha B_U(3,1)| \leq \frac{27 + 19\sqrt{3}}{30} 3^{-(n-1)/2}.$$ 

However, $\frac{27+19\sqrt{3}}{30} < 2$ and $3^{-(n-1)/2} \leq \frac{1}{3^{1/2}}$, and so we get

$$\alpha B_U(3,1) - \frac{2}{3^{1/2}} \leq r_U(2n,3) < \alpha B_U(3,1) + \frac{2}{3^{1/2}}.$$ 

The bounds for $n \geq 3$ now follow from (18). \hfill \Box

9. Controlling the eigenspaces of $\text{inv}(y)$

We wish to estimate the proportion of pairs $(t,y) \in \Delta_U(2n,q)$ for which $\text{inv}(y)$ induces a strong involution on one of the eigenspaces of $t$. A fundamental issue underpinning this is to understand the link between the eigenspaces of $\text{inv}(y)$ and the characteristic polynomial of $y$ (acting on some subspace $U$ of $V$). Suppose that there is a $y$-invariant decomposition $U = U^+ \oplus U^-$ such that

(a) the restriction $y^- := y|_{U^-}$ has a certain 2-part order, say $2^B$, while

(b) the restriction $y^+ := y|_{U^+}$ is guaranteed to have 2-part order strictly less than $2^B$.

If these conditions hold then $U^\pm$ will be the $\pm 1$-eigenspace of $\text{inv}(y)|_U$. It is often possible to detect, from the characteristic polynomial of $y|_U$, whether these conditions hold. In Subsections 9.1 and 9.2 we introduce functions $G_{U,B}(q,u)$, $R_{U,B}(q,u)$ and $G_{U,B}^-(q,u)$, each related to $R_U(q,u)$, for certain non-negative integers $b$. These three functions will help in detecting these properties. From their definitions, we will see that $G_{U,B}^-(q,u)$ counts pairs
(t^-, y^-) for which the 2-part order of y^- is precisely 2^{b-1}(q^2 - 1)_2, while the pairs (t^+, y^+) counted by R_{U,b}(q, u) are such that the 2-part order of y^+ is strictly less than 2^{b-1}(q^2 - 1)_2. Moreover these properties of y^\pm are determined by their characteristic polynomials.

The functions G_{U,b}(q, u) and R_{U,b}(q, u) are therefore crucial for our investigation. In particular we will need lower bounds on the sizes of the coefficients of their power series, and we find these bounds with the aid of several more functions. In Subsection 9.1 we also define functions T_{U,b}(q, u), for positive integers b, and prove that R_{U,b}(q, u) = R_U(q, u)T_{U,b}(q, u)^{-1} (Lemma 9.3). In Subsection 9.2, we introduce a truncated version F_{U,b}(q, u) of G_{U,b}(q, u) from which it is easier to deduce lower bounds for the coefficients of G_{U,b}(q, u). Also in Subsection 9.2 we prove the fundamental Lemma 9.6 that links the number of pairs (t, y) in \Delta_U(2n, q), where y has a particular type of characteristic polynomial, with products of certain coefficients of R_{U,b}(q, u) and G_{U,b}(q, u). In the remaining three technical subsections we obtain the required lower bounds: first for the coefficients of T_{U,b}(q, u)^{-1} (Subsection 9.3), next we use these bounds together with results from Section 8 about R_U(q, u), to bound the coefficients of R_{U,b}(q, u) (Subsection 9.4); and finally we bound the coefficients of F_{U,b}(q, u) (Subsection 9.5). These bounds are exploited in Section 10 to prove our main result Theorem 1.

9.1. Related functions G_{U,b}(q, u), R_{U,b}(q, u) and T_{U,b}(q, u). Recall the expression for R_U(q, u) given in Theorem 8.2, and the relationships between the various power series given in Lemma 7.5.

For each b \geq 0, we now define an infinite series G_{U,b}(q, u) = \sum_{n \geq 0} g_b(2n, q)u^n as follows. First define the series

\begin{equation}
G_{U,0}(q, u) := \prod_{r \geq 1} \left(1 + \frac{ur}{q^r - 1}\right)^{A(q, r)} \prod_{r \geq 1} \left(1 + \frac{ur}{q^r + 1}\right)^{B(q, r) + C(q, r)} = S_0(q, u) \prod_{r \geq 1} \left(1 + \frac{ur}{q^r - 1}\right)^{\frac{1}{2}N^*(q^2, r)} \prod_{r \geq 1} \left(1 + \frac{ur}{q^r + 1}\right)^{N^-(q, r)}.
\end{equation}

It follows from Section 8 that the quantity g_0(2n, q)|GU_{2n}(q)| equals the number of pairs (t, y) \in \Delta_U(2n, q) for which each factor in the U*-factorisation of the characteristic polynomial c_y(X) is of type A, B or C.

For the remaining infinite product of S(q, u), the terms are labeled by integers r such that r = 2^{b-1}m for some positive integers b, m with m odd. We henceforth abbreviate “all odd integers m \geq 1” simply as “m odd”. For each b \geq 1, define

\begin{equation}
G_{U,b}(q, u) := \prod_{m \text{ odd}} \left(1 + \frac{u^{2^bm}}{q^{2^bm} - 1}\right)^{D(q; 2^{b-1}m)_2}.
\end{equation}
and so by Lemma 7.5

\[
G_{U,b}(q,u) = \begin{cases} 
\prod_{m \text{ odd}} \left( 1 + \frac{u^{2m}}{q^{2m} - 1} \right)^{\frac{1}{2}M^*(q^{2},2^{b-1}m) - \frac{1}{2}N^*(q,2^{b-1}m)} & \text{for } b > 1, \\
\left( 1 + \frac{u^2}{q^2 - 1} \right)^{3/2} \prod_{m \text{ odd}} \left( 1 + \frac{u^{2m}}{q^{2m} - 1} \right)^{\frac{1}{2}M^*(q^{2},m) - \frac{1}{2}N^*(q,m)} & \text{for } b = 1.
\end{cases}
\]

It follows from Section 8 that for \( b \geq 1 \) the quantity \([u^n]G_{U,b}(q,u)\) \(|GU_{2n}(q)|\), that is to say, \( g_b(2n,q)|GU_{2n}(q)| \), is equal to the number of pairs \((t,y) \in \Delta_U(2n,q)\) for which each factor in the \( U_* \)-factorization of the characteristic polynomial \( c_y(X) \) is of type \( D \), and each \( U_* \)-irreducible has four irreducible factors over \( \mathbb{F}_q^2 \) each of degree \( r = 2^{b-1}m \) for some odd \( m \). In particular, the \( U_* \)-irreducible polynomial \( g(X) \) has degree \( 4r = 2^{b+1}m \) with \( m \) odd, and \( \omega_2(g) \leq (q^{2r} - 1)_2 = 2^{b-1}(q^2 - 1)_2 \); moreover a large fraction of these polynomials \( g(X) \) have \( \omega_2(g) = (q^{2r} - 1)_2 = 2^{b-1}(q^2 - 1)_2 \) (see Definition 4.9 and Lemma 4.10).

For \( b \geq 1 \), we now define an ascending chain of subsets \( \Delta_{U,b}(2n,q) \) of \( \Delta_U(2n,q) \). Let \( \Delta_{U,b}(2n,q) \) consist of those \((t,y) \in \Delta_U(2n,q)\) such that each \( U_* \)-irreducible factor \( g(X) \) of \( c_y(X) \) is either of type \( A \), \( B \), or \( C \), or is of type \( D \) and has the 2-part of its degree dividing \( 2b \). Thus in particular \( \Delta_{U,1}(2n,q) \) contains only those \((t,y)\) where each \( U_* \)-irreducible factor of \( c_y(X) \) is of type \( A \), \( B \), or \( C \); whilst \( \Delta_{U,2}(2n,q) \) also allows \( U_* \)-irreducible factors to be in type \( D \), provided that their degree is \( 4m \) for some odd \( m \).

**Definition 9.1.** For \( b \geq 1 \), we define \( r_{U,b}(2n,q) := \frac{[\Delta_{U,b}(2n,q)\]}{|GU_{2n}(q)|} \) for \( n > 0 \), and let \( r_{U,b}(0,q) := 1 \). We define \( R_{U,b}(q,u) := \sum_{n=0}^{\infty} r_{U,b}(2n,q)u^n \).

The functions \( G_{U,b}(q,u) \), \( R_{U,b}(q,u) \), and \( R_U(q,u) \) are related as follows.

**Theorem 9.2.** The power series \( R_U(q,u) \), \( G_{U,b}(q,u) \) (for \( b \geq 0 \)), and \( R_{U,b}(q,u) \) (for \( b \geq 1 \)) all converge absolutely and uniformly in the open disc \(|u| < 1\). Moreover, in this disc,

\[
R_U(q,u) = \prod_{b=0}^{\infty} G_{U,b}(q,u) \quad \text{and} \quad R_{U,b}(q,u) = \prod_{k=0}^{b-1} G_{U,k}(q,u).
\]

**Proof.** By Theorem 8.2, the power series \( R_U(q,u) \) converges absolutely and uniformly in the open disc \(|u| < 1\). An exactly similar argument shows that the \( G_{U,b}(q,u) \) converge absolutely and uniformly for \(|u| < 1\). From (13), we see that \( R_U(q,u) \) is a product of exactly the same terms as \( \prod_{b=0}^{\infty} G_{U,b}(q,u) \), just in a different order. The absolute convergence for \(|u| < 1\) of each infinite expression in the first displayed equality in the statement implies that this equality holds.

Next, let \( b \geq 1 \). Since \( 0 < r_{U,b}(2n,q) < r_U(2n,q) \) for all \( n \), \( R_{U,b}(q,u) \) converges absolutely and uniformly for \(|u| < 1\). Finally, it follows from the discussion following (20), and Definition 9.1, that \( R_{U,b}(q,u) \) is a product of exactly the same terms as \( \prod_{k=0}^{b-1} G_{U,k}(q,u) \), just in a different order. The absolute convergence for \(|u| < 1\) of each infinite expression in the second displayed equality in the statement implies that this equality holds. \( \square \)
For $b \geq 1$, set
\begin{equation}
T_{U,b}(q,u) := \prod_{k \geq b} G_{U,k}(q,u).
\end{equation}

**Lemma 9.3.** Let $b \geq 1$. On the open disc $|u| < 1$, the power series $T_{U,b}(q,u)^{-1}$ is absolutely and uniformly convergent, and
\[ R_{U,b}(q,u) = R_{U}(q,u)T_{U,b}(q,u)^{-1}. \]

**Proof.** From Theorem 9.2, the function $R_{U}(q,u)$ is absolutely and uniformly convergent, and equal to $\prod_{b=0}^{\infty} G_{U,b}(q,u)$. Given an absolutely convergent series, any subseries is also absolutely convergent, so $T_{U,b}(q,u)$ is also absolutely convergent for each $b$. Since convergent products converge to nonzero limits, it follows that $T_{U,b}(q,u)^{-1}$ is also absolutely convergent, and so the given equality of functions holds. \qed

### 9.2. Truncations of the power series $G_{U,b}(q,u)$.

**Definition 9.4.** For $b \geq 1$, we ‘truncate’ the infinite product defined by (20) by reducing the exponent of each term, and hence removing some of the factors. We set
\begin{equation}
G_{U,b}^{-}(q,u) = \sum_{n \geq 0} g_{U,b}(2n,q)u^n := \prod_{m \text{ odd}} \left(1 + \frac{u^{2^m} q^{2^m b^{b+1}_m}}{q^{2^m b^{b+1}_m} - 1}\right)^{N_{U}^{-}(q,2^{b+1}_m)}.
\end{equation}

**Remark 9.5.** For $b > 1$ the product expression for $G_{U,b}^{-}(q,u)$ is a truncation of the one for $G_{U,b}$, because $D_{4r}^{\ast} \subset D_{4r}$. For $b = 1$ notice that this either preserves or decreases exponents even for the term $m = 1$, as the exponent of $(1 + u^2 q)$ in $G_{U,1}(q,u)$ is
\[
\frac{3}{2} + \frac{1}{2} M^{\ast}(q^2, 1) - \frac{1}{2} N^{-}(q,1) = D(q,1) = \frac{1}{4} (q-1)^2 \geq \frac{1}{8} (q^2 - 1)
\]
since $q \geq 3$. Notice that since $G_{U,b}^{-}(q,u)$ is a truncation of $G_{U,b}(q,u)$, Theorem 9.2 shows that each $G_{U,b}^{-}(q,u)$ is absolutely convergent on the open disc $|u| < 1$.

We do not know the precise value of $N_{U}^{-}(q,2^{b+1}_m)$, but we found a lower bound for it in Lemma 4.10(iii). Hence, rather than calculate $G_{U,b}^{-}(q,u)$ it is simpler to compute
\begin{equation}
F_{U,b}(q,u) = \sum_{n=0}^{\infty} f_{U,b}(2n,q)u^n := \prod_{m \text{ odd}} \left(1 + \frac{u^{2^m} q^{2^m b^{b+1}_m}}{q^{2^m b^{b+1}_m} - 1}\right)^{[\frac{1}{2} N(q^2,2^{b+1}_m)]}.
\end{equation}

Our next result shows the important role that the coefficients of $R_{U,b}(q,u)$ and $G_{U,b}^{-}(q,u)$ (and hence also of $F_{U,b}(q,u)$) play in estimating the proportion of pairs $(t,y) \in \Delta_{U}(2k,q)$ with the properties (a) and (b) discussed at the beginning of this section.

**Lemma 9.6.** Fix $b > 1$, let $k \geq \ell \geq 0$ with $k > 0$, and let $a_{k\ell} := r_{U,b}(2k-2\ell,q)g_{U,b}(2\ell,q)$. Then $a_{k\ell}|GU_{2k}(q)|$ is equal to the number of pairs $(t,y) \in \Delta_{U}(2k,q)$ such that the characteristic polynomial $c_{y}(X)$ for $y$ has the form $c_{y}(X) = c_{y}^{-}(X)c_{y}^{+}(X)$, where
(i) $c_g^+(X)$ is the product of the $U^*$-irreducible factors $g(X)$ of $c_Y(X)$ which lie in $\bigcup_{m \text{ odd}} D_{2^{b+1}m}$; so in particular each has degree with 2-part $2^{b+1}$ and satisfies $\omega_2(g) = 2^{b-1}(q^2 - 1)_2$.

Furthermore, $\deg c_g^-(X) = 2\ell$.

(ii) $c_g^-(X)$ is a product of $U^*$-irreducible polynomials $g(X)$ which are either not of type $D$ or have degree with 2-part $2^b$, and satisfy $\omega_2(g) \leq 2^{b-2}(q^2 - 1)_2$.

(iii) If $\ell > 0$ then $\inv(y)$ is of type $(2k - 2\ell, 2\ell)$.

(iv) $0 \ll F_{U,b}(q,u) \ll G_{U,b}(q,u)$, and if $f_{U,b}(2n,q) \neq 0$ then $2^b$ divides $n$.

(v) $[u^n]F_{U,b}(q,u)|\text{GU}_{2n}(q)|$ is at most the number of pairs $(t, y)$ in $\Delta_U(2n, q)$ such that each $U^*$-irreducible factor $g(X)$ of $c_y(X)$ satisfies $\omega_2(g) = 2^{b-1}(q^2 - 1)_2$.

**Proof.** Recall from Definition 9.1 that $r_{U,b}(2k - 2\ell, q)|\text{GU}_{2k-2\ell}(q)|$ counts the number of pairs $(t, y) \in \Delta_U(2k - 2\ell, q)$ such that each $U^*$-irreducible is either of type $A, B$ or $C$, or of type $D$ with the 2-part of its degree dividing $2^b$. By Lemma 4.10(i)(ii), it follows from $b \geq 2$ that $|y|_2 \leq 2^{b-2}(q^2 - 1)_2$.

By construction, $g_{U,b}(2\ell, q)|\text{GU}_{2\ell}(q)|$ is equal to the number of pairs $(t, y) \in \Delta_U(2\ell, q)$ such that each $U^*$-irreducible factor of $c_y(X)$ lies in $\bigcup_{m \text{ odd}} D_{2^{b+1}m}$, and from the definition of $D_{2^{b+1}m}$ it follows that such a $y$ satisfies $|y|_2 = 2^{b-1}(q^2 - 1)_2$, and the 2-part of the degree of each $U^*$-irreducible factor is $2^{b+1}$.

Notice that

$$a_{k\ell}|\text{GU}_{2k}(q)| = r_{U,b}(2k - 2\ell, q)|\text{GU}_{2k-2\ell}(q)||\text{GU}_{2\ell}(q)| \cdot \frac{|\text{GU}_{2k}(q)|}{|\text{GU}_{2k-2\ell}(q) \times \text{GU}_{2\ell}(q)|}.$$ 

By Lemma 6.2, to count the number of pairs $(t, y) \in \Delta_U(2k, q)$ with decomposition $c_y(X) = c_y^-(X)c_y^+(X)$ satisfying (i) and (ii), we can first count the number of decompositions of $V$ as $U \perp W$ with $U$ and $W$ non-degenerate, dim$(U) = 2k - 2\ell$, and dim$(W) = 2\ell$: this is precisely $\frac{|\text{GU}_{2k}(q)|}{|\text{GU}_{2k-2\ell}(q) \times \text{GU}_{2\ell}(q)|}$. We then multiply by the number of possible actions of $t|_U$ and $y|_U$ such that all $U^*$-irreducible factors of $y$ are of type $A$, $B$ or $C$, or of type $D$ but of 2-part of the degree at most $2^b$: this is exactly $r_{U,b}(2k - 2\ell)|\text{GU}_{2k-2\ell}(q)|$. Finally we multiply by $g_{U,b}(2\ell, q)|\text{GU}_{2\ell}(q)|$ for the choices of $t|_W$ and $y|_W$ that ensure that each irreducible factor $g(X)$ of $c_y|_W(X)$ lies in $D_{2^{b+1}m}$ for some odd $m$. Parts (i) and (ii) now follow immediately.

For Part (iii), notice that by Part (i), $\omega_2(c_y^-(X)) = 2^{b-1}(q^2 - 1)_2$, whilst by Part (ii), $\omega_2(c_y^+(X)) = 2^{b-2}(q^2 - 1)_2$. Hence if $\ell > 0$ then $\inv(y)$ has $-1$-eigenspace of dimension $\deg(c_y^-) = 2\ell$, and $\inv(y)$ has type $(2k - 2\ell, 2\ell)$.

For Part (iv) it is immediate from (23) that each coefficient $f_{U,b}(2n,q)$ of $F_{U,b}(q,u)$ is non-negative, and from Lemma 4.10(iii) that $g_{U,b}(2n,q) \geq f_{U,b}(2n,q)$ for all $n$. For the final claim, notice that if $f_{U,b}(2n,q) > 0$ then $g_{U,b}(2n,q) > 0$, and so, as argued for Part (i) above, there exists $(t, y) \in \Delta_U(2n, q)$ such that each $U^*$-irreducible factor of $c_y(X)$ has degree divisible by $2^{b+1}$. Hence in particular $2^{b+1}$ divides $2n$, and the result follows.

Part (v) now follows from Part (iv) and the proof of Part (i).
we shall derive in this subsection for the coefficients of $T_{U,b}(q, u)^{-1}$, to obtain bounds for the coefficients of $R_{U,b}(q, u)$. It will suffice to consider only $b \geq 3$. Now

$$T_{U,b}(q, u)^{-1} = \prod_{k=b}^{\infty} G_{U,k}(q, u)^{-1} = \prod_{k=b, m \text{ odd}} \left( 1 + \frac{u^{2k_m}}{q^{2^k m} - 1} \right)^{-D(q, 2^k - 1, m)},$$

(24)

where the final rearrangement giving (24) is permissible in the disc $|u| < 1$ due to Lemma 9.3.

Fix a value of $b \geq 3$ and define $d := 2^b$, $U := u^2$ and $Q := q^b$. We are going to bound the coefficients $t_n := [U^n] T(U)$ of the power series $T(U)$, where

$$1 - T(U) := \prod_{m=1}^{\infty} \left( 1 + \frac{U^m}{Q^m - 1} \right)^{-D(q, dm/2)}.$$  

(25)

However, we will need to take a somewhat indirect route to do so.

**Lemma 9.7.** Assume that $b \geq 3$, that is, $d \geq 8$, and define

$$W(U) = \sum_{n \geq 0} w_n U^n := -\log (1 - T(U)) + \frac{1}{2d} \log(1 - U).$$

(i) The functions $T(U)$ and $W(U)$ are absolutely and uniformly convergent on the open disc $|U| < 1$ (that is, $|u| < 1$).

(ii) In this disc, $1 - T(U) = T_{U,b}(q, u)^{-1}$.

(iii) $w_0 = 0$, and $|w_n| < 2d^{-1}n^{-1}(Q - 1)^{-n/2}$ for all $n \geq 1$.

**Proof.** For Part (i), notice that the product in (25) converges absolutely and uniformly if and only if the product $\prod_{m=1}^{\infty} \left( 1 + \frac{U^m}{Q^m - 1} \right)^{D(q, dm/2)}$ does so too. By [4, Lemma 1.3.1], this happens if and only if

$$\sum_{m=1}^{\infty} D(q, dm/2)|U^m|/(Q^m - 1)$$

also converges absolutely and uniformly. By Lemma 7.7(ii), $D(q, dm/2) < (q^{dm} - 1)/2dm < Q^m/2dm$, so the convergence of $1 - T(U)$ in the disc $|U| < 1$ follows. Thus $W(U)$ also converges absolutely and uniformly for $|U| < 1$.

Part (ii) is now immediate from (24) and (25).

For Part (iii), first observe that since $\log(1 - z) = -\sum_{k=1}^{\infty} z^k/k$ for $|z| < 1$

$$W(U) = \sum_{m=1}^{\infty} \left\{ D(q, dm/2) \log \left( 1 + \frac{U^m}{Q^m - 1} - \frac{U^m}{2dm} \right) \right\}$$

$$= W_1(U) + W_2(U)$$
where
\[ W_1(U) := \sum_{m=1}^{\infty} \left\{ D(q, dm/2) \frac{U^m}{Q^m - 1} - \frac{U^m}{2dm} \right\} = \sum_{n=1}^{\infty} w_{1,n} U^n, \text{ say} \]
and
\[ W_2(U) := \sum_{m=1}^{\infty} \sum_{k=2}^{\infty} (-1)^{k+1} D(q, dm/2) \frac{U^{mk}}{k(Q^m - 1)^k} = \sum_{n=2}^{\infty} w_{2,n} U^n, \text{ say.} \]
Notice that \( w_0 = 0 \).

In order to treat the \( w_{1,n} \), we use Lemma 7.7(iii) to get
\[ D(q, dm/2) \frac{U^m}{Q^m - 1} = \frac{U^m}{2dn} \left( 1 - \frac{\eta(q, dm/2)}{Q^{m/2} + 1} \right) \]
where \( 1 - 2Q^{-m/3} \leq \eta(q, \frac{md}{2}) < 2.2 \). Thus for all \( n \geq 1 \),
\[ w_{1,n} = \frac{D(q, dn/2)}{Q^n - 1} - \frac{1}{2dn} = \frac{-\eta(q, dn/2)}{2nd(Q^{n/2} + 1)} \]
and so
\[ |w_{1,n}| = \frac{1}{2dn} \left| \frac{\eta(q, dn/2)}{Q^{n/2} + 1} \right| \leq \frac{1}{2dn} \cdot \frac{2.2}{Q^{n/2} + 1} \leq \frac{1.1(Q - 1)^{-n/2}}{dn}. \]

From \( D(q, dm/2) \leq (Q^m - 1)/2dm \), we mimic the proof of [3, Lemma 4.2] to deduce that
\[ |w_{2,n}| \leq \sum_{1 \leq m \leq n/2} \frac{1}{2dn(Q^m - 1)^{n/m - 1}} \]
and hence to see that
\[ |w_{2,n}| < \frac{1}{2dn} (Q - 1)^{-n/2} (1 - (Q - 1)^{-1})^{-1} \leq \frac{1.0002(Q - 1)^{-n/2}}{2dn}. \]
Hence
\[ |w_n| \leq |w_{1n}| + |w_{2n}| < \frac{2(Q - 1)^{-n/2}}{dn} \]
for all \( n \geq 1 \) as required. \( \square \)

**Corollary 9.8.** Let \( W(U) \) be as in Lemma 9.7, let \( d = 2^h \geq 8 \), and let \( q \geq 3 \) be odd. Then the coefficients of \( E(U) := \exp(-W(U)) - 1 = \sum_{n=1}^{\infty} e_n U^n \)
satisfy \( |e_n| \leq \frac{2^{h-1} \gamma^n}{1 + d^{-1}} \) for all \( n \geq 1 \), where \( \gamma = (1 + d^{-1})(Q - 1)^{-1/2} \). In particular, \( \gamma \leq 0.014 \) and \( d |e_1| < 0.025 \).
theorem. Lemma 9.7 shows that $|w_n| \leq 2d^{-1}(Q - 1)^{-n/2}$ for all $n \geq 1$. Let $\beta = (Q - 1)^{-1/2}$ and $\alpha = 2d^{-1}\beta$, so that $|w_n| \leq \alpha \beta^{n-1}$ for all $n \geq 1$, and $\gamma := \frac{\alpha}{2} + \beta = (1 + d^{-1})(Q - 1)^{-1/2} \leq 1$. Thus [3, Lemma 3.4] applies to $-W(U)$ with this $\alpha$ and $\beta$, and yields $|e_n| \leq \alpha \gamma^{n-1} = \frac{2}{1+d} \gamma^n$ for all $n \geq 1$. From $q^d \geq 3^8$ we see that $\gamma \leq 0.014$, and that $d|e_1| \leq \frac{2d}{1+d} \gamma = 2(Q - 1)^{-1/2} < 0.025$. \hfill $\Box$

Let $h(U) = \sum_{k=1}^{\infty} h_k U^k$, say, be the series for $1 - (1 - U)^{1/2d}$. It follows from the definition of $W(U)$ in Lemma 9.7, and of $E(U)$ in Corollary 9.8, that
\begin{equation}
1 - T(U) = (1 - U)^{1/2d}(1 + E(U)) = (1 - h(U))(1 + E(U)).
\end{equation}
Comparing (26) with [3, Equation (13)], we see that replacing $d$ by $2d$ in the discussion in [3], we may deduce from [3, Equation (14)] that for $k \geq 2$
\begin{equation}
1 > 2dkh_k > \exp\left(-\frac{(1 + \log k)}{2d - 1}\right).
\end{equation}
We use this to estimate the values of the coefficients $t_k$.

**Lemma 9.9.** Suppose that $d = 2^b \geq 8$. Then $dkt_k < 0.5065$ for $k \geq 1$, whenever $dk \leq e^{d^2}/2$.

**Proof.** First let $k = 1$. From the product formula for $1 - T(U)$ in (25) we see that $t_1 = \frac{D(q,d/2)}{q^d - 1}$. By Lemma 7.7(i), this is equal to $\frac{1}{2d}(q^{d/2} - 1)/(q^{d/2} + 1)$ since $d$ is a power of 2. Because $q^d \geq 3^8$, this implies that $t_1 \leq 0.5d^{-1}$. Suppose therefore for the rest of the proof that $2 \leq k \leq e^{d^2}/2d$.

Equations (26) and (27) show that $t_k = h_k - e_k + \sum_{i=1}^{k-1} e_{k-i}h_i$ and $0 < h_k < 1$. Thus Corollary 9.8 gives
\begin{equation}
t_k - h_k \leq -e_k + \sum_{i=1}^{k-1} \frac{e_{k-i}}{2di} \leq \frac{2}{1 + d} \left\{ \gamma^k + \frac{1}{2d} \sum_{i=1}^{k-1} i^{-1} \gamma^{k-i} \right\} \quad \text{for } k \geq 2
\end{equation}
where $\gamma = (1 + d^{-1})(q^d - 1)^{-1/2} \leq 1.125(q^d - 1)^{-1/2}$. Hence $dk\gamma \leq e^{d^2}/2 \times 1.125(q^d - 1)^{-1/2} \leq 1.125e^4(3^8 - 1)^{-1/2} < 0.759$.

The remainder of the proof is similar to that of [3, Lemma 4.4], and we only give the necessary details. First, it is shown in [3, Proof of Lemma 4.4] that
\begin{equation}
\sum_{i=1}^{k-1} i^{-1} \gamma^{k-i} \leq \frac{\gamma}{(k-1)(1-\gamma)^2}.
\end{equation}
Also $\gamma \leq 0.0144$ by Corollary 9.8, so $(1 - \gamma)^{-2} < 1.0295$. Hence
\begin{equation}
t_k - h_k \leq \frac{2}{1 + d} \left( \gamma^k + \frac{\gamma}{2d(k-1)(1-\gamma)^2} \right) < 3.577\gamma d^{-2}k^{-1}.
\end{equation}
Since $3.577\gamma d^{-1} \leq 3.577 \times 0.0144 \times 0.125 < 0.0065$ we have $t_k - h_k < 0.0065d^{-1}k^{-1}$ for $2 \leq k \leq e^{d^2}/2d$. It is immediate from (27) that $dh_k < 0.5$, so we conclude that $dk t_k = dk(t_k - h_k) + dkh_k < 0.5065$ for $2 \leq k \leq e^{d^2}/2d$, as required. \hfill $\Box$
9.4. Bounding the coefficients of $R_{U,b}(q,u)$. Recall from Definitions 8.1 and 9.1 that $R_U(q,u) = \sum_{n=0}^{\infty} r_U(2n,q) u^n$ and $R_{U,b}(q,u) = \sum_{n=0}^{\infty} r_{U,b}(2n,q) u^n$. We now prove a lower bound on the coefficients $r_{U,b}(2n,q)$, provided that $n$ is not too large.

First we shall prove that $R_U(3,u) \ll R_U(q,u)$ and $R_{U,b}(3,u) \ll R_{U,b}(q,u)$. Recall the expression for $R_U(q,u)$ in Theorem 9.2. We shall show that $0 \ll G_{U,b}(3,u) \ll G_{U,b}(q,u)$ for all $b$, from which the result will follow.

First we record a useful result from \[3\].

**Lemma 9.10.** \[3, Lemma 3.1\] *Let $M, N \in \mathbb{Z}_{>0}$, and let $a, b \in \mathbb{R}_{>0}$, such that $M \geq N$, $a \leq b$, and $Ma \geq Nb$. Then as a power series in $z$ we have $(1 + bz)^N \ll (1 + az)^M$.***

**Proof.** Recall the expression for $G_{U,0}(q,u)$ in (19). From Theorem 7.1 we find that

$$G_{U,0}(q,u) = \left(1 + \frac{u}{q+1}\right)^{q-2} \prod_{r \geq 2} \left(1 + \frac{u^r}{q^r - 1}\right)^{\frac{1}{2}N^*(q^2,r)} \prod_{r \geq 2} \left(1 + \frac{u^r}{q^r + 1}\right)^{-N^*(q,r)}.$$ 

It is clear that $0 \ll (1 + \frac{u}{3r+1})^{N^*(q^2,r)} \ll (1 + \frac{u}{q+1})^{q-2}$, so consider next the general $r$ term of the first infinite product. By Lemma 7.8(ii)

$$\frac{N^*(q^2,r)}{q^r - 1} \geq \frac{N^*(3^2,r)}{3^r - 1}.$$ 

Since $\frac{1}{2} N^*(q^2,r) = A(q,r)$ counts certain polynomials over $\mathbb{F}_q$, it is an integer, and so it follows from Lemma 9.10 (with $N = \frac{1}{2} N^*(3^2,r)$, $M = \frac{1}{2} N^*(q^2,r)$, $a = (q^r + 1)$ and $b = (3^r - 1)$) that

$$0 \ll \left(1 + \frac{u^r}{3^r + 1}\right)^{\frac{1}{2}N^*(3^2,r)} \ll \left(1 + \frac{u^r}{q^r - 1}\right)^{\frac{1}{2}N^*(q^2,r)}$$

for all $q \geq 3$ and $r > 1$.

Next consider the general $r$ term of the second infinite product. By Lemma 7.8(iii),

$$\frac{N^-(q,r)}{q^r + 1} \geq \frac{N^-(3,r)}{q^r + 1}$$

for all $r \geq 1$, so as in the previous paragraph, from Lemma 9.10 we deduce that

$$0 \ll \left(1 + \frac{u^r}{3^r + 1}\right)^{N^-(3,r)} \ll \left(1 + \frac{u^r}{q^r + 1}\right)^{N^-(q,r)}.$$ 

The result follows by multiplying all of these terms together. \[\square\]

**Lemma 9.12.** *For all odd $q \geq 3$, and all $b \geq 1$, we can bound $0 \ll G_{U,b}(3,u) \ll G_{U,b}(q,u)$.***
Proof. Recall (20). We showed in Lemma 7.8(i) that for all \( n \geq 1 \)

\[
\frac{D(q, n)}{q^{2n} - 1} \geq \frac{D(3, n)}{3^{2n} - 1}
\]
so it follows from Lemma 9.10 that

\[
\left(1 + \frac{u^{2m}}{3^{2m} - 1}\right)^{D(3, m)} \ll \left(1 + \frac{u^{2m}}{q^{2m} - 1}\right)^{D(q, m)}
\]
for all \( m \geq 1 \) and all odd \( q \geq 3 \), and hence that for all \( b \geq 1 \)

\[
0 \ll G_{U,b}(3, u) \ll G_{U,b}(q, u).
\]

\[\square\]

Corollary 9.13. For all odd \( q \) and for all \( b \geq 1 \),

\[
0 \ll R_{U}(3, u) \ll R_{U}(q, u) \quad \text{and} \quad 0 \ll R_{U,b}(3, u) \ll R_{U,b}(q, u).
\]

Furthermore, for \( b \geq 2 \),

\[
R_{U,b-1}(3, u) \ll R_{U,b}(3, u).
\]

Proof. Here \( R_{U}(q, u) = \prod_{b=0}^{\infty} G_{U,b}(q, u) \), and \( R_{U,b}(q, u) = \prod_{k=0}^{b-1} G_{U,k}(q, u) \), so the first two claims follow immediately from Lemmas 9.11 and 9.12.

The final claim follows from noting that \( R_{U,b}(3, u) = R_{U,b-1}(3, u)G_{U,b-1}(3, u) \), and that \( G_{U,b-1}(3, u) \) is a power series with non-negative coefficients and constant term 1.

\[\square\]

Lemma 9.14. The union of the intervals \([0, 23] \) and \([3 \cdot 2^k, e^{2k-1}] \), for \( k \in \mathbb{Z}_{\geq 3} \) is \( \mathbb{Z}_{\geq 0} \).

Proof. For \( k = 3 \), the value of \( 3 \cdot 2^k \) is 24, so no integers are missing at the bottom of these ranges. It therefore suffices to show that \( 3 \cdot 2^{k+1} \leq e^{2k-1} + 1 \), which is straightforward to verify for all \( k \geq 3 \).

\[\square\]

Lemma 9.15. Let \( b \geq 3 \) and \( d = 2^b \). Then \( r_{U,b}(2n, q) > 0.247 \) for all odd \( q \) and all \( n \leq e^{d/2} \).

Proof. We showed in Corollary 9.13 that \( r_{U,b}(2n, q) \geq r_{U,b}(2n, 3) \), so from now on assume that \( q = 3 \).

From Definition 9.1 we see that \( r_{U,b}(0, 3) = 1 \). The values of \( r_{U,b}(2n, 3) \) for \( 1 \leq n < 24 \) may be computed: they are all at least 0.25. Corollary 9.13 then shows that if \( b \geq 3 \) then \( r_{U,b}(2n, 3) \geq r_{U,b}(2n, 3) \geq 0.25 > 0.247 \) for all \( n < 24 \).

We now claim that to show that \( r_{U,b}(2n, 3) > \alpha \) for all \( n \leq e^{2b-1} \) and for all \( b \geq 3 \), it suffices to show that \( r_{U,b}(2n, 3) > 0.247 \) for each consecutive \( b \), and \( n \) in the range \( 3 \cdot 2^b \leq n \leq e^{2b-1} \). To see this, first notice that by Lemma 9.14, for \( b \geq 3 \) the union of each of these intervals for \( 3 \leq b' \leq b \) is \([0, \ldots, e^{2b-1}] \). Secondly, \( r_{U,b}(2n, 3) \geq r_{U,b}(2n, 3) \) for each \( b' \leq b \) by Corollary 9.13, so the claim follows.
Thus it remains only to prove that $r_{U,b}(2n,3) > 0.247$ for $3d \leq n < e^{d/2}$. Recall from (24) and (25) that

$$ R_{U,b}(q,u) = R_U(q,u)T_{U,b}(q,u)^{-1} = R_U(q,u)(1 - T(u^d)) = \left( \sum_{n=0}^{\infty} r_U(2n,q)u^n \right) \left( 1 - \sum_{k=1}^{\infty} t_k u^{dk} \right). $$

Hence, setting $k = \lfloor n/d \rfloor$, we get

$$ r_{U,b}(2n,3) = r_U(2n,3) - \sum_{1 \leq k \leq k_0} r_U(2(n - kd),3)t_k. $$

Our assumption that $n \geq 3d$ implies that $k_0 \geq 3$. If $k < k_0$ then $n - kd \geq d \geq 8$, and so, by Theorem 8.10, $r_U(2n,3) > 0.3433$ for $n \geq d$; $r_U(2(n - kd),3) \leq 0.3795$ for $1 \leq k \leq k_0 - 1$. Since $kdt_k \leq 0.5065$ for all $k$ such that $dk \leq e^{d/2}$ by Lemma 9.9, and since $3d \leq n \leq e^{d/2}$ by hypothesis,

$$ r_{U,b}(2n,3) \geq 0.3433 - \frac{0.5065}{d} \left\{ \frac{1}{k_0} + 0.3795 \sum_{1 \leq k \leq k_0 - 1} \frac{1}{k} \right\} $$

$$ \geq 0.3433 - \frac{0.5065}{d} \left\{ \frac{1}{k_0} + 0.3795 (\log k_0 + 1) \right\}. $$

However $\log k_0 + 1 \leq \log(n/d) + 1 \leq \log n - \log d + 1 \leq \log n - 1 \leq d/2 - 1$, by the hypothesis on $n$, and $1/k_0 \leq 1/3 < 0.3795$. Therefore

$$ r_{U,b}(2n,3) \geq 0.3433 - 0.5065 \cdot 0.3795/2 > 0.247 $$

as required. \[\square\]

9.5. Bounding the coefficients of $F_{U,b}(q,u)$. We shall continue to assume that $b \geq 3$, $d := 2^b \geq 8$, $U = u^d$ and $Q = q^d$ with $q$ odd. With this notation (23) becomes

$$ F_{U,b}(q,u) = \sum_{n \geq 0} f_{U,b}(2n,q)u^n = \prod_{m \text{ odd}} \left( 1 + \frac{U_m}{Q^m - 1} \right)^{[\frac{1}{2}N(q^2,md/2)]} $$

$$ = F_b(U), \text{ say.} $$

Recall from Lemma 9.6(v) that $[u^n]F_{U,b}(q,u) |GU_{2n}(q)|$ is a lower bound on the number of pairs $(t,y)$ in $\Delta_U(2n,q)$ such that the 2-part of the order of each eigenvalue of $y$ is $2^{b-1}(q^2-1)_2$.

We can now find a lower bound for certain coefficients of $F_b(U)$.

**Lemma 9.16.** Assume $b \geq 3$, so $d = 2^b \geq 8$. Then

$$ f_{U,b}(2dk,q) = [U^k]F_b(U) \geq 0.2117d^{-1}k^{-1} $$

for all $k$ such that $kd \leq e^{d/2}$. 

The proof of this lemma is almost identical to that of [3, Lemma 4.6], and so is omitted. To see why these proofs are equivalent, notice that in [3] the exponent of the $m$th term in the infinite product for $F_b(q, u)$ is $\left\lfloor \frac{1}{4} N(q, md) \right\rfloor$, and the bounds $\frac{1}{4} N(q, md) \geq \frac{1}{4md} (q^{md} - 2q^{md})$ and $\frac{1}{4} N(q, md) \geq \frac{0.5md}{4md} (q^{md} - 1)$ are used. Our exponent is $\frac{1}{8} N(q^2, md/2)$, and Lemma 7.2(i) gives $\frac{1}{8} N(q^2, md/2) \geq \frac{2}{8md} (q^{md} - 2q^{md})$ and $\frac{1}{8} N(q^2, md/2) > \frac{2 \times 0.956}{8md} (q^{md} - 1)$ for $md/2 \geq 5$. It is not hard to find an equivalent bound when $md/2 = 4$. Notice also that the assumption that $k$ is odd in [3, Lemma 4.6] is unnecessary.

10. Proof of Theorem 1

We begin with some preliminary lemmas.

**Definition 10.1.** Suppose that $0 \leq \alpha < \beta \leq 1$, and let $J_U(2m, q; \alpha, \beta)$ be the set of all $(t, y) \in \Delta_U(2m, q)$ for which $\text{inv}(y)$ is $(\alpha, \beta)$-balanced. Set

$$j_U(2m, q; \alpha, \beta) := |J_U(2m, q; \alpha, \beta)| / |GU_{2m}(q)|.$$

**Definition 10.2.** For $0 \leq \alpha < \beta \leq 1$ and $b \geq 1$, let $F_{U,b}(q, u; m(1 - \beta), m(1 - \alpha))$ be the truncated power series obtained from $F_{U,b}(q, u) = \sum_{k=0}^{\infty} f_{U,b}(2^{b+k}k, q)u^{2^{b+k}}$ by keeping only the terms $f_{U,b}(2^{b+k}k, q)u^{2^{b+k}}$ for which $m(1 - \beta) \leq 2^{b+k} \leq m(1 - \alpha)$.

**Lemma 10.3.** Fix $m > 0$, and let $0 \leq \alpha < \beta \leq 1$. Then

$$j_U(2m, q; \alpha, \beta) \geq [u^m] \sum_{b=2}^{\infty} R_{U,b}(q, u)F_{U,b}(q, u; m(1 - \beta), m(1 - \alpha))$$

**Proof.** If $c_y(X) \in \Pi_U(2m, q)$ is the characteristic polynomial for $y$ and $c_y^{-}(X)$ is the polynomial as in Lemma 9.6, then by Lemma 9.6(iii), $\text{inv}(y)$ has $(-1)$-eigenspace of dimension $\deg c_y^{-}(X)$, and so $\text{inv}(y)$ is $(\alpha, \beta)$-balanced if and only if $2m(1 - \beta) \leq \deg c_y^{-}(X) \leq 2m(1 - \alpha)$. It follows from Lemma 9.6 that we may bound $j_U(2m, q; \alpha, \beta)$ by summing the coefficients of $u^{m}\ell'$ in the power series $R_{U,b}(q, u)F_{U,b}(q, uz)$, over $b > 1$, and over $\ell$ in the range $[m(1 - \beta), m(1 - \alpha)]$ (and we recall that non-zero summands in $F_{U,b}(q, uz) = \sum_{\ell \geq 0} f_{U,b}(2\ell, q)(uz)\ell'$ occur only if $2^b$ divides $\ell$).

The proof of the following is very similar to that of [3, Lemma 3.8], so we only sketch the details.

**Lemma 10.4.** Let $a$ and $c$ be real numbers with $0 < a < c$. Then

$$\sum_{\frac{a}{k} \leq c \leq c} \frac{1}{k} \geq \log \left( \frac{c}{a} \right) - \frac{1}{a}.$$

**Proof.** Each non-negative integer $\ell$ satisfies $1/\ell \geq \int_{\ell}^{\ell+1} x^{-1}dx$. Set $\ell_0 := [a]$ and $\ell_1 := [c]$. Then the sum in question is equal to

$$\sum_{\ell = \ell_0}^{\ell_1} \frac{1}{\ell} \geq \int_{\ell_0}^{\ell_1+1} x^{-1}dx \geq \int_{\ell_0}^{\ell_1} x^{-1}dx = \log \left( \frac{c}{a} \right) - \log \left( \frac{\ell_0}{a} \right).$$
From $\ell_\alpha/a < 1 + 1/a$ we deduce that $\log (\ell_\alpha/a) < \frac{1}{a}$, so the required inequality follows. □

**Lemma 10.5.** Let $b \geq 3$ and $d := 2^b$. Then for all $\alpha$ and $\beta$ with $0 \leq \alpha < \beta < 1$ and positive integers $m \leq e^{d/2}$, we have

$$j_U(2m, q; \alpha, \beta) \geq \frac{0.05228}{d} \left( \log \left( \frac{1 - \alpha}{1 - \beta} \right) - \frac{d}{m(1 - \beta)} \right).$$

**Proof.** The coefficient $f_{U,b}(2dk, q)$ of $F_{U,b}(q, u)$ is $[U^k]F_{U,b}(U)$, and by Lemma 9.16 for all $k$ such that $dk \leq e^{d/2}$, we have $f_{U,b}(2dk, q) \geq 0.2117/dk$. Set $a := m(1 - \alpha)$ and $c := m(1 - \beta)$, and consider the sum $s$ of the coefficients of $F_{U,b}(q, u)$ for terms with degrees between $c$ and $a$. By Lemma 9.6(iv), if $f_{U,b}(2n, q) \neq 0$ then $n = dk$ for some $k$. Thus, using Lemma 10.4 we see that

$$s = \sum_{c \leq dk \leq a} f_{U,b}(2dk, q) \geq \sum_{c/dk \leq a/d, k \in \mathbb{Z}} 0.2117/dk$$

$$\geq \frac{0.2117}{d} \left( \log \left( \frac{a}{c} \right) - \frac{d}{c} \right).$$

Since $r_{U,b}(2n, q) = [u^n]R_{U,b}(q, u) > 0.247$ for all $n \leq e^{d/2}$, by Lemma 9.15, it follows from Lemma 10.3 that $j_U(2m, q; \alpha, \beta) \geq 0.247s$, so the result follows. □

**Definition 10.6.** Let

$$\ell_U(n, s, q; \alpha, \beta) := |L_U(n, s, q; \alpha, \beta)| / |K_{U,s}|^2,$$

the proportion of pairs in $K_{U,s} \times K_{U,s}$ which lie in $L_U(n, s, q; \alpha, \beta)$ (as in Definition 3.2).

We define

$$\varphi_U(m, z) = \prod_{i=1}^{m} (1 - (-1)^{i}z^{-i}), \text{ for } z > 1 \text{ and } m \in \mathbb{N}$$

and note that $|\text{GU}_m(q)| = q^{m^2}\varphi_U(m, q)$.

**Lemma 10.7.** Let $2n/3 \geq s \geq n/2 \geq 2$, let $j_U(2n - 2s, q; \alpha, \beta)$ be as in (28), and let $\theta(n, s, q) = \varphi_U(n - s, q)^2\varphi_U(s, q)^2 / \varphi_U(n, q)\varphi_U(2s - n, q)$. Then

$$\ell_U(n, s, q; \alpha, \beta) = \theta(n, s, q) j_U(2n - 2s, q; \alpha, \beta),$$

and $\theta(n, s, q) > \frac{81}{98}$.

**Proof.** Let $h := 2s - n$, so that $n - h = 2(n - s)$, and let $\Omega_U$ be the set of pairs $(V_1, V_2)$ of non-degenerate subspaces of the formed space $V$ for $\text{GU}_n(q)$, of dimensions $h, n - h$ respectively, such that $V_1^\perp = V_2$. Then for each pair $(V_1, V_2) \in \Omega_U$, and each pair $(t_2, y_2) \in \Delta_U(n - h, q)$ acting on $V_2$ such that $\text{inv}(y_2)$ is $(\alpha, \beta)$-balanced, there is (see Lemma 2.7) a unique pair $(t, t')$ of involutions in $\text{GU}_n(q)$ such that $t|_{V_2} = t_2$, $t'|_{V_2} = t_2y_2$, and $t|_{V_1} = t_1$. Then $\ell_U(n, s, q; \alpha, \beta) = \theta(n, s, q) j_U(2n - 2s, q; \alpha, \beta)$, and $\theta(n, s, q) > \frac{81}{98}$. □
and $t_{|V_1} = t'_{|V_1} = I$. Moreover, since each of $t_2$ and $t_2y_2$ conjugates $y_2$ to its inverse, each is of type $(\frac{1}{2}(n-h), \frac{1}{2}(n-h))$ by [3, Lemma 2.2]. It follows from Definition 3.2 that $(t, t') \in L_U(n, s, q; \alpha, \beta)$.

Conversely, for each $(t, t') \in L_U(n, s, q; \alpha, \beta)$, relative to $V_1, V_2$ as in Definition 3.2, the pair $(t_{|V_2}, tt'_{|V_2}) \in \Delta_U(n-h, q)$. Hence $|L_U(n, s, q; \alpha, \beta)| = |\Omega_U| \times |J_U(n-h, q; \alpha, \beta)|$. Thus by (28) and Definition 10.6, we conclude that

$$
\ell_U(n, s, q; \alpha, \beta) = \frac{|\Omega_U| |GU_{n-h}(q)| j_\theta(n-h, q; \alpha, \beta)}{|K_{U,s}|^2}.
$$

Then since

$$
|\Omega_U| = \frac{|GU_n(q)|}{|GU_h(q)| |GU_{n-h}(q)|} \quad \text{and} \quad |K_{U,s}| = \frac{|GU_n(q)|}{|GU_s(q)| |GU_{n-s}(q)|}
$$

we obtain (recalling from (29) that $|GU_n(q)| = q^{r^2} \varphi_U(n, q)$), the expression for $\theta(n, s, q)$ given in the statement.

To prove that $\theta(n, s, q) > 81/98$, we use bounds derived in [13]. For $1 \leq k \leq n, 1 \leq r < n$, define

$$
\Omega(k, n; -q) := \prod_{i=k}^{n} (1 - (-q)^{-i}) \quad \text{and} \quad \Delta(r, n; -q) := \frac{\Omega(1, n; -q)}{\Omega(1, r; -q) \Omega(1, n-r; -q)}
$$

so that (noting that $2s - n \leq n/3$ by assumption),

$$
\theta(n, s, q) = \frac{\Omega(2s - n + 1, n; -q)}{\Delta(s, n; -q)^2}.
$$

By [13, Lemma 3.2(b)], $\Delta(s, n; -q)$ is less than 1 if $s$ is odd and less than $28/27$ if $s$ is even. Since $s < n$, it follows from [13, Lemma 3.2(a)] that $\Omega(2s - n + 1, n; -q)$ is greater than 1 if $n$ is even and greater than $1 - q^{-2s+n-1} \geq 8/9$ if $n$ is odd. Hence $\theta(n, s, q) > \left(\frac{27}{28}\right)^2 \left(\frac{8}{9}\right)$. \hfill $\square$

**Proof of Theorem 1.** We shall prove this theorem at first for random elements $g \in GU_n(q)$ that are uniformly distributed in $GU_n(q)$. See the end of the proof for a short discussion of why these arguments generalise to nearly uniformly distributed random elements.

Let $t$ be a strong involution in $GU_n(q)$. Then $t$ is $(1/3, 2/3)$-balanced and so is of type $(s, n-s)$ with $n/3 \leq s \leq 2n/3$. We claim that it is enough to consider the case where $s \geq n/2$. Indeed, if $s < n/2$, then $-t$ is a strong involution in $GU_n(q)$ of type $(n-s, s)$ with $n-s > n/2$, and since $(-t)(-t^g) = tt^g$ the value of $z(g) := \text{inv}(tt^g)$ is unchanged. Thus by replacing $t$ by $-t$ where necessary, we assume for the rest of this proof that $n/2 \leq s \leq 2n/3$.

First consider the proof of (i). Let $K_{U,s}$ be the conjugacy class of $t$ in $GU_n(q)$, that is, the set of involutions of type $(s, n-s)$, and let $\pi_+$ be the probability that, for a random $g \in GU_n(q)$, the restriction of $\text{inv}(tt^g)$ to $E_+(t)$ is $(1/3, 2/3)$-balanced. Now $\pi_+$ is independent of the choice of $t$ in $K_{U,s}$. A straightforward counting argument shows that $\pi_+$ is equal to the proportion of $(t, t') \in K_{U,s} \times K_{U,s}$ such that:

(*) the restriction of $\text{inv}(tt')$ to $E_+(t)$ is $(1/3, 2/3)$-balanced.
If we choose \( \alpha \) and \( \beta \) as in Lemma 3.4, we see from Lemma 3.4(ii) that (*) holds for \((t, t')\) whenever \((t, t') \in L_U(n, s; q, \alpha, \beta)\). It is immediate from Definition 10.6 that \( \pi_+ \geq \ell_U(n, s, q; \alpha, \beta) \).

We now find \( \kappa \) and \( n_0 \) such that \( \ell_U(n, s, q; \alpha, \beta) \geq \kappa / \log n \) for all \( n \geq n_0 \). Suppose that \( n > e^4 \), or equivalently, that \( n > 54 \). Then there exists a unique \( b \geq 4 \) such that \( 2^{b-2} < \log n < 2^{b-1} \), or equivalently, setting \( d := 2^b \), \( n \) satisfies \( e^{d/4} < n \leq e^{d/2} \). Thus the conditions of Lemma 10.5 hold with \( m = n - s < e^{d/2} \), and hence

\[
(30) \quad j_U(2(n - s), q; \alpha, \beta) \geq \frac{0.05228}{d} \left( \log \left( \frac{1 - \alpha}{1 - \beta} \right) - \frac{d}{(n - s)(1 - \beta)} \right).
\]

Using the definitions of \( \alpha \) and \( \beta \) from Lemma 3.4, we first deduce that \((n - s)(1 - \beta) = (n - s)\frac{2}{3(n-s)} = \frac{2}{3} \geq \frac{2}{3} \) so that \( 1/(n - s)(1 - \beta) \leq 6/n \). We also see that

\[
\frac{1 - \alpha}{1 - \beta} = \begin{cases} \frac{2}{3(n-s)} & \text{if } n/2 \leq s \leq \frac{3n}{5}, \\ \frac{2}{s} & \text{if } \frac{3n}{5} \leq s \leq \frac{2n}{3}, \\ \end{cases}
\]

which implies that \( \log ((1 - \alpha)/(1 - \beta)) \geq \log 3/2 > 0.4054 \). Substituting into (30) we get

\[
j_U(2(n - s), q; \alpha, \beta) \geq \frac{0.05228}{d} \left( 0.4054 - \frac{6d}{n} \right) = 0.05228 \left( \frac{0.4054}{d} - \frac{6}{n} \right) = \zeta_1(n, d), \text{ say.}
\]

Elementary calculus shows that the \( \zeta_1(n, d) \log n \) increases with \( n \), for fixed \( d > 0 \) and \( n \geq 3 \). First consider the case where \( b = 4 \) and \( d = 2^4 \) (in this case \( 54 = [e^4] < n \leq 2980 = [e^8] \)). Since \( \zeta_1(250, 16) \log 250 > 0.0003 \), we have \( \zeta_1(n, 16) \log n > 0.0003 \) for all \( n \geq 250 \). On the other hand, when \( b \geq 5 \), \( d := 2^b \) and \( e^{d/4} < n \leq e^{d/2} \), we have \( d/n < e^{-d/4}d \leq 32e^{-8} \leq 0.01074 \) and \( \log n > d/4 \). Thus \( \zeta_1(n, d) \log n > \frac{0.05228}{d}(0.4054 - 6 \times 0.01074)d > 0.0044 \) in this case. Hence \( j_U(2(n - s), q; \alpha, \beta) > \frac{0.0003}{\log n} \) holds for all \( n \geq 250 \). Finally, we have, applying Lemma 10.7,

\[
\pi_+ \geq \ell_U(n, s, q; \alpha, \beta) = \theta(n, s, q) j_U(n - h, q, \alpha, \beta)
\]

\[
> \frac{81}{98} \times \frac{0.0003}{\log n} > \frac{0.0002}{\log n}
\]

for all \( n \geq 150 \). This proves (i) with \( n_0 = 150 \) and \( \kappa = 0.0002 \), for uniformly distributed random elements.

The proof of Theorem 1 (ii) is similar. In this case we can take \( \alpha = 1/3 \) and \( \beta = 2/3 \) since Lemma 3.4 (ii) shows that \( z_{V_2} \) is an involution of type \((2k_+, 2k_-)\) and \( z_{E_8(t)} \) is of type \((k_+, k_-)\) so the former is \((1/3, 2/3)\)-balanced exactly when the latter is. We make a similar estimate using Lemma 10.5 for \( j_U(2(n - s), q; 1/3, 2/3) \) (noting that now \( 1/(n - s)(1 - \beta) = 3/(n - s) \leq 9/n \)). This shows that, for all \( n \geq 250 \), and \( d \) chosen as the power of \( 2 \) such that \( e^{d/4} < n \leq e^{d/2} \)

\[
j_U(2(n - s), q; \frac{1}{3}, \frac{2}{3}) \geq \frac{0.05228}{d} (\log 2 - \frac{9d}{n}) = \zeta_2(n, d), \text{ say.}
\]

We calculate that \( \zeta_2(250, 16) \log 250 > 0.00211 \) and conclude that \( \zeta_2(n, 16) \log n > 0.00211 \) for \( n \geq 250 \). Furthermore an argument similar to the one above
shows that when $b \geq 5$ and $e^{d/4} \leq n \leq e^{d/2}$ then $\zeta_2(n, d) \log n > \frac{0.05228}{d}(\log 2 - 9 \times 0.01074)^{1/2} > 0.0077$. Hence for all $n \geq 250$ we have

$$j_U(2(n-s), q; \frac{1}{3}, \frac{2}{3}) > \frac{0.00211}{\log n}$$

and so

$$\pi_- \geq \ell_U(n, s, q; \frac{1}{3}, \frac{2}{3}) > \frac{81}{98} \times \frac{0.00211}{\log n} > 0.00174 \log n.$$

This proves (ii) with $n_0 = 250$ and $\kappa = 0.0017$, and thus completes the proof of Theorem 1 with $\kappa = 0.0002$ and $n_0 := 250$, for uniformly distributed random elements.

For the general case of nearly uniformly distributed random elements, as at the beginning of this proof, let $\pi_+$ be the probability that for a nearly uniformly distributed random element $g \in G$, the restriction of $\text{inv}(t)g$ to $E_+(t)$ is $(1/3, 2/3)$-balanced. Since each $g \in G$ occurs with probability at least $\frac{1}{2|G|}$ (Definition 1.2), it follows that $\pi_+ > \frac{1}{2\log n}$. The rest of the proof follows as before, but the final value of $\kappa$ is halved. The argument for $\pi_-$ goes through in the same way. □

11. Proofs of remaining main theorems

11.1. Proof of Theorems 2 and 3. Before proving Theorem 2, we give a lemma which reduces the problem to proving the result for uniform distributions.

**Lemma 11.1.** Let $X$ be a nearly uniform random variable on a finite group $G$. Let $Y = [x_1, x_2, x_3]$ be the results of three independent trials. Then

$$P(g \in Y) \geq \frac{1}{|G|} \text{ for all } g \in G.$$

**Proof.** We may assume without loss of generality that $G$ is nontrivial. By definition of a nearly uniform distribution,

$$P(X = g) > \frac{1}{2|G|}.$$

Then $P(g \not\in Y) = (1 - P(X = g))^3 = 1 - 3P(X = g) + 3P(X = g)^2 - P(X = g)^3$, so

$$P(g \in Y) \geq \frac{3}{2|G|} - 3\left(\frac{1}{2|G|}\right)^2 + \left(\frac{1}{2|G|}\right)^3 = \frac{1}{|G|} + \frac{1}{|G|} \left(\frac{1}{2} - \frac{3}{4|G|} + \frac{1}{8|G|}\right),$$

which is greater than $\frac{1}{|G|}$ for all non-trivial $G$. □

The following definition is from [13].

**Definition 11.2.** Let $H$ be a group, and let $\mathcal{H} = \langle C_1, \ldots, C_c \rangle$ be a sequence of conjugacy classes of $H$. Then a $c$-tuple $(h_1, \ldots, h_c)$ is a class-random sequence from $\mathcal{H}$ if $h_i$ is a uniformly distributed random element of $C_i$ for all $i$, and the $h_i$ are independent.
Remark 11.3. As remarked in various previous papers, see for example [3], if \( g \) is a uniformly distributed random element of \( G \), and \( t \in G \) is an involution, then the element \( \text{inv}(tt^g) \) is uniformly distributed in its \( C_G(t) \)-conjugacy class. For let \( h \in C_G(t) \), and let \( \text{inv}(tt^g) = (tt^g)^m \). Then \( h^{-1}(tt^g)^m h = (t^{gh})^m = (tt^g)^m = (tt^g)^m \).

Proof of Theorem 2 By Lemma 11.1, it suffices to prove the theorem for uniform random elements, as tripling the number of random elements is sufficient to produce any given element with probability at least \( 1/|G| \).

In [13] it is shown that there exist constants \( c \) and \( n_2 \) such that for \( m \geq n_2 \), for any sequence \( H \) of \( c \) conjugacy classes of involutions, a class-random sequence from \( H \) generates \( SU_m(q) \) with probability at least \( 1 - q^{-m} \) (the constant \( n_2 \) can be taken to be around 400, and \( c \) to be 110).

Let \( s = \dim(V_+) \), and \( \epsilon \in \{+,-\} \). Let \( n_1 \) be such that \( n_1 \geq \max\{3n_2,n_0\} \), so that \( s,n-s \geq n_2 \).

By Theorem 1, the probability that a sequence of \( \kappa^{-1} \log n \) random elements \( g \) produce no strong involutions \( \text{inv}(tt^g)|_{V_+} \) is at most \((1 - \kappa / \log n)^{\kappa^{-1} \log n} < 1 - 1 + 1/2 - 1/6 + 1/24 = 3/8 \). Let \( m \in \mathbb{Z} \). Then the probability that \( m \kappa^{-1} \log n \) random elements \( g \) produce no strong involutions \( \text{inv}(tt^g)|_{V_+} \) is at most \((3/8)^m \), and can be made as small as required, subject to choosing \( m \) sufficiently large. By Remark 11.3, each such element \( \text{inv}(tt^g)|_{V_+} \) is uniformly distributed within its conjugacy class.

Let \( C \) be chosen such that with probability at least 0.9, a sequence \( A \) of \( C \log n \) independent uniform random elements of \( G \) contains an initial subsequence \( A_+ \) containing at least \( c \) elements \( g \) such that \( \text{inv}(tt^g)|_{V_+} \) is a strong involution, followed by a subsequence \( A_- \) containing at least \( c \) elements \( g \) such that \( \text{inv}(tt^g)|_{V_-} \) is a strong involution, and finally subsequence \( B \) containing at least one further \( g \in G \) such that \( z = \text{inv}(gg^g) \) is a strong involution on \( V_- \).

Let \( K_1 = \langle \text{inv}(tt^g) : g \in A_+ \rangle \), and \( K_2 = \langle \text{inv}(tt^g) : g \in A_- \rangle \). Set \( K = \langle K_1, K_2 \rangle \leq C_{GU_m(q)}(t) \). By [13], \( K_1|_{V_+} \geq SU(V_+) \) with probability at least \( 1 - q^{-s} \), and independently \( K_2|_{V_-} \geq SU(V_-) \) with probability at least \( 1 - q^{-(n-s)} \). Hence the probability of \( K \) inducing both \( SU(V_+) \) and \( SU(V_-) \) is at least \((1 - q^{-s})(1 - q^{-(n-s)}) \), and noting that this expression is decreasing as \( s \) goes from \( n/3 \) to \( n/2 \) we see that this probability is at least \( 1 - q^{-n/3} - q^{-2n/3} + q^{-n} \).

If \( s \neq n/2 \) then any subdirect product \( K \) of \( SU_s(q) \times SU_{n-s}(q) \) is the full direct product, and the theorem is shown, with \( H = K \), so assume now that \( s = n/2 \) and that \( K \cong SU_{n/2}(q) \) is a diagonal subgroup, with isomorphism \( \phi \) from \( K^{SU(V_+)} \) to \( K^{SU(V_-)} \).

Let \( H = \langle K,z \rangle \), let \( z_+ = z|_{V_+} \) and \( z_- = z|_{V_-} \). If \( \phi(z_+) \) is not conjugate to \( z_- \) in \( SU(V_-) \) then \( H \geq SU_{n/2}(q)^2 \), so assume otherwise. The element \( z \) is uniformly distributed in its \( C_G(t) \)-conjugacy class, so \( z_- \) is uniformly distributed in its \( SU(V_-) \).2-conjugacy class (where \( SU(V_-) \).2 denotes the elements of \( GU(V_-) \) with determinant \( \pm 1 \)). The smallest conjugacy class of strong involutions in \( GU_{n/2}(q) \) has size \( |GU_{n/2}(q)|/|GU_{n/6}(q) \times GU_{n/3}(q)| \geq \frac{2}{16} q^{n^2/4 - n^2/36 - n^2/9} \) (using the bounds on \( |GU_{n}(q)| \) from [13, Table 4]). Each conjugacy class in \( GU_{n/2}(q) \) splits into at most \( q + 1 < q^2 \) conjugacy classes in \( SU_{n/2}(q) \), so each conjugacy
class of strong involutions in $SU_{n/2}(q)$ has size greater than $\frac{q}{16}q^{n^2/9-2}$. Thus, the probability that $z_-$ is equal to $\phi(z_+)$ is less than $2q^{-n^2/9+2}$, and so the probability that $H$ contains $SU_s(q) \times SU_{n-s}(q)$ is at least

$$0.9(1 - q^{-n/3} - q^{-2n/3} + q^{-n})(1 - 2q^{-n^2/9+2}) > 0.9(1 - q^{-n/3} - q^{-2n/3}).$$

This completes the proof of Theorem 2. \hfill \Box

**Proof of Theorem 3** This follows immediately from Theorem 2 for $n \geq n_1$, so assume that $n < n_1$. Parker and Wilson show in [12] that there is a positive constant $a$ such that if $t$ is any involution in $G$, then the proportion of ordered pairs $(t, t^g)$ such that $tt^g$ has odd order is bounded below by $an^{-1}$. If $tt^g$ has odd order $2k+1$, then $g[t, g]^k$ is a uniformly distributed random element of $C_G(t)$ (see [2]). Since the probability that two random elements of $SU_m(q)$ generate $SU_m(q)$ is greater than $1/2$ (see [10]), reasoning as in the case $n \geq n_1$ we can see that there is a constant $C_1$ such that if $A$ is a sequence of $C_1$ uniformly distributed random elements $g$ then the probability that $(g[t, g]^k : g \in A, |tt^g| = 2k + 1$ for some $k)$ contains $SU(V_+) \times SU(V_-)$ is greater than $0.9(1 - 3^{-n_1}) > 0.9(1 - q^{-n/3} - 2n/3)$. The result follows.

### 11.2. Proof of Theorem 5

The proof of the following lemma is similar to the proof of [14, Lemma 4.1(b)]. In it, we assume that the Gram matrix of the unitary form is the identity matrix. Recall $\varphi_U(m, z)$ from (29). We let $\varphi_U(z) = \lim_{m \to \infty} \varphi_U(m, z)$, and define $\varphi_U(0, z) = 1$.

**Lemma 11.4.** For $m \geq 1$ and $q$ odd, $\iota_U(2m, q) = r_U(2m, q)\Phi_U(m, q)$, where $\Phi_U(m, q) = \varphi_U(m, q)^4/\varphi_U(2m, q)$, and

$$\iota_U(2m + 1, q) = \iota_U(2m, q) \frac{(1 - (-1)^{m+1}q^{m-1})^2}{(1 + q^{-2m-1})(1 + q^{-1})} = r_U(2m, q) \varphi_U(m, q)^2 \varphi_U(m + 1, q)^2 \frac{(1 + 1/q)\varphi_U(2m + 1, q)}{(1 + q^{-1})^2}.$$

**Proof.** Assume first that $n = 2m$ is even, and let $x \in C_U(V)$, the conjugacy class of perfectly balanced involutions in $GU_{2m}(q)$ (see Definition 1.3). Then

$$|C_U(V)| = \left| \frac{GU_{2m}(q)}{|GU_{m}(q)|^2} \right|.$$

Hence, by (1),

$$\iota_U(2m, q) = \frac{|C_U(V)|}{|\iota_U(V)|^2} = \frac{|C_U(V)|}{|GU_{m}(q)|^2} = r_U(2m, q)\frac{|GU_{2m}(q)|^4}{|GU_{m}(q)|^4} \quad \text{(by Lemma 2.7)}$$

$$= r_U(2m, q)\frac{q^{m(m-1)/2} \prod_{i=1}^{m} (q^i - (-1)^i)}{\prod_{i=1}^{2m} (q^i - (-1)^i)}$$

$$= r_U(2m, q)\frac{q^{m^2}\varphi_U(m, q)}{q^{2m} \varphi_U(2m, q)} = r_U(2m, q)\frac{2_m(U, q)^4}{\varphi_U(2m, q)} = r_U(2m, q)\Phi_U(m, q).$$
as required. Now let $n = 2m + 1$ be odd, so that $V = \mathbb{F}_{q^2}^{2m+1}$. Similarly to the even-dimensional case, we see that

$$|C_u(V)| = \frac{|GU_{2m+1}(q)|}{|GU_m(q)| \cdot |GU_{m+1}(q)|}.$$ 

Let $(x, x') \in I_u(V)$, as in (1), and $y = xx'$. By [14, Lemma 3.1(b)], $\gcd(c_y(X), X^2 - 1) = X - 1$, and $x$ and $x'$ both negative the 1-dimensional fixed point space $V_+$ of $y$. The element $y$, and hence also the pair $(x, x')$, determine a decomposition of $V$ as in (10), which we can write as

$$V = V_0 \perp V_\pm,$$

where $V_0$ is the sum of the $V_f$ for $f$ in Case A, B, C and D. We define $x_0 := x|_{V_0}$ and $y_0 = y|_{V_0}$, and note that since $V_0$ is non-degenerate, $x_0, y_0 \in GU(V_0)$ and so in particular $(x_0, y_0) \in \Delta_u(V_0)$.

Conversely, the decomposition $V = V_0 \perp V_\pm$, together with the pair $(x_0, y_0)$, uniquely determines $(x, y)$ and hence also $(x, x')$, because (i) $x$ negates $V_\pm$, so $x = -I_{\pm} + x_0$; whilst (ii) $y$ fixes $V_\pm$, so $y = I_{\pm} \oplus y_0$.

Thus $|I_u(V)|$ is the product of $|\Delta_u(V_0)| = |\Delta_u(2m, q)|$, and the number of decompositions of $V$ into an orthogonal sum of a non-degenerate $2m$-space and a non-degenerate 1-space. The number of such decompositions is the index in $GU_{2m+1}(q)$ of the stabiliser of a non-degenerate 1-space, so

$$\iota_u(2m + 1, q) = \frac{|I_u(V)|}{|C(V)|^2} = \frac{|GU_{2m+1}(q)|}{|GU_m(q)||GU_{m+1}(q)|} = \frac{|\Delta_u(2m, q)|}{(q+1)|GU_{2m}(q)||GU_{m+1}(q)|^{2}}$$

$$= \frac{r_u(2m, q) \cdot |GU_m(q)|^2|GU_{m+1}(q)|^2}{(q+1)|GU_{2m}(q)||GU_{m+1}(q)|^{2}} = \frac{r_u(2m, q) \cdot \varphi_u(m, q)^2 \varphi_u(m+1, q)^2}{(1+q^2)\varphi_u(2m+1, q)^2}\frac{\varphi_u(2m, q)^2 \varphi_u(m, q)^2}{(1+q)\varphi_u(2m+1, q)^2}$$

$$= \iota_u(2m, q) \cdot \frac{\varphi_u(m, q)^2 \varphi_u(m+1, q)^2}{(1+q^2)\varphi_u(2m+1, q)^2}$$

as required. 

Recall that we showed in Theorem 8.3 that $r_u(\infty, q) := \lim_{m \to \infty} r_u(2m, q)$ exists. The following corollary is immediate.

**Corollary 11.5.** The limits as $m \to \infty$ of $\iota_u(2m, q)$ and $\iota_u(2m+1, q)$ exist and satisfy

$$\lim_{m \to \infty} \iota_u(2m, q) = r_u(\infty, q) \cdot \varphi_u(q)^3$$

$$\lim_{m \to \infty} \iota_u(2m + 1, q) = r_u(\infty, q) \cdot \frac{\varphi_u(q)^3}{1+q^{-1}}$$

**Proof of Theorem 5.** By Corollary 9.13, $r_u(2m, q) \geq r_u(2m, 3)$ for all odd $q \geq 3$. Hence by Theorem 8.10, $r_u(2m, q) \geq 0.3433$ for $m \geq 2$, whilst $r_u(2, q) \geq 0.25$.

**Claim:** For $m \geq 1$, $\Phi_u(m, q) = \frac{\varphi_u(m, q)^4}{\varphi_u(2m, q)^2} > 1$. 

First, for \( m = 1 \), we have \( D(1, q) = \frac{(1+q^{-1})^4}{(1+q^{-1})(1-q^{-2})} = \frac{(1+q^{-1})^2}{(1-q^{-1})} > 1 \). Similarly, for \( m = 2 \),
\[
\Phi_U(2, q) = \frac{(1 + q^{-1})^4(1 - q^{-2})^4}{(1 + q^{-1})(1 - q^{-2})(1 + q^{-3})(1 - q^{-4})} = \frac{(1 + q^{-1})^2(1 - q^{-2})^2}{(1 - q^{-1} + q^{-2})(1 + q^{-2})} > 1
\] since \( (1 + q^{-1})^2 > 1 + q^{-2} \) and \( (1 - q^{-2})^2 > 1 - q^{-1} + q^{-2} \) for \( q \geq 3 \). So assume that \( m \geq 3 \). If \( m \) is odd then an easy calculation shows that
\[
\Phi_U(m, q) = \Phi_U(m - 1, q) \cdot \frac{(1 + q^{-m})^4}{(1 + q^{-2m+1})(1 - q^{-2m})} > \Phi_U(m - 1, q).
\]
Thus it is sufficient to prove that \( \Phi_U(m, q) \geq \Phi_U(m - 2, q) \) for even \( m \geq 4 \) (since from this we conclude that, for \( m \geq 2 \), \( \Phi_U(m, q) \geq \Phi_U(2, q) > 1 \). For \( m \geq 4 \) even,
\[
\Phi_U(m, q) = \Phi_U(m - 2, q) \cdot \frac{(1 + q^{-m+1})^4(1 - q^{-m})^4}{(1+q^{-2m+1})(1-q^{-2m+2})(1+q^{-2m+2})(1-q^{-2m+1})}.
\]
The largest of the four terms in the denominator is \( 1 + q^{-2m+3} \), and it is straightforward to check that this is strictly less than \( (1 + q^{-m+1})(1 - q^{-m}) \). Thus \( \Phi_U(m, q) > \Phi_U(m - 2, q) \), and the Claim is proved.

Hence by Lemma 11.4 we find that \( \nu(2m, q) > r_u(2m, q) \geq 0.3433 \) for \( m \geq 2 \), whilst \( \nu(2, q) > r_u(2, q) \geq 0.25 \). This concludes the arguments for even dimension.

Let \( \delta(m, q) = \frac{(1 - (q^{-1} - q^{-2})}{{(1+q^{-2m-1})(1+q^{-1})}} \). Setting \( m = 1 \) and carrying out the division, we can bound \( \delta(1, q) > 1 - q^{-1} - q^{-2} \). We can explicitly calculate \( \delta(1, 3) = 4/7 \), whilst for \( q = 5 \) our bound shows that \( \delta(1, q) > 1 - 1/5 - 1/25 = 19/25 > 4/7 \), so \( \delta(1, q) > 4/7 \) for all \( q \).

If \( m \geq 2 \) then performing the division shows that \( \delta(m, q) > 1 - q^{-1} + q^{-2} - q^{-3} \geq 20/27 \).

The result for \( \nu(2m + 1, q) \) now follows from Lemma 11.4 and our bounds for \( \nu(2m, q) \). \( \square \)

References

[1] László and Guest Babai Simon and Praeger, Proportions of r-regular elements in finite classical groups, J. Lond. Math. Soc. (2) 88 (2013), 202–226. ↑1
[2] J.N. Bray, An improved method for generating the centralizer of an involution, Arch. Math. (Basel) 74 (2000), 241–245. ↑1, 50
[3] John D. Dixon, Cheryl E. Praeger, and Ákos Seress, Strong involutions in finite special linear groups of odd characteristic, J. Algebra 498 (2018), 413–447, DOI 10.1016/j.jalgebra.2017.11.047. ↑2, 3, 10, 20, 21, 30, 31, 39, 40, 41, 44, 46, 49
[4] Jason Fulman, Peter M. Neumann, and Cheryl E. Praeger, A generating function approach to the enumeration of matrices in classical groups over finite fields, Mem. Amer. Math. Soc. 176 (2005), no. 830, vi+90, DOI 10.1090/memo/0830. MR2145026 (2006b:05125) ↑8, 19, 20, 21, 28, 29, 38
[5] B. Huppert, Endliche Gruppen. I, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967 (German). MR0224703 (37 #302) ↑11, 13, 15
[6] Bertram Huppert, Isometrien von Vektorräumen I, Arch. Math. (Basel) 35 (1980), no. 1-2, 164–176. ↑12, 15
[7] Isometrien von Vektorräumen II, Math. Z. 175 (1980), no. 1, 5–20. ↑12, 15
[8] Irving Kaplansky, Linear Algebra and Geometry: A Second Course, 2nd edition, Chelsea Publishing Company, New York, 1974 (English). ↑12
[9] C.R. Leedham-Green and E.A. O’Brien, Constructive recognition of classical groups in odd characteristic, J. Algebra 322 (2009), 833–881. ↑3
[10] Nina E. Menezes, Martyn Quick, and Colva M. Roney-Dougal, The probability of generating a finite simple group, Israel J. Math 198 (2013), 371–392.

[11] Alice C. Niemeyer, Tomasz Popiel, and Cheryl E. Praeger, Algorithms to identify abundant p-singular elements in finite classical groups, Bull. Aust. Math. Soc. 86 (2012), no. 1, 50–63, DOI 10.1017/S0004972712000317.

[12] C. W. Parker and R. A. Wilson, Recognising simplicity of black-box groups by constructing involutions and their centralisers, J. Algebra 324 (2010), 885–915.

[13] Cheryl E. Praeger and Ákos Seress, Probabilistic generation of finite classical groups in odd characteristic by involutions, J. Group Theory 14 (2011), no. 4, 521–545, DOI 10.1515/JGT.2010.061.

[14] Cheryl E. Praeger and Ákos Seress, Regular semisimple elements and involutions in finite general linear groups of odd characteristic, Proc. Amer. Math. Soc. 140 (2012), no. 9, 3003–3015, DOI 10.1090/S0002-9939-2012-11491-1.

[15] Olga Taussky and Hans Zassenhaus, On the similarity transformation between a matrix and its transpose (1958).

[16] A. Voss, Zur Theorie der orthogonalen Substitutionen, Math. Ann. 13 (1878), 320–374.

[17] G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, J. Austral. Math. Soc. 3 (1963), 1–62. MR0150210 (27 #212)

Stephen Glasby & Cheryl E. Praeger: Centre for the Mathematics of Symmetry and Computation, Department of Mathematics and Statistics, University of Western Australia, Crawley, WA 6009, Australia

Colva M. Roney-Dougal: Mathematical Institute, University of St Andrews, KY16 9SS, United Kingdom