# Involution centralisers in finite unitary groups of odd characteristic

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

Abstract. We analyse the complexity of constructing involution centralisers in unitary groups over fields of odd order. In particular, we prove logarithmic bounds on the number of random elements required to generate a subgroup of the centraliser of a strong involution that contains the last term of its derived series. We use this to strengthen previous bounds on the complexity of recognition algorithms for unitary groups in odd characteristic. Our approach generalises and extends two previous papers by the second author and collaborators on strong involutions and regular semisimple elements of linear groups.

## 1. Introduction

Parker and Wilson [**12**] showed in 2010 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 $(t, t^g)$ of involutions. If $g$ is a uniformly distributed random element of a group $G$, and $y = tt^g$ has odd order $2k + 1$, then $z = gy^k$ is a uniformly distributed random element of $C = C_G(t)$. This observation is due to Richard Parker, see [**2**, Theorem 3.1]. Parker and Wilson in [**12**, Theorem 2] showed that if $G$ is a simple classical group of dimension $n$, then the proportion of elements $g$ of $G$ 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**, p. 897] and [**1**, Theorem 1.2]). If $y = tt^g$ has even order $2k$, then $z = y^k$ is an involution in the centraliser $C$ of $t$. However, these elements $z$ are *not* uniformly distributed in $C$; instead $z$ is uniformly distributed only within its $C$-conjugacy class.

In this paper we analyse the centralisers $C$ of strong involutions $t$ (see Definition 1.1) in unitary groups $G$ in odd characteristic. We show that there exists an absolute constant $D$ such that given a strong involution $t$, a set of $D \log n$ random elements $g$ suffices to

---

*Date*: Friday 20$^{\text{th}}$ September, 2019.

*Key words and phrases.* Involution centralisers, recognition algorithms, classical groups, unitary groups, regular semisimple elements, group generation.

construct a set of involutions that generates a group containing the last term in the derived series of $C_G(t)$. A careful analysis of the highest power of 2 dividing $|tt^g|$ is required here. Our methods build on the work of Praeger and Seress [**14**], and of Dixon, Praeger and Seress [**3**], but we encounter fundamental new difficulties: the structure of regular semisimple elements in $\mathrm{GU}_n(q)$ that are "almost irreducible" (in a sense that we shall make precise in Definition 2.7) and conjugate to their inverses is very different from those in $\mathrm{GL}_n(q)$. 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 $\mathrm{Sp}_4(3)$ and $\mathrm{Sp}_6(3)$ there are no regular semisimple elements that are inverted by involutions.

DEFINITION 1.1. For an involution $t \in \mathrm{GL}_n(q^2)$, we write $E_+(t)$ and $E_-(t)$ to denote its eigenspaces for eigenvalues $+1$ and $-1$. Such a $t$ is *strong* if $n/3 \leqslant \dim(E_+(t)) \leqslant 2n/3$. For an element $x$ of a group $G$, let $\mathrm{inv}(x)$ denote $x^{|x|/2}$ when $|x|$ is even, and $1_G$ otherwise.

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 $n \geqslant n_0$, that $t$ is a strong involution in $\mathrm{GU}_n(q)$ with $q$ odd, and that $g$ is a nearly uniformly distributed random element of $\mathrm{GU}_n(q)$. Let $z(g) := \mathrm{inv}(tt^g)$, and let $z(g)_\varepsilon$ be the restriction of $z(g)$ to the eigenspace $E_\varepsilon(t)$ (where $\varepsilon \in \{+,-\}$). 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 are $n_0 = 700, \kappa = 0.0001$, and echoing the view expressed there, 'we believe that these constants are far from best possible'.

From Theorem 1, and [**3**, Theorem 1.1], we are able to deduce the following result (see §11).

THEOREM 2. *There exist constants $\lambda, n_1 \in \mathbb{R}$ such that the following is true. Let $n \geqslant n_1$, let $G = \mathrm{GL}_n(q)$ or $\mathrm{GU}_n(q)$ with $q$ odd, and let $t \in G$ be a strong involution. For $\varepsilon \in \{+,-\}$, let $S_\varepsilon = \mathrm{SL}(E_\varepsilon(t))$ if $G = \mathrm{GL}_n(q)$, or $\mathrm{SU}(E_\varepsilon(t))$ if $G = \mathrm{GU}_n(q)$. Let $A$ be a sequence of at least $\lambda \log n$ random elements of $G$, chosen independently and nearly uniformly, and let $H = \langle \mathrm{inv}(tt^g) \mid g \in A \rangle$. Then*

$$\mathbb{P}(H \text{ contains } S_+ \times S_-) > 0.9(1 - q^{-n/3} - q^{-2n/3}).$$

One of our motivations for proving the preceding two theorems was an application to computational group theory. Two key steps in many algorithms (for example, those in [**7**, **8**, **12**]) are first to construct an involution $t$ in a group $G$ of Lie type, and then to construct a subgroup of the centraliser of $t$ that contains the last term, $C_G(t)^\infty$, in the derived series of $C_G(t)$. For some of these algorithms, including the constructive recognition algorithms in [**7**], the involution $t$ is required to be strong.

Definition 1.3. Let $G$ be a group. For an involution $t$ and an element $g$ of $G$, we let $R(g,t)$ be $\mathrm{inv}(y)$ when $y := tt^g$ has even order, and $gy^{\lfloor |y|/2 \rfloor}$ when $|y|$ is odd. It follows that $R(g,t) \in C_G(t)$.

Building on work of Lübeck, Niemeyer and Praeger [**9**], we can remove the degree restriction in Theorem 2, and include the step of finding a strong involution, whilst only slightly worsening the probability of success (see §11).

Theorem 3. *There exists a positive constant $\mu$ such that for all $n \geqslant 3$, for all odd $q$, and for $G = \mathrm{GL}_n(q)$ or $\mathrm{GU}_n(q)$, the following holds with probability at least* $0.89(1 - q^{-n/3} - q^{-2n/3})$. *A sequence $S$ of $\lceil \mu \log n \rceil$ independent nearly uniformly distributed random elements of $G$ contains an element $x$ such that $t := \mathrm{inv}(x)$ is a strong involution, and moreover $C_G(t) \geqslant \langle R(g,t) \mid g \in S \rangle \geqslant C_G(t)^\infty$.*

Leedham-Green and O'Brien in [**7**] define certain generating sets for the quasisimple classical groups in odd characteristic, called *standard generators*, and use a recursive approach, via repeated involution centralisers, to find these standard generators in the given group. Our improved analysis in Theorem 3 of the number of random elements required to construct an involution centraliser enables us to replace a factor of $n$ in their complexity analysis with a factor of $\log n$. Let $\xi$ denote an upper bound on the number of field operations needed to construct an independent nearly uniformly distributed random element of $\mathrm{SU}_n(q)$, and let $\chi(q)$ be an upper bound on the number of field operations equivalent to a call to a discrete logarithm oracle for $\mathbb{F}_q$. Reasoning in the same way as [**3**, §1.1], the following can be deduced from [**7**] and Theorem 3.

Theorem 4. *Let $q$ be odd, and let $S = \mathrm{SU}_n(q)$. There is a Las Vegas algorithm that takes as input a set $A$ of generators for $S$ of bounded cardinality, and returns standard generators for $S$ as straight line programmes of length $O(\log^3 n)$ in $A$. The algorithm has complexity $O(\log n(\xi + n^3 \log n + n^2 \log n \log\log n \log q + \chi(q^2)))$, measured in field operations.*

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

Definition 1.4. Denote the characteristic polynomial of a square matrix $y$ by $c_y(X)$. Such a matrix $y$ is *regular semisimple* if $c_y(X)$ is multiplicity-free. Let $V = \mathbb{F}_{q^2}^n$, with $q$ odd, equipped with a unitary form having Gram matrix the identity matrix $I_n$. We say that an involution $t \in \mathrm{GL}_n(q^2)$ is *perfectly balanced* if $\dim(E_+(t)) = \lfloor n/2 \rfloor$. Following [**14**], we define $\mathcal{C}(V)$ to be the class of perfectly balanced involutions in $\mathrm{GL}_n(q^2)$, and we define $\mathcal{C}_{\mathsf{U}}(V)$ to be $\mathcal{C}(V) \cap \mathrm{GU}_n(q)$.

We let

$$\mathbf{I}_{\mathsf{U}}(V) = \mathbf{I}_{\mathsf{U}}(n,q) = \{(t,t') \in \mathcal{C}_{\mathsf{U}}(V) \times \mathcal{C}_{\mathsf{U}}(V) \mid y := tt' \text{ is regular semisimple}\}. \tag{1}$$

THEOREM 5. *For $q$ odd, let $\iota_{\mathsf{U}}(n,q) = |\mathbf{I}_{\mathsf{U}}(V)|/|\mathcal{C}_{\mathsf{U}}(V)|^2$ be the probability that a random element $(t,t') \in \mathcal{C}_{\mathsf{U}}(V) \times \mathcal{C}_{\mathsf{U}}(V)$ lies in $\mathbf{I}_{\mathsf{U}}(V)$. If $n \neq 3$ then $\iota_{\mathsf{U}}(n,q) > 0.25$, and $\iota_{\mathsf{U}}(3,q) > 0.142$.*

REMARK 1.5. We prove that $\iota_{\mathsf{U}}(2,q) > 0.25$, that $\iota_{\mathsf{U}}(n,q) > 0.343$ for $n \geqslant 4$ even, and that $\iota_{\mathsf{U}}(n,q) > 0.254$ for $n \geqslant 5$ odd. We shall also prove in Corollary 11.4 that the limits as $m \to \infty$ of $\iota_{\mathsf{U}}(2m,q)$ and $\iota_{\mathsf{U}}(2m+1,q)$ exist, and determine each limit.

The structure of this paper is as follows. In §2 we begin our exploration of the conjugacy classes of $\mathrm{GU}_n(q)$, and of the characteristic polynomials of elements of $\mathrm{GU}_n(q)$. In §3 we define a set of ordered pairs of conjugate involutions $(t, t^g)$ such that $\mathrm{inv}(tt^g)|_{E_+(t)}$ is guaranteed to be a strong involution. Thus to prove Theorem 1 it suffices to show that this set is sufficiently large. In §§4, 5 and 6 we classify the $\mathsf{U}*$-irreducible regular semisimple elements of $\mathrm{GU}_n(q)$ (that is, such elements that are as close to irreducible as possible, see Definition 2.7), determine their centralisers, and count the number of involutions inverting them. In §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 $\mathsf{U}*$-irreducible regular semisimple elements. In §8 we define and analyse our key generating function, $R_{\mathsf{U}}(q,u)$. In §9 we factorise $R_{\mathsf{U}}(q,u)$, and prove bounds on the coefficients of certain generating functions that refine the information in $R_{\mathsf{U}}(q,u)$. This additional information allows us to control the powers of 2 dividing the orders of the roots of the characteristic polynomial of $tt^g$, and hence to bound the dimension of the $(-1)$-eigenspace of $\mathrm{inv}(tt^g)$. In §10 we prove Theorem 1, and finally in §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 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. We thank Eamonn O'Brien for his extremely careful reading of several drafts of this article.

## 2. Preliminaries

In this section we study the conjugacy classes and characteristic polynomials of involutions in $\mathrm{GU}_n(q)$, and of regular semisimple elements of $\mathrm{GU}_n(q)$ that are products of involutions. We shall assume throughout the paper that $q$ is an odd prime power.

Let $V = \mathbb{F}_{q^2}^n$ be the natural module for $\mathrm{GU}_n(q)$, and unless stated otherwise, take the sesquilinear form fixed by $\mathrm{GU}_n(q)$ to have the identity matrix $I_n$ as its Gram matrix as in Definition 1.4. Determining conjugacy in $\mathrm{GU}_n(q)$ is straightforward:

THEOREM 2.1. (Wall, [**16**, p. 34]) *Let $g, h \in \mathrm{GU}_n(q)$. If $g$ and $h$ are conjugate in $\mathrm{GL}_n(q^2)$ then they are conjugate in $\mathrm{GU}_n(q)$.*

DEFINITION 2.2. An involution $t \in \mathrm{GL}_n(q^2)$ has *type* $(a,b)$ if $\dim(E_+(t)) = a$ and $\dim(E_-(t)) = b$.

For $q$ odd, involutions in $\mathrm{GL}_n(q^2)$ are conjugate if and only if they have the same type. The following corollary of Theorem 2.1 is therefore immediate.

Corollary 2.3. *Each type $(n_+, n_-)$ of involution in $\mathrm{GL}_n(q^2)$ forms a unique conjugacy class in $\mathrm{GU}_n(q)$. In particular, $\mathcal{C}_{\mathsf{U}}(V)$ is a $\mathrm{GU}_n(q)$-conjugacy class.*

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

$$f(X) := X^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{F}_{q^2}[X], \tag{2}$$

and let $\sigma$ be the involutory automorphism $\sigma : x \mapsto x^q$ of $\mathbb{F}_{q^2}$. Then we define the $\sigma$-*conjugate* of $f(X)$ 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 $*$-*conjugate* of $f(X)$ to be

$$f^*(X) := X^n + a_1 a_0^{-1} X^{n-1} + a_2 a_0^{-1} X^{n-2} + \cdots + a_{n-1} a_0^{-1} X + a_0^{-1} \tag{3}$$

and define

$$f^\sim(X) := f^{\sigma *}(X) = f^{*\sigma}(X).$$

It is clear that the operations $*$ and $\sim$ 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 $\mathrm{GL}_n(q^2)$ induced by replacing each matrix entry by its image under $\sigma$. We write $A^T$ for the transpose of a matrix $A$, and write $h^\sim = h^{-\sigma T}$ for $h \in \mathrm{GL}_n(q^2)$.

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

Lemma 2.4. *A conjugate of $h \in \mathrm{GL}_n(q^2)$ lies in $\mathrm{GU}_n(q)$ if and only if $h$ is conjugate to $h^\sim$.*

Notice that the characteristic polynomial $g(X) = c_h(X)$ of $h \in \mathrm{GL}_n(q^2)$ satisfies $c_{h^{-1}}(X) = g^*(X)$, and $c_{h^\sim}(X) = g^\sim(X)$.

Corollary 2.5. *Let $y \in \mathrm{GL}_n(q^2)$ be regular semisimple, and let $g(X) = c_y(X)$.*

(i) *A conjugate of $y$ lies in $\mathrm{GU}_n(q)$ if and only if $g(X) = g^\sim(X)$.*
(ii) *If $y \in \mathrm{GU}_n(q)$ then $y$ is conjugate in $\mathrm{GU}_n(q)$ to $y^{-1}$ if and only if $g(X) = g^*(X)$.*

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 $g(X)$ is multiplicity-free. The fact that $y$ and $y^{-1}$ are conjugate in $\mathrm{GU}_n(q)$ (rather than just in $\mathrm{GL}_n(q^2)$) follows from Theorem 2.1. □

Recall that $\mathcal{C}(V)$ is the class of perfectly balanced involutions (Definition 1.4). The importance of $\mathcal{C}(V)$ for studying regular semisimple elements is illustrated by the following:

Lemma 2.6 ([**14**, Lemma 3.1]). *Let $t, y \in \mathrm{GL}_n(q^2)$, 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 $\mathcal{C}(V)$ and $n$ is even.*

(ii) *If* $t, t' \in \mathrm{GL}_n(q^2)$ *are conjugate in* $\mathrm{GL}_n(q^2)$ *then either* $t, t' \in \mathcal{C}(V)$ *or* $-t, -t' \in \mathcal{C}(V)$.

(iii) *If* $t, t' \in \mathcal{C}(V)$ *and* $n$ *is even, then* $\gcd(c_y(X), X^2 - 1) = 1$.

Proof. 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)]. □

We shall need the following three properties of polynomials.

Definition 2.7. Let $g(X) \in \mathbb{F}_{q^2}[X]$. We say that $g(X)$ is *separable* if it has no repeated roots in the algebraic closure $\overline{\mathbb{F}_{q^2}}$. The polynomial $g(X)$ is $\mathsf{U}*$-*closed* if $g(X) = g^{\sim}(X) = g^*(X)$, and is $\mathsf{U}*$-*irreducible* if it is $\mathsf{U}*$-closed and no proper nontrivial divisor of $g(X)$ is $\mathsf{U}*$-closed.

Definition 2.8. Define $\Pi_{\mathsf{U}}(n, q)$ to be the set of separable, degree $n$, monic, $\mathsf{U}*$-closed polynomials over $\mathbb{F}_{q^2}$ with no roots 0, 1, $-1$.

For $n = 2m$, we define the following set, recalling that $\mathcal{C}_{\mathsf{U}}(V) = \mathcal{C}(V) \cap \mathrm{GU}_n(q)$:

$$\Delta_{\mathsf{U}}(V) = \Delta_{\mathsf{U}}(2m, q) := \left\{ (t, y) \;\middle|\; \begin{array}{l} t \in \mathcal{C}_{\mathsf{U}}(V), y \in \mathrm{GU}(V), y^t = y^{-1}, y \text{ regular} \\ \text{semisimple, and } c_y(X) \text{ coprime to } X^2 - 1 \end{array} \right\}. \tag{4}$$

This set is analogous to the set $\mathbf{RI}(V)$ defined in [**14**, Equation (3)]. We now show the link between $\Delta_{\mathsf{U}}(V)$ and and $\Pi_{\mathsf{U}}(n, q)$. Recall the definition of $\mathbf{I}_{\mathsf{U}}(n, q)$ from (1).

Lemma 2.9. *With respect to a fixed unitary form,* $\Delta_{\mathsf{U}}(n, q)$ *is equal to the set*

$$\left\{ (t, y) \mid t \in \mathrm{GU}_n(q),\ y \in \mathrm{SU}_n(q),\ t^2 = 1, y^t = y^{-1}, c_y(X) \in \Pi_{\mathsf{U}}(n, q) \right\}.$$

*When* $n$ *is even,* $|\Delta_{\mathsf{U}}(n, q)| = |\mathbf{I}_{\mathsf{U}}(n, q)|$.

Proof. Let $S$ denote the displayed set. We show first that $S \subseteq \Delta_{\mathsf{U}}(n, q)$. Let $(t, y) \in S$. Then $t$ inverts $y$, and our assumption that $c_y(X) \in \Pi_{\mathsf{U}}(n, q)$ implies that $y$ is regular semisimple and $\gcd(c_y(X), X^2 - 1) = 1$. Hence $t \in \mathcal{C}_{\mathsf{U}}(V)$ by Lemma 2.6, and therefore $(t, y) \in \Delta_{\mathsf{U}}(n, q)$.

For the reverse containment, let $(t, y) \in \Delta_{\mathsf{U}}(n, q)$. Since $y^t = y^{-1}$, with $y$ regular semisimple and $c_y(X)$ coprime to $X^2 - 1$, all involutions in $\mathrm{GU}_n(q)$ inverting $y$ are in $\mathcal{C}_{\mathsf{U}}(V)$ by Lemma 2.6. Let $t' = ty$. Then $t'$ also inverts $y$, so $t' \in \mathcal{C}_{\mathsf{U}}(V)$ by Lemma 2.6. Hence, by Theorem 2.1 the involutions $t$ and $t'$ are $\mathrm{GU}_n(q)$-conjugate. Then $y = tt'$ is a product of two conjugate involutions in $\mathrm{GU}_n(q)$, and so $y \in \mathrm{SU}_n(q)$. Therefore $(t, y) \in S$.

For the final claim, consider the map $\theta : (t, t') \mapsto (t, tt') = (t, y)$ from $\mathbf{I}_{\mathsf{U}}(V)$ to $\mathcal{C}_{\mathsf{U}}(V) \times \mathrm{GU}(V)$. 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 $\Delta_{\mathsf{U}}(V)$. Hence $|\mathbf{I}_{\mathsf{U}}(V)| \leqslant |\Delta_{\mathsf{U}}(V)|$. It follows from [**14**, Lemma 4.1(a)] that $\Delta_{\mathsf{U}}(V) \subseteq \mathrm{Im}(\theta)$, 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 $\mathrm{GU}_n(q)$ whose product $y = tt^g$ is such that $\mathrm{inv}(y)|_{E_+(t)}$ is strong. Recall that $V = \mathbb{F}_{q^2}^n$ is the natural module for $\mathrm{GU}_n(q)$.

First we make a simple observation about subspaces of $E_+(t)$.

LEMMA 3.1. *Let $t \in \mathrm{GU}_n(q)$ be an involution, and let $U$ be a subspace of $E_+(t)$. Then $U^\perp$ is $t$-invariant, and further if $U$ is non-degenerate then $U^\perp$ is also 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 $t^2 = 1$. This is equal to zero since $u^t \in U$. 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. □

Recall the definition of *type* (Definition 2.2), and that types naturally parametrise the conjugacy classes of involutions in $\mathrm{GU}_n(q)$ by Corollary 2.3.

DEFINITION 3.2. Given $0 \leqslant \alpha < \beta \leqslant 1$, an involution $t \in \mathrm{GL}_n(q^2)$ of type $(n_+, n_-)$ is *$(\alpha, \beta)$-balanced* if $\alpha \leqslant n_+/n \leqslant \beta$.

We shall now define a key set of ordered pairs of conjugate involutions.

DEFINITION 3.3. Let $K_{\mathsf{U},s}$ be the $\mathrm{GU}_n(q)$-conjugacy class of involutions of type $(s, n-s)$. Fix $0 \leqslant \alpha < \beta \leqslant 1$, and let $L_{\mathsf{U}}(n, s, q; \alpha, \beta)$ be the set of ordered pairs $(t, t') \in K_{\mathsf{U},s} \times K_{\mathsf{U},s}$ such that:

(i) $V_1 := E_+(t) \cap E_+(t')$ is a non-degenerate subspace of $V$, and has dimension $h = 2s - n$, (so, by Lemma 3.1, $V_2 := V_1^\perp$ is non-degenerate, $\langle t, t' \rangle$-invariant, and of dimension $n - h = 2(n - s)$);

(ii) $(t|_{V_2}, tt'|_{V_2}) \in \Delta_{\mathsf{U}}(n - h, q)$ and $\mathrm{inv}(tt'|_{V_2})$ is $(\alpha, \beta)$-balanced.

LEMMA 3.4. *Let $(t, t') \in L_{\mathsf{U}}(n, s, q; \alpha, \beta)$, and let $V_2$ be as in Definition 3.3. If $W$ is a $\langle t, t' \rangle$-invariant subspace of $V_2$, then $\dim W$ is even, and the involutions $t|_W$ and $t'|_W$ are both perfectly balanced.*

PROOF. The characteristic polynomial of $tt'|_{V_2}$ lies in $\Pi_{\mathsf{U}}(2(n - s), q)$ by Lemma 2.9, and in particular it is coprime to $X^2 - 1$. Thus also, by Definition 2.8, the characteristic polynomial of $tt'|_W$ lies in $\Pi_{\mathsf{U}}(r, q)$, where $r = \dim(W)$. It then follows from Lemma 2.6 that $r$ is even and both $t|_W$ and $t'|_W$ lie in $\mathcal{C}_{\mathsf{U}}(W)$ (and hence are perfectly balanced). □

LEMMA 3.5. *Let $s$ satisfy $2n/3 \geqslant s \geqslant n/2$, 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 $(t, t') \in L_{\mathsf{U}}(n, s, q; \alpha, \beta)$, and let $V_1$ and $V_2$ be as in Definition 3.3. Let $z = \mathrm{inv}(tt')$, $V_{2+} := V_2 \cap E_+(z)$ and $V_{2-} := E_-(z)$.*

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

| | $E_+(t)$ | $E_-(t)$ | $V$ |
|---|---|---|---|
| $V_1$ | $h$ | $0$ | $h$ |
| $V_{2+}$ | $k_+$ | $k_+$ | $2k_+$ |
| $V_{2-}$ | $k_-$ | $k_-$ | $2k_-$ |
| $V$ | $s$ | $n - s$ | $n$ |

(ii) *The involution $z_{\mid E_+(t)}$ is $(1/3, 2/3)$-balanced.*

PROOF. This proof has similarities to [**3**, p. 445], but we have modified the approach to make it more transparent and to deal with the unitary form. It is clear from the definitions of $\alpha$ and $\beta$ that $0 \leqslant \alpha \leqslant 1/3$ and $1/3 \leqslant \beta \leqslant 2/3$, and that if $\alpha = 1/3$ then $\beta > 1/3$, and so $\alpha < \beta$.

(i). The first and last rows of the table are clear, so we need only prove the middle two rows. Since $t$ is conjugate in $\mathrm{GU}_n(q)$ to a diagonal matrix, and our standard unitary form is the identity matrix, the spaces $E_\pm(t)$ 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, the subspace $V_1$ is fixed pointwise by $t$ and $t'$ and hence also by $z$, so that $E_+(z)$ contains both $V_1$ and $V_{2+}$. Since $V_{2+} \leqslant V_2 = V_1^\perp$ we have $V_1 \perp V_{2+} \leqslant E_+(z)$. Since $V = V_1 \perp V_2$, an arbitrary vector $v \in E_+(z)$ 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 $V_{2-} = E_-(z) = E_+(z)^\perp \leqslant V_1^\perp = V_2$.

Let $D = \langle t, t' \rangle$. By Lemma 3.1, $V_2$ is $D$-invariant, and $D$ centralises $z$, so $V_{2+}$ and $V_{2-}$ are $D$-invariant subspaces of $V_2$. It follows from Lemma 3.4 that, for $\varepsilon = \pm$, $V_{2\varepsilon}$ has even dimension, say $2k_\varepsilon$, and that $\dim(E_+(t) \cap V_{2\varepsilon}) = \dim(E_-(t) \cap V_{2\varepsilon}) = \dim(V_{2\varepsilon})/2 = k_\varepsilon$.

(ii). The involution $z|_{V_2}$ is $(\alpha, \beta)$-balanced by Definition 3.3, so

$$\alpha \leqslant \frac{2k_+}{n-h} = \frac{k_+}{n-s} \leqslant \beta.$$

Let $z' := z|_{E_+(t)}$, 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 $1/3 \leqslant (h + k_+)/s \leqslant 2/3$.

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

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

Hence $s/3 \leqslant k_- \leqslant 2s/3$, which in turn implies that $1/3 \leqslant 1 - k_-/s = (h + k_+)/s \leqslant 2/3$, as required. □

## 4. U∗-irreducible polynomials

Recall the three involutory operations on polynomials that we defined in §2, and what it means for a polynomial to be U∗-irreducible (Definition 2.7). In this section we classify the U∗-irreducible polynomials, and determine the 2-*part-orders* of their roots (that is, the maximal power of 2 dividing the order of their roots).

In the remainder of the paper, we shall sometimes refer to a polynomial $f(X) \in \mathbb{F}_{q^2}[X]$ as simply $f$, when the meaning is clear.

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

(i) *If $f^*(X) = f(X)$ then either $f(X)$ is $X+1$ or $X-1$ or $m$ is even.*
(ii) *If $f^\sigma(X) = f(X)$ then $m$ is odd.*
(iii) *If $f(X) \neq X \pm 1$ then at least one of $f^\sigma(X), f^*(X)$ does not equal $f(X)$.*
(iv) *If $f(X) \neq X \pm 1$ and $f(X) = f^\sim(X)$ then $m$ is odd.*

Proof. Parts (i) and (ii) are proved in [4, Lemma 1.3.15(c) and Lemma 1.3.11(b)], respectively. Part (iii) follows immediately, so consider Part (iv). Suppose that $f(X) = f^\sim(X) \neq X \pm 1$. By Part (iii), at least one of $f^\sigma, f^*$ is not equal to $f$. Conversely, $f^\sim = f^{\sigma *} = f$, so we deduce that $f^\sigma = f^* \neq f$.

Let $\zeta \in \mathbb{F}_{q^{2m}}$ be a root of $f$, so that $f$ is the minimal polynomial of $\zeta$ over $\mathbb{F}_{q^2}$. Then the set of roots of $f^\sigma$ is $\{\zeta^q, \zeta^{q^3}, \ldots, \zeta^{q^{2m-1}}\}$ and the set of roots of $f^*$ is $\{\zeta^{-1}, \zeta^{-q^2}, \ldots, \zeta^{-q^{2m-2}}\}$. Since these sets are equal, $\zeta^{-1} = \zeta^{q^{2i+1}}$ for some $i$, and so $\zeta^{q^{2i+1}+1} = 1$. Hence $\zeta \in \mathbb{F}_{q^{4i+2}} = \mathbb{F}_{(q^2)^{2i+1}}$, an odd degree extension of $\mathbb{F}_{q^2}$. Thus $m = |\mathbb{F}_{q^2}(\zeta) : \mathbb{F}_{q^2}|$ is odd. □

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, $\omega(g)$ denotes the order of one (and hence all) of the roots of a $\mathsf{U}*$-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 $\omega(f)$.

Let $y \in \mathrm{GU}_n(q)$ be both regular semisimple and conjugate to its inverse. We distinguish five possibilities for irreducible factors $f(X)$ of the characteristic polynomial $c_y(X)$.

Proposition 4.3. *Let $y \in \mathrm{GU}_n(q)$ be regular semisimple, and let $f(X)$ be an irreducible factor of $c_y(X) \in \mathbb{F}_{q^2}[X]$ of degree $m$. If $y$ is conjugate to $y^{-1}$ in $\mathrm{GU}_n(q)$, then $c_y(X)$ is $\mathsf{U}*$-closed, and $f(X)$ satisfies precisely one of the following:*

**Type A.** *$f = f^* \neq f^\sigma$. Thus $f^\sim = f^\sigma \neq f$, $ff^\sim \mid c_y(X)$, $m$ is even, and $\omega(f) \mid (q^m+1)$.*
**Type B.** *$f = f^\sigma \neq f^*$. Thus $f^\sim = f^* \neq f$, $ff^\sim \mid c_y(X)$, $m$ is odd, and $\omega(f) \mid (q^m-1)$.*
**Type C.** *$f \neq f^* = f^\sigma$. Thus $f^\sim = f$, $ff^* \mid c_y(X)$, $m$ is odd, and $\omega(f) \mid (q^m+1)$.*
**Type D.** *$|\{f, f^*, f^\sigma, f^\sim\}| = 4$, $ff^*f^\sigma f^\sim \mid c_y(X)$, and $\omega(f) \mid (q^{2m}-1)$.*
**Type E.** *$f(X) = X \pm 1$.*

Proof. Let $g(X) = c_y(X)$. Since $y$ is conjugate to $y^{-1}$, we have $g = g^*$, and by Corollary 2.5, $g = g^\sim$. Thus $g^* = g^\sim$, and hence $g = g^\sigma$, so $g$ is $\mathsf{U}*$-closed.

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

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

Let $\zeta$ be a root of $f$. In Type A, the degree $m$ of $f$ is even by Lemma 4.1(i), and since $f = f^*$, the roots of $f$ in $\mathbb{F}_{q^{2m}}$ are

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

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

In Type B, the degree $m$ is odd by Lemma 4.1(ii), and we deduce from $f = f^\sigma$ that $\zeta^{q^{2i+1}-1} = 1$ for some $i$, and hence that $2i+1 = m$. In Type C, the degree $m$ is odd by Lemma 4.1(iv), and we use $f = f^{*\sigma}$ to reach a similar conclusion. For Type D, we shall see in §5 a construction of regular semisimple elements that is independent of the parity of $m$. □

Remark 4.4. We shall eventually see that almost all irreducible polynomials are of Type D, independent of the parity of $m$.

Remark 4.5. Observe that Type E is equivalent to $f(X) = f^*(X) = f^\sigma(X) \neq X$. Hence if $\deg f > 1$, then the hypotheses for Types A, B, C can be abbreviated to $f = f^*$, $f = f^\sigma$, and $f = f^\sim$, respectively.

Definition 4.6. If one (and hence all) of the irreducible factors of a $\mathsf{U}*$-irreducible polynomial $g(X) \neq X \pm 1$ are of Type A, B, C or D, then we say that $g(X)$ has this type.

Definition 4.7. Let $N(q^2, r)$ denote the number of monic irreducible polynomials $f(X) \in \mathbb{F}_{q^2}[X]$ 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 $|\mathcal{P}_{r,q^2}| = N(q^2, r)$).*

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

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

Definition 4.9. Let $\mathcal{D}_{4r}$ be the $\mathsf{U}*$-irreducible polynomials in $\mathbb{F}_{q^2}[X]$ of type D and degree $4r$ (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 $N_{\mathsf{U}}^-(q, 4r)$ be the number of monic $\mathsf{U}*$-irreducible polynomials $g \in \mathbb{F}_{q^2}[X]$ of degree $4r$ such that $\omega_2(g) = (q^{2r}-1)_2$.

We shall now show that $\mathcal{D}_{4r}^-$ contains all monic $\mathsf{U}*$-irreducible polynomials $g \in \mathbb{F}_{q^2}[X]$ of degree $4r$ such that $\omega_2(g) = (q^{2r}-1)_2$, so that $|\mathcal{D}_{4r}^-| = N_{\mathsf{U}}^-(q, 4r)$.

Lemma 4.10. *Let $g(X) \in \mathbb{F}_{q^2}[X]$ be a $\mathsf{U}*$-irreducible polynomial with an irreducible factor $f(X)$ of degree $r$.*

(i) *If $g(X)$ has type A, B or C, then $\omega_2(g) < (q^2-1)_2$.*
(ii) *If $g(X) \in \mathcal{D}_{4r}$ then $\omega_2(g) \leqslant (q^{2r}-1)_2$. At least $N(q^2, r)/8$ of the polynomials $g(X) \in \mathcal{D}_{4r}$ satisfy $\omega_2(g) = (q^{2r}-1)_2$.*
(iii) *$N_{\mathsf{U}}^-(q, 4r) = \left|\mathcal{D}_{4r}^-\right| \geqslant N(q^2, r)/8$, with equality if $r = 1$; and if $r = 2^{b-1} \geqslant 1$ then $N_{\mathsf{U}}^-(q, 4r) = (q^{2r}-1)/(8r)$.*

Proof. (i) It follows from Proposition 4.3 that $\omega_2(g)$ divides $2$, $q-1$, $q+1$ for Types, A, B and C, respectively. The result follows.

(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 $N(q^2,r)/2$ 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 types A, B or C, so the result follows.

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

Let $r=1$. The set $\mathcal{D}_4^-$ consists of polynomials $(X-\zeta)(X-\zeta^{-1})(X-\zeta^{-q})(X-\zeta^q)$ in $\mathbb{F}_{q^2}[X]$ such that the order of $\zeta$ is divisible by $(q^2-1)_2$. We now count the number of such polynomials. Observe that $\zeta, \zeta^{-1}, \zeta^{-q}, \zeta^q$ all have the same order and $\zeta \notin \{\zeta^{-1}, \zeta^{-q}, \zeta^q\}$. It follows that $|\{\zeta, \zeta^{-1}, \zeta^{-q}, \zeta^q\}| = 4$. The elements of $\mathbb{F}_{q^2}^*$ with order divisible by $(q^2-1)_2$ are precisely the nonsquares, and there are $(q^2-1)/2$ nonsquares. We take these nonsquares four at a time to make $\mathsf{U}*$-irreducible polynomials, and so $|\mathcal{D}_4^-| = (q^2-1)/8$.

Now consider $r = 2^{b-1} > 1$. By Lemma 4.8, there are $(q^{2r}-1)/(2r)$ degree $r$ monic irreducible polynomials $f(X)$ over $\mathbb{F}_{q^2}$ such that $\omega_2(f) = (q^{2r}-1)_2$. Part (i) implies that each such $f(X)$ corresponds to a $\mathsf{U}*$-irreducible polynomial $g(X)$ of type D, yielding exactly $(q^{2r}-1)/(8r)$ such $g(X)$. By Part (ii), each such $g(X)$ satisfies $\omega_2(g) = (q^{2r}-1)_2$, and hence 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 of $\mathsf{U}*$-irreducible, regular semisimple elements

In this section we investigate the centralisers and normalisers of cyclic subgroups of $\mathrm{GU}_n(q)$ whose generators are regular semisimple, $\mathsf{U}*$-irreducible, and conjugate in $\mathrm{GU}_n(q)$ to their inverse. We also count the number of involutions in $\mathrm{GU}_n(q)$ that invert these generators.

The field $\mathbb{F}_{q^{2m}}$ may be regarded as a vector space $\mathbb{F}_{q^2}^m$, and from this point of view the multiplicative group of $\mathbb{F}_{q^{2m}}$ is a subgroup of $\mathrm{GL}_m(q^2)$ acting regularly on the nonzero vectors. There is a single conjugacy class of such *Singer subgroups* of $\mathrm{GL}_m(q^2)$, and their generators are *Singer cycles*. Thus if $\langle z\rangle \cong C_{q^{2m}-1}$ is a Singer subgroup in $\mathrm{GL}_m(q^2)$ then we may identify $\mathbb{F}_{q^2}^m$ 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, $N_{\mathrm{GL}_m(q^2)}(\langle z\rangle) = \langle z, s\rangle \cong C_{q^{2m}-1} \rtimes C_m \cong \Gamma\mathrm{L}_1(\mathbb{F}_{q^{2m}}/\mathbb{F}_{q^2})$, with $s\colon z \mapsto z^{q^2}$ corresponding to the field automorphism $\phi\colon \zeta \mapsto \zeta^{q^2}$ 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, and work with matrices written relative to a decomposition

$$V = W_0 \oplus W_0^{\sim} \quad \text{where } W_0 \text{ and } W_0^{\sim} \text{ are totally isotropic subspaces.}$$

Choose an ordered basis $(v_1, \ldots, v_{2m})$ for $V$ such that $W_0 := \langle v_1, \ldots, v_m\rangle$ and $W_0^{\sim} := \langle v_{m+1}, \ldots, v_{2m}\rangle$. In this subsection our unitary form has Gram matrix

$$J = \begin{pmatrix} 0 & I_m \\ I_m & 0 \end{pmatrix}, \tag{5}$$

where $I_m$ is the identity matrix. We denote this unitary group by $\mathrm{GU}(J) \cong \mathrm{GU}_{2m}(q)$. Consider the monomorphism

$$\alpha\colon \mathrm{GL}_m(q^2) \to \mathrm{GL}_{2m}(q^2) \quad \text{defined by} \quad a \mapsto \begin{pmatrix} a & 0 \\ 0 & a^{-\sigma T} \end{pmatrix}. \tag{6}$$

To see that $\alpha(a) \in \mathrm{GU}(J)$, it is straightforward to check that $\alpha(a)J\alpha(a^{\sigma T}) = J$, or equivalently $\alpha(a)^J = \alpha(a^{-\sigma T})$. Thus the automorphism $a \mapsto a^{-\sigma T}$ of $\mathrm{GL}_m(q^2)$ induces the automorphism $\alpha(a) \mapsto \alpha(a)^J$ on the image of $\alpha$.

**5.2. Types A and B: $|\{f, f^\sigma, f^*, f^\sim\}| = 2$, with $f \neq f^\sim$.** To assist with our analysis of Types A and B of Proposition 4.3, we first consider the more general situation where $y \in \mathrm{GU}_{2m}(q)$ is regular semisimple 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 $V = W \oplus W^\sim = \mathbb{F}_{q^2}^m \oplus \mathbb{F}_{q^2}^m$ 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 [**11**, Definition 2.2 and 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 $a \in \mathrm{GL}_m(q)$. Then $a$ is conjugate in $\mathrm{GL}_m(q)$ to its transpose. In fact, by a result of Voss [**15**] (see also [**6**, Theorem 66]), there is a symmetric matrix $c \in \mathrm{GL}_m(q)$ which conjugates $a$ to its transpose, that is $c = c^T$ and $c^{-1}ac = a^T$.

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

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 $z \in \mathrm{GL}_m(q^2)$ be a Singer cycle for $\mathrm{GL}_m(q^2)$, and let $s \in N_{\mathrm{GL}_m(q^2)}(\langle z \rangle)$ be such that $z^s = z^{q^2}$.*

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

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

$$Z^B = Z^{-q} \quad \text{and } B^2 = \alpha(b^{1-\sigma T}) = \alpha(z^\ell s) \text{ for some } \ell \in \mathbb{Z}.$$

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

Proof. (i) The fact that $H \leqslant \mathrm{GU}(J)$ follows from our remark after (6). The spaces $W_0$ and $W_0^\sim$ are non-isomorphic irreducible $\mathbb{F}_{q^2}H$-submodules of $V$. Define $\widehat{H}$ to be the stabiliser in $\mathrm{GU}(J)$ of both $W_0$ and $W_0^\sim$. We shall show that $\widehat{H} = H$. The restriction $\widehat{H}|_{W_0} = H|_{W_0} \cong \mathrm{GL}_m(q^2)$, and the subgroup $K$ of $\widehat{H}$ fixing $W_0$ pointwise must fix the hyperplane $\langle w \rangle^\perp \cap W_0^\sim$ of $W_0^\sim$ for each non-zero $w \in W_0$. Thus $K$ induces a subgroup of scalar matrices on $W_0^\sim$. However $\left(\begin{smallmatrix} I & 0 \\ 0 & \lambda I \end{smallmatrix}\right) \in \mathrm{GU}(J)$ implies $\lambda = 1$, so $K$ is trivial. It follows that $\widehat{H} = H$. Finally each element of $\mathrm{Stab}_{\mathrm{GU}(J)}(W_0 \oplus W_0^{\sim})$ either fixes setwise, or interchanges, the subspaces $W_0$ and $W_0^{\sim}$, and it is straightforward to check that $J \in \mathrm{GU}(J)$, and that $J$ interchanges these two subspaces. Hence $\mathrm{Stab}_{\mathrm{GU}(J)}(W_0 \oplus W_0^{\sim}) = H \rtimes \langle J \rangle$.

(ii) The spaces $W_0$ and $W_0^{\sim}$ are also non-isomorphic irreducible $\mathbb{F}_{q^2}\langle Z \rangle$-modules, so that $C_{\mathrm{GU}_{2m}(q)}(Z)$ fixes each of $W_0, W_0^{\sim}$ setwise, and so is contained in their stabiliser $H$, by Part (i). Since $C_{\mathrm{GL}_m(q^2)}(z) = \langle z \rangle \cong C_{q^{2m}-1}$ (see [**5**, Satz II.7.3]), we have $C_{\mathrm{GU}_{2m}(q)}(Z) = \langle Z \rangle$. To prove the second assertion we note that $N$ must preserve the decomposition $V = W_0 \oplus W_0^{\sim}$, since $N$ normalises $\langle Z \rangle$. Thus $N \leqslant H \rtimes \langle J \rangle$, by Part (i). Also $N \cap H$ is the image under $\alpha$ of $N_{\mathrm{GL}_m(q^2)}(\langle z \rangle)$, 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 $B \in N \setminus (N \cap H)$.

Let $f(X) = c_z(X)$, and let $\zeta$ be a root of $f(X)$. Then the roots of $f(X)$ are $\zeta^{q^{2i}}$ for $0 \leqslant i \leqslant m-1$. Since $|z| = q^{2m} - 1$, the element $z^q$ is irreducible and one of the roots of $c_{z^q}(X)$ is $\zeta^q$. Similarly $z^{q\sigma}$ is irreducible and one of the roots of $c_{z^{q\sigma}}(X)$ is $(\zeta^q)^\sigma = \zeta^{q^2}$. Hence, by Remark 5.1, $z$ is conjugate in $\mathrm{GL}_m(q^2)$ to $z^{q\sigma}$ which in turn is conjugate to $z^{q\sigma T}$. Let $b \in \mathrm{GL}_m(q^2)$ be such that $b^{-1}zb = z^{q\sigma T}$, and let $B := \alpha(b)J$. Then, using the fact noted after (6) that $\alpha(a)^J = \alpha(a^{-\sigma T})$ for all $a$,

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

In particular, $B$ normalises $\langle Z \rangle$ and interchanges $W_0$ and $W_0^{\sim}$. Thus $N = \langle Z, \alpha(s), B \rangle$. A straightforward computation shows that $B^2$ and $\alpha(s)$ both conjugate $Z$ to $Z^{q^2}$, so $B^2\alpha(s)^{-1} \in C_{\mathrm{GU}(J)}(Z) = \langle Z \rangle$. Hence $N = \langle Z, B \rangle$, and $B^2 = \alpha(z^\ell s)$ 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 $\mathrm{GU}_{2m}(q)$, and hence to an element of $\mathrm{GU}(J)$, is immediate from Corollary 2.5. The primary decomposition of $V$ with respect to $y$, as discussed at the beginning of §5.2, is $V = W \oplus W^{\sim}$ where both $W$ and $W^{\sim}$ are totally isotropic, and the restrictions of $y$ to $W$ and $W^{\sim}$ are irreducible with characteristic polynomials $f(X)$ and $f^{\sim}(X)$, respectively. Since $\mathrm{GU}(J)$ 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 $W^{\sim} = W_0^{\sim}$.

Then $y$ fixes both $W_0$ and $W_0^{\sim}$ setwise, and hence $y = \alpha(y_0)$ for some $y_0 \in \mathrm{GL}_m(q^2)$, 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 exists $c \in \mathrm{GL}_m(q^2)$ such that $y_0^c \in \langle z \rangle$ and $N_{\mathrm{GL}_m(q^2)}(\langle y_0 \rangle)^c = N_{\mathrm{GL}_m(q^2)}(\langle z \rangle) = \langle z, s \rangle$. Thus, replacing $y$ by its conjugate $y^{\alpha(c)}$, we have $C_{\mathrm{GU}_{2m}(q)}(y) = C_{\mathrm{GU}_{2m}(q)}(Z) = \langle Z \rangle$ and $N_{\mathrm{GU}_{2m}(q)}(\langle y \rangle) \cap H = \langle Z, \alpha(s) \rangle$. Since $N_{\mathrm{GU}_{2m}(q)}(\langle y \rangle)$ normalises $C_{\mathrm{GU}_{2m}(q)}(y) = \langle Z \rangle$, it is contained in $N$, and since $B = \alpha(b)J$ normalises the cyclic group $\langle Z \rangle$, it also normalises $\langle y \rangle$. Thus $N_{\mathrm{GU}_{2m}(q)}(\langle y \rangle) = N$. $\square$

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

Corollary 5.3. *Let $y \in \mathrm{GL}_{2m}(q^2)$ be regular semisimple, with $\mathsf{U}*$-irreducible characteristic polynomial $g(X) = f(X)f^{\sim}(X)$, where $f(X)$ is irreducible and $f(X) \neq f^{\sim}(X)$.*

*Then up to conjugacy* $y \in \mathrm{GU}_{2m}(q)$*, and some element of* $\mathrm{GU}_{2m}(q)$ *inverts this conjugate of* $y$ *if and only if one of the following holds.*

(i) $f(X)$ *is of Type A and exactly* $q^m+1$ *involutions invert* $y$.
(ii) $f(X)$ *is of Type B and exactly* $q^m-1$ *involutions invert* $y$.

Proof. Note that $f(X) \neq X \pm 1$ since $f(X) \neq f^{\sim}(X)$, 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(iii), 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 every element of $\mathrm{GU}_{2m}(q)$ that inverts $y$, if one exists, must lie in $N$. If both $n$ and $n'$ invert $y$, then $n'n^{-1}$ centralises $y$ and hence, by Lemma 5.2(iii), $n' = \alpha(z^i)n$, for some $i$. Moreover, if $n$ inverts $y$ then certainly $\alpha(z^i)n$ 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 types, and then we count the number of them which are involutions.

It follows from Lemma 5.2(ii) that if an element $n$ of $\mathrm{GU}_{2m}(q)$ inverts $y$, then $n$ is of the form $\alpha(z^j)B^k \in N$ for some $j, k$ such that $0 \leqslant j \leqslant q^{2m}-2$ and $1 \leqslant k \leqslant 2m-1$. 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 $y^B = y^{-q}$.

Suppose first that $k$ is even. Then

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

and so $z^{iq^k} = z^{-i}$, which is equivalent to $z^{i(q^k+1)} = 1$. This implies that $z^i \in \mathbb{F}_{q^{2k}} \cap \mathbb{F}_{q^{2m}} = \mathbb{F}_{q^{2(k,m)}}$ (identifying $z$ with an element of $\mathbb{F}_{q^{2m}}$). However, $z^i$ acts irreducibly on $\mathbb{F}_{q^2}^m$, so $z^i$ lies in no proper subfield of $\mathbb{F}_{q^{2m}}$ that contains $\mathbb{F}_{q^2}$. Hence $k = m$, and in particular $m$ is even (since $k$ is assumed to be even), and we are in Type 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

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

and so $z^{i(q^k-1)} = 1$, whence $z^i \in \mathbb{F}_{q^k} \cap \mathbb{F}_{q^{2m}} = \mathbb{F}_{q^{(k,m)}} \subset \mathbb{F}_{q^{2(k,m)}}$ since $k$ is odd. As in the previous case, $z^i$ lies in no proper subfield of $\mathbb{F}_{q^{2m}}$ containing $\mathbb{F}_{q^2}$. Hence $(k, m) = m$, so again $k = m$. Thus $m$ is odd (since $k$ is odd), and we are in Type 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. Observe that, by Lemma 5.2(ii), $B^2 = \alpha(z^\ell s)$ for some $\ell \in \{0, \ldots, q^{2m}-2\}$, where $s^{-1}zs = z^{q^2}$, with $z^{q^{2m}-1} = 1$ and $s^m = 1$. Hence

$$B^{2m} = \alpha(z^\ell s)^m = \alpha((z^\ell s)^{m-1} s z^{\ell q^2}) = \cdots = \alpha(z^{\ell(q^{2m}-1)/(q^2-1)}). \tag{7}$$

*Type 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

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

Hence, by (7), $n^2 = 1$ if and only if $q^{2m}-1$ divides $j(q^m+1) + \ell(q^{2m}-1)/(q^2-1)$. Since $m$ is even, this holds if and only if $q^m-1$ divides $j + \ell(q^m-1)/(q^2-1)$. In particular $j = j'(q^m-1)/(q^2-1)$ (there are $(q^m+1)(q^2-1)$ integers $j$ with this property in $\{1,\dots,q^{2m}-2\}$), 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 $y$.

*Type B:* Each inverting element is of the form $n=\alpha(z^j)B^m$, for some $j\in\{0,\dots,q^{2m}-2\}$, 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 (7), $n^2=1$ if and only if $q^{2m}-1$ divides $-j(q^m-1)+\ell(q^{2m}-1)/(q^2-1)$. In particular, $q^m-1$ must divide $\ell(q^{2m}-1)/(q^2-1)$, or equivalently, $\ell(q^m+1)/(q^2-1)$ must be an integer. Given this condition, $n^2=1$ if and only if $q^m+1$ divides $-j+\ell(q^m+1)/(q^2-1)$. As $j$ runs through $\{0,\dots,q^{2m}-2\}$, 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 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 $\mathrm{GL}_m(q^2)$ lies in $\mathrm{GL}_m(q)$ (the subgroup of $\mathrm{GL}_m(q^2)$ of matrices with entries in $\mathbb{F}_q$). We may therefore conjugate $y=\alpha(z^i)$ by an element of $\alpha(\mathrm{GL}_m(q^2))\subseteq\mathrm{GU}_{2m}(q)$ (see (6)) and obtain an element in $\alpha(\mathrm{GL}_m(q))$. Let us replace $y$ by this element so that $y=\alpha(z^i)$ with $z^i\in\mathrm{GL}_m(q)$. By Remark 5.1, there is a symmetric matrix $c\in\mathrm{GL}_m(q)$ which conjugates $z^i$ to its transpose, that is, $c=c^T$ and $c^{-1}z^ic=(z^i)^T$. Note that $(z^i)^T=(z^i)^{\sigma T}$ and $c^{\sigma T}=c$, since $z^i,c\in\mathrm{GL}_m(q)$ and $c=c^T$. Therefore $c^{\sigma T}(z^i)^{-\sigma T}c^{-\sigma T}=(c^{-1}z^{-i}c)^T=z^{-i}$, and it follows from (6) that $\alpha(c)^{-1}y\alpha(c)$ is the block diagonal matrix $\alpha(z^{iT})$ with diagonal components $z^{iT},z^{-i}$. 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. Type C: $|\{f,f^\sigma,f^*,f^\sim\}|=2$, $f=f^\sim$.** We now consider regular semisimple $y\in\mathrm{GU}_{2m}(q)$ with $\mathsf{U}*$-irreducible characteristic polynomial $c_y(X)=f(X)f^*(X)$, where $f(X)=f^\sim(X)$ has degree $m$. So $y$ is in Type C of Proposition 4.3, and in particular $m$ is odd. The primary decomposition of $V$ as an $\mathbb{F}_{q^2}\langle y\rangle$-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. Reasoning in exactly the same way as in the proof of [**11**, Lemma 2.4], we see that $U^*\leqslant U^\perp$. Since $\dim U^*=m=\dim U$, we deduce that $U^*=U^\perp$, and so both $U$ and $U^*$ are nondegenerate.

For the analysis in this subsection it is convenient to work with matrices with respect to an ordered basis $(v_1,\dots,v_{2m})$ where $U=\langle v_1,\dots,v_m\rangle$ and $U^*=\langle v_{m+1},\dots,v_{2m}\rangle$, and with Gram matrix $J=I_{2m}$, where $I_{2m}$ denotes the identity matrix. The stabiliser in $\mathrm{GU}_{2m}(q)$ of the subspace $U$ (and hence also of $U^*=U^\perp$) is $H:=\mathrm{Stab}_{\mathrm{GU}_{2m}(q)}(U)=\mathrm{GU}(U)\times\mathrm{GU}(U^*)\cong\mathrm{GU}_m(q)\times\mathrm{GU}_m(q)$. It is convenient to write elements of $H$ as pairs $(h,h')$ with $h,h'\in\mathrm{GU}_m(q)$. The stabiliser in $\mathrm{GU}_{2m}(q)$ of the decomposition $V=U\perp U^*$ is $\widehat{H}:=H\cdot\langle\tau\rangle$, where $\tau\colon(h,h')\mapsto(h',h)$ for $(h,h')\in H$.

By [**5**, 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 $\mathrm{GU}_m(q)$, and moreover, such that $y_2$ is equal to $y_1^{-1}$.

LEMMA 5.4. *Let $y \in \mathrm{GL}_{2m}(q^2)$ be regular semisimple, with $c_y(X)$ a $\mathsf{U}*$-irreducible polynomial in Type C. Then up to conjugacy, $y \in \mathrm{GU}_{2m}(q)$, $m$ is odd, and with the notation from the previous two paragraphs*

(i) $N_{\mathrm{GU}_{2m}(q)}(\langle z\rangle \times \langle z\rangle) = \langle z, \phi\rangle \wr \langle \tau\rangle \cong \Gamma\mathrm{U}_1(q^m) \wr C_2$ *where* $\phi\colon z^i \mapsto z^{iq^2}$;
(ii) $y \in C_{\mathrm{GU}_{2m}(q)}(\langle y\rangle) \leqslant H$, *and* $C_{\mathrm{GU}_{2m}(q)}(\langle y\rangle) = \langle z\rangle \times \langle z\rangle \cong C^2_{q^m+1}$;
(iii) $y$ *is inverted by precisely* $q^m + 1$ *involutions in* $\mathrm{GU}_{2m}(q)$.

PROOF. First note that by Corollary 2.5, up to conjugacy $y \in \mathrm{GU}_{2m}(q)$, 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 $\mathbb{F}_{q^2}C$-submodules are $U$ and $U^*$, and so $C \leqslant H$ and $N_{\mathrm{GU}_{2m}(q)}(C) \leqslant \widehat{H}$. Now the normaliser of $\langle z\rangle$ in $\mathrm{GU}_m(q)$ is $N_1 := \langle z, \phi\rangle$, and so $N_{\mathrm{GU}_{2m}(q)}(C) = N_1 \wr C_2$.

(ii) As observed above, $U$ and $U^*$ are non-isomorphic irreducible $\mathbb{F}_{q^2}\langle y\rangle$-submodules, and we may assume that $y = (y_1, y_1^{-1})$. Hence $C_{\mathrm{GU}_{2m}(q)}(\langle y\rangle) \leqslant H$. Moreover, since $y_1$ is irreducible on $U$, its centraliser in $\mathrm{GU}_m(q)$ is $\langle z\rangle$, and hence $C_{\mathrm{GU}_{2m}(q)}(\langle y\rangle) = C$.

(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 $y$. □

**5.4. Type D: $|\{f, f^\sigma, f^*, f^\sim\}| = 4$.** We now consider regular semisimple $y \in \mathrm{GU}_{4m}(q)$ with $\mathsf{U}*$-irreducible characteristic polynomial

$$c_y(X) = f(X)f^\sim(X)f^*(X)f^\sigma(X),$$

where $f(X)$ has degree $m$, so that $y$ is in Type D of Proposition 4.3. The primary decomposition of $V$ as an $\mathbb{F}_{q^2}\langle y\rangle$-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 $\mathbb{F}_{q^2}\langle y\rangle$-submodules, and so the centraliser $C := C_{\mathrm{GU}_{4m}(q)}(y)$ lies in the stabiliser $H$ in $\mathrm{GU}_{4m}(q)$ of all four submodules $U$, $U^\sim$, $U^*$ and $U^\sigma$.

Let $W := U \oplus U^\sim$ and $W^* := U^* \oplus U^\sigma$. Then the characteristic polynomials of $y|_W$ and $y|_{W^*}$, namely $g(X) := f(X)f^\sim(X)$ and $g^*(X) = g^\sigma(X) = f^*(X)f^\sigma(X)$, are both $\sim$-invariant. Thus both $W$ and $W^*$ are non-degenerate, and $V = W \perp W^*$. Moreover on considering $y|_W$, $y|_{W^*}$ as in §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 $U = \langle v_1, \ldots, v_m\rangle$, $U^\sim = \langle v_{m+1}, \ldots, v_{2m}\rangle$, $U^* = \langle v_{2m+1}, \ldots, v_{3m}\rangle$, and $U^\sigma = \langle v_{3m+1}, \ldots, v_{4m}\rangle$, and with the Gram matrix

$$J = \begin{pmatrix} 0 & I_m & 0 & 0 \\ I_m & 0 & 0 & 0 \\ 0 & 0 & 0 & I_m \\ 0 & 0 & I_m & 0 \end{pmatrix},$$

where $I_m$ denotes the identity matrix. Then, by Lemma 5.2, the subgroup of $\mathrm{GU}(J)$ leaving each of $U, U^{\sim}, U^*$ and $U^\sigma$ invariant is

$$H = \left\{ \begin{pmatrix} \alpha(a) & 0 \\ 0 & \alpha(b) \end{pmatrix} \mid a, b \in \mathrm{GL}_m(q^2) \right\}$$

where the matrices $\alpha(a), \alpha(b) \in \mathrm{GU}_{2m}(q)$ are as defined in (6). We note that $\mathrm{GU}(J)$ contains

$$\tau := \begin{pmatrix} 0 & I_{2m} \\ I_{2m} & 0 \end{pmatrix},$$

which interchanges the subspaces $W$ and $W^*$ and normalises $H$. We often write elements of $H$ as pairs $(\alpha(a), \alpha(b))$ with $a, b \in \mathrm{GL}_m(q^2)$. Since $y_1 := y|_U \in \mathrm{GL}_m(q^2)$ is irreducible, it is contained in a Singer subgroup $\langle z \rangle$ of $\mathrm{GL}_m(q^2)$, and it follows from Lemma 5.2 that $y|_W = \alpha(y_1)$ and $C_{\mathrm{GU}(W)}(y|_W) = \langle Z \rangle$, where $Z := \alpha(z)$. Also, since $y|_{U^*}$, $y|_{U^\sigma}$ 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 $y \in \mathrm{GL}_{4m}(q^2)$ be regular semisimple, with $c_y(X)$ a $\mathsf{U}*$-irreducible polynomial in Type D. Then, up to conjugacy, and with the previous notation, the following hold:*

(i) *$y = (\alpha(y_1), \alpha(y_1^{-1})) \in \mathrm{GU}_{4m}(q)$, where $y_1 \in \mathrm{GL}_m(q^2)$, with characteristic polynomial $f(X)$, $y_1$ is contained in a Singer subgroup $\langle z \rangle$, and $C := C_{\mathrm{GU}_{4m}(q)}(y) = \langle Z \rangle \times \langle Z \rangle \cong C^2_{q^{2m}-1}$, where $Z = \alpha(z)$;*
(ii) *$N_{\mathrm{GU}_{4m}(q)}(C) = N \wr C_2 = \langle Z, B \rangle \wr \langle \tau \rangle$, with $N, B$, as in Lemma 5.2;*
(iii) *$y$ is inverted by precisely $q^{2m} - 1$ involutions in $\mathrm{GU}_{4m}(q)$*
(iv) *The integer $m$ can be even or odd. Let $m = 2^{b-1}r$ with $b \geqslant 1$ and $r$ odd. Then $|y|_2 \leqslant 2^{b-1}(q^2-1)_2$, and equality can be attained in this bound.*

Proof. (i) The assertions about $y$ follow from Corollary 2.5, 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 $N_{\mathrm{GU}(W)}(\langle y|_W \rangle)) = N = \langle Z, B \rangle$, as in Lemma 5.2, and $N_{\mathrm{GU}_{4m}(q)}(C)$ is therefore equal to $N \wr \langle \tau \rangle$.

(iii) The element $\tau$ is an involution which inverts $y = (y_1, y_1^{-1})$, and hence, if $x \in \mathrm{GU}(V)$ 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 $(q^{2m} - 1)_2 = (q^{2^b r} - 1)_2 = 2^{b-1}(q^2 - 1)_2$. 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 $f(X) = c_{y_1}(X)$ are of the form $\{\zeta, \zeta^{q^2}, \ldots, \zeta^{q^{2m-2}}\}$, 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 $\mathsf{U}*$-irreducible, we now consider the general case. We remind the reader that we assume throughout this paper that $q$ is an odd prime power.

Let $y$ be a regular semisimple element of $G = \mathrm{GU}_n(q)$, 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 $g(X) = g_0(X)(X-1)^{\delta_-}(X+1)^{\delta_+}$ where $\delta_-, \delta_+ \in \{0,1\}$ 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 $\mathsf{U}*$-irreducible polynomial $g(X)$ in Type A. Similarly, we define $\mathcal{B}, \mathcal{C}, \mathcal{D} \subset \mathbb{F}_{q^2}[X]$ to contain one irreducible factor of each $\mathsf{U}*$-irreducible polynomial from Types B, C and D, respectively. For a $\mathsf{U}*$-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

$$\left(\prod_{f\in\mathcal{A}_g} f(X)f^\sigma(X)\right)\left(\prod_{f\in\mathcal{B}_g} f(X)f^*(X)\right)\left(\prod_{f\in\mathcal{C}_g} f(X)f^*(X)\right)\left(\prod_{f\in\mathcal{D}_g} f(X)f^\sim(X)f^*(X)f^\sigma(X)\right). \tag{8}$$

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

$$V = \bigoplus_{f\in\mathcal{A}_g} V_f \oplus \bigoplus_{f\in\mathcal{B}_g} V_f \oplus \bigoplus_{f\in\mathcal{C}_g} V_f \oplus \bigoplus_{f\in\mathcal{D}_g} V_f \oplus V_\pm. \tag{9}$$

such that

(A) for each $f \in \mathcal{A}_g$, the restriction $y_f = y|_{V_f} \in \mathrm{GU}(V_f)$ has characteristic polynomial $f(X)f^\sigma(X)$, with $f(X) = f^*(X) \neq f^\sigma(X) = f^\sim(X)$;
(B) for each $f \in \mathcal{B}_g$, the restriction $y_f = y|_{V_f} \in \mathrm{GU}(V_f)$ has characteristic polynomial $f(X)f^*(X)$, with $f(X) = f^\sigma(X) \neq f^*(X) = f^\sim(X)$;
(C) for each $f \in \mathcal{C}_g$, the restriction $y_f = y|_{V_f} \in \mathrm{GU}(V_f)$ has characteristic polynomial $f(X)f^*(X)$, with $f(X) = f^\sim(X) \neq f^*(X) = f^\sigma(X)$;
(D) for each $f \in \mathcal{D}_g$, the restriction $y_f = y|_{V_f} \in \mathrm{GU}(V_f)$ has characteristic polynomial $f(X)f^*(X)f^\sigma(X)f^\sim(X)$, 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 $y|_{V_+}$, $y|_{V_-}$, $y|_{V_\pm}$ has characteristic polynomial $X-1$, $X+1$, $X^2-1$, respectively.

LEMMA 6.2. *Let $y \in \mathrm{GU}_n(q) = \mathrm{GU}(V)$, where $y$ is regular semisimple and conjugate in $\mathrm{GU}_n(q)$ 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 (8).*

(i) *Each non-zero summand in (9) is a non-degenerate unitary space, and distinct summands are pairwise orthogonal.*

(ii) *The centraliser $C_{\mathrm{GU}(V)}(y)$ has order*

$$\left(\prod_{f\in\mathcal{A}_g\cup\mathcal{B}_g}(q^{2\deg f}-1)\right)\left(\prod_{f\in\mathcal{C}_g}(q^{\deg f}+1)^2\right)\left(\prod_{f\in\mathcal{D}_g}(q^{2\deg f}-1)^2\right)(q+1)^{\delta_++\delta_-}.$$

(iii) *The number of involutions in $\mathcal{C}_{\mathsf{U}}(V)$ (see Definition 1.4) that invert $y$ is equal to*

$$\left(\prod_{f\in\mathcal{A}_g}(q^{\deg f}+1)\right)\left(\prod_{f\in\mathcal{B}_g}(q^{\deg f}-1)\right)\left(\prod_{f\in\mathcal{C}_g}(q^{\deg f}+1)\right)\left(\prod_{f\in\mathcal{D}_g}(q^{2\deg f}-1)\right)\varepsilon(y),$$

*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 $(t, y') \in \Delta_{\mathsf{U}}(V)$ (as defined in (4)) such that $y'$ has characteristic polynomial $g(X)$ is*

$$\frac{|\mathrm{GU}_{2m}(q)|}{\left(\prod_{f\in\mathcal{A}_g}(q^{\deg f}-1)\right)\left(\prod_{f\in\mathcal{B}_g}(q^{\deg f}+1)\right)\left(\prod_{f\in\mathcal{C}_g}(q^{\deg f}+1)\right)\left(\prod_{f\in\mathcal{D}_g}(q^{2\deg f}-1)\right)}.$$

PROOF. (i) Each space in the primary decomposition of $V$ as an $\mathbb{F}_{q^2}\langle y\rangle$ module is either non-degenerate or totally singular. It follows from §5 that the spaces corresponding to a $\mathsf{U}*$-irreducible summand always span a non-degenerate space. Let $U, W$ be distinct such summands, corresponding to $\mathsf{U}*$-irreducible polynomials $h(X)$, $h'(X)$ respectively. Let $h(X) = \sum_{i=0}^r a_iX^i \in \mathbb{F}_{q^2}[X]$, so that $a_r = 1$. Then $h, h'$ are coprime, and so $uh(y) = \sum_{i=0}^r a_iuy^i = 0$, for each $u \in U$, while $h(y)|_W$ is a bijection. Denote by $(u, w)$ the value of the unitary form on $u \in U, w \in W$. Then

$$0 = (uh(y), w) = \sum_{i=0}^r a_i(uy^i, w) = \sum_{i=0}^r a_i(u, wy^{-i}) = (u, \sum_{i=0}^r a_i^q wy^{-i}) = (u, wh^\sim(y)y^{-r}).$$

Since $h$ is $\mathsf{U}*$-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 $|\mathrm{GU}_n(q)|/|C_{\mathrm{GU}_n(q)}(y)|$ of conjugates of $y$ times the number of $t \in \mathcal{C}_{\mathsf{U}}(V)$ inverting $y$. By Lemma 2.6(i) if $g(X) = g_0(X)$ then all involutions inverting $y$ lie in $\mathcal{C}(V)$, since $n$ is even. Thus all involutions in $\mathrm{GU}_n(q)$ that invert $y$ lie in $\mathcal{C}_{\mathsf{U}}(V)$, and hence Part (iv) follows from Parts (ii) and (iii). □

## 7. Formulae for the number of $\mathsf{U}*$-irreducible polynomials in each Type

Recall the division of $\mathsf{U}*$-irreducible polynomials into Types A to E from Proposition 4.3. We count the number of polynomials with irreducible factors of degree $r$ in each type.

First we present some standard counts of polynomials. Let $\mathrm{Irr}(r, \mathbb{F}_q)$ denote the set of monic irreducible polynomials in $\mathbb{F}_q[X]$ of degree $r$. By Definition 4.7, $N(q,r) = |\mathrm{Irr}(r, \mathbb{F}_q)|$ 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. We define the following quantities as in [**4**, pp. 23–26]:

$$N^{\sim}(q,r) = \text{number of } f \in \mathrm{Irr}(r, \mathbb{F}_{q^2}) \text{ with } f^{\sim} = f \text{ (over } \mathbb{F}_{q^2} \text{ not } \mathbb{F}_q).$$
$$N^{*}(q,r) = \text{number of } f \in \mathrm{Irr}(r, \mathbb{F}_q) \text{ with } f^* = f.$$
$$M^{*}(q,r) = \text{number of subsets } \{f, f^*\} \text{ with } f \in \mathrm{Irr}(r, \mathbb{F}_q) \text{ and } f^* \neq f.$$

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

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

The following formulae can be found in [**4**, Lemmas 1.3.10(a), 12(a), 16(a) and (b)].

THEOREM 7.1. *Let $r \geqslant 1$ and let $q$ be an odd prime power. Then*

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

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

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

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

We now prove some bounds on these quantities.

LEMMA 7.2. *Set $\xi = q/(q-1)$, and let $r \geqslant 1$. If $r \geqslant 2$ then let $p_1 < p_2 < \cdots < p_t$ be the prime divisors of $r$.*

(i) $q^r - 2q^{r/2} < q^r - \xi q^{r/p_1} < rN(q,r) \leqslant q^r - 1$, *and* $N(q,r) > 0.956(q^r-1)/r$ *for* $r \geqslant 5$.
(ii) $N(q, r+1) > N(q,r)$.

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

$$|\delta| < \sum_{d|r,\, d>p_1} q^{r/d} < q^{r/p_1} \sum_{i=1}^{\infty} q^{-i} = q^{r/p_1} \left( \frac{1}{1-\frac{1}{q}} - 1 \right) = q^{r/p_1}(\xi - 1).$$

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

(iii) Let $r = 2^b k$ where $b \geqslant 1$ and $k > 1$ is odd. Then from Theorem 7.1 we get

$$rN^*(q,r) = \sum_{d|k,\, d \text{ odd}} \mu(d) q^{r/(2d)} - \sum_{d|k,\, d \text{ odd}} \mu(d) = \sum_{d|k} \mu(d) q^{r/(2d)},$$

since $k > 1$ implies that $\sum_{d|k} \mu(d) = 0$. If $t = 2$, then the result now follows, so assume that $t \geqslant 3$. Then similarly to the proof of Part (i)

$$q^{r/2} - q^{r/(2p_2)} - q^{r/(2p_3)} \left( 1 + \sum_{i=1}^{\infty} q^{-i} \right) < rN^*(q,r) < q^{r/2} - q^{r/(2p_2)} - q^{r/(2p_3)} \left( 1 - \sum_{i=1}^{\infty} q^{-i} \right).$$

Thus writing $\xi = q/(q-1)$ gives

$$q^{r/2} - q^{r/(2p_2)} - \xi q^{r/(2p_3)} < rN^*(q,r) < q^{r/2} - q^{r/(2p_2)} - (2-\xi) q^{r/(2p_3)}. \tag{10}$$ □

Lemma 7.3. *Let $r$ be a positive integer. Then*

$$\frac{1}{2}\left( N^*(q^2, 2r) + M^*(q^2, r) - N^{\sim}(q,r) \right) = \begin{cases} N(q,2r) - 3/2 & \text{if } r = 1, \\ N(q,2r) & \text{if } r > 1. \end{cases}$$

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 $N^{\sim}(q,1) = q+1$ and $N(q,2) = (q^2-q)/2$, 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 $(N(q^2,r) - N^{\sim}(q,r))/2 = N(q,2r)$ (note this also holds for $r$ even since in that case $N^{\sim}(q,r) = 0$). □

Definition 7.4. We define $A(q,r)$ to be the number of $\mathsf{U}*$-irreducible polynomials in Type 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 $\mathsf{U}*$-irreducible polynomials in Types B and C of degree $2r$, and $D(q,r)$ to be the number of $\mathsf{U}*$-irreducible polynomials in Type D of degree $4r$. Recall Definition 4.9: it is immediate that $|\mathcal{D}_{4r}| = D(q,r)$.

LEMMA 7.5. *Let $r \geqslant 1$. 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 type, the equivalence of the two statements for $r = 1$ follows immediately from Theorem 7.1. In each of the following types, we first count the number of polynomials $f \in \mathrm{Irr}(r, \mathbb{F}_{q^2})$ satisfying the type conditions, and then deduce the number of $\mathsf{U}*$-irreducible polynomials of the relevant degree.

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

TYPE B. By Proposition 4.3, in this type $f = f^\sigma \neq f^*$, and if $f$ exists then $r$ is odd. Thus if $r$ is even then $B(q,r) = 0 = N^\sim(q,r)/2$. 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 $\zeta \notin \{0, \pm 1\}$. Moreover, since $f = f^\sigma$, we have $\zeta = \zeta^\sigma$ 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 $\{f, f^*\}$ is $B(q,1) = (q-3)/2$. Suppose now that $r > 1$ and $r$ is odd. Then $f \neq f^*$ by Lemma 4.1, and hence in this case $B(q,r)$ is the number of pairs $\{f, f^*\} \subset \mathrm{Irr}(r, \mathbb{F}_{q^2})$ satisfying $f = f^\sigma$, namely $B(q,r) = N(q,r)/2 = N^\sim(q,r)/2$.

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

TYPE D. In this type the irreducible polynomials $f, f^\sigma, f^*, f^\sim$ 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 $\{f, f^*\} \subset \mathrm{Irr}(r, \mathbb{F}_{q^2})$ satisfying $f \neq f^*$ is, by definition, $M^*(q^2,r)$. We enumerate these pairs by a different argument. We showed under 'Type B' and 'Type 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 $\{f, f^\sigma, f^*, f^\sim\}$ 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. *The following identities hold.*

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

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

Lemma 7.7. (i) *If $r = 2^b$ for $b \geqslant 0$ then $D(q,r) = (q^r-1)^2/(4r)$.*
(ii) *If $r=3$, then $4rD(q,r) = q^6-2q^3-q^2+2q < q^{2r}-q^r+\frac{q+1}{q}q^{r/3}$. For all other $r$,*

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

(iii) *$4rD(q,r) = (q^{2r}-1)-\eta(q,r)(q^r-1)$, where $0 < 1-2q^{-2r/3} < \eta(q,r) < 2.2$.*

Proof. If $r>1$, then let the prime divisors of $r$ be $p_1 < p_2 < \ldots < p_t$.
(i) The result for $r=1$ is immediate from Lemma 7.5. Otherwise, by Corollary 7.6, $D(q,r) = (N(q^2,r)-N^*(q^2,r))/4$. Then using Theorem 7.1 and the fact that $r = 2^b > 1$, we deduce that

$$D(q,r) = \frac{1}{4}\left(\frac{q^{2r}-q^r}{r} - \frac{q^r-1}{r}\right) = \frac{(q^r-1)^2}{4r},$$

as required.

(ii) By Part (i) we may assume that $r$ is not a 2-power, and in particular that $r \geqslant 3$. Before commencing the main part of the proof, notice first that if $q^{2r}-q^r+\frac{q+1}{q}q^{r/3} \geqslant q^{2r}-1$ then $q^r-1 \leqslant \frac{q+1}{q}q^{r/3} < 2q^{r/3}$, so $(q^r-1)^3 < 8q^r$, which is impossible, since $q \geqslant 3$ and $r \geqslant 3$. 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, $D(q,r) = (N(q^2,r)-N^*(q^2,r))/4$. We deduce from Lemma 7.2(i)(iii) that

$$\begin{aligned} 4rD(q,r) &> (q^{2r}-q^2(q^2-1)^{-1}q^r) - (q^r - q^{r/p_2}) \\ &> q^{2r}-(2q^2-1)(q^2-1)^{-1}q^r = q^{2r}-2q^r-\frac{1}{q^2-1}q^r, \end{aligned}$$

and (using the fact that $r/p_3 \leqslant r/p_2 - 2$ if $p_3$ exists)

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

Suppose now that $r > 1$ is odd, so that $D(q,r) = N(q^2,r)/4 - N(q,r)/2$, by Corollary 7.6. If $r$ is an odd prime then $rN(q^\varepsilon,r) = q^{\varepsilon r} - q^\varepsilon$ and so $4rD(q,r) = (q^{2r}-q^2) - 2(q^r-q) = q^{2r} - 2q^r - q^2 + 2q$. This is less than the required upper bound for all odd primes $r$, 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 $r \geqslant 9$), 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 $r$,

$$-1 - \eta(q^r-1) \leqslant -q^r + \frac{q+1}{q}q^{r/3}, \quad \text{or equivalently,} \quad \eta \geqslant 1 - \frac{q+1}{q} \cdot \frac{q^{r/3}}{q^r-1}.$$

We must show that

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

For all $r \geqslant 3$ and $q \geqslant 3$, 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 $((q+1)/q) \cdot q^r/(q^r-1) < 2$, from which the claimed lower bound on $\eta$ follows.

For $r$ an odd prime

$$4rD(q,r) = q^{2r} - 2q^r - q^2 + 2q = q^{2r} - 1 - (2q^r + q^2 - 2q - 1)$$

which gives $\eta(q,r) = 2 + (q-1)^2/(q^r-1)$ so $2 < \eta(q,r) \leqslant 2 + 2/13 < 2.2$. Otherwise, Part (ii) yields

$$\eta(q^r-1) = q^{2r} - 1 - 4rD(q,r) \leqslant -1 + 2q^r + \frac{1}{q^2-1}q^r = 2(q^r-1) + \frac{q^r - 1 + q^2}{q^2-1}$$

so using $r > 2$ and $q \geqslant 3$ gives

$$\eta \leqslant 2 + \frac{1}{q^2-1} + \frac{q^2}{(q^r-1)(q^2-1)} = 2 + \frac{1}{q^2-1} + \frac{1}{q^r-1} + \frac{1}{(q^r-1)(q^2-1)}$$
$$< 2.1683.$$

□

LEMMA 7.8. *Let $q \geqslant 5$ and $r \geqslant 1$. Then*

(i) $\dfrac{D(q,r)}{q^{2r}-1} \geqslant \dfrac{D(3,r)}{3^{2r}-1}$; (ii) $\dfrac{N^*(q^2,r)}{q^r-1} \geqslant \dfrac{N^*(3^2,r)}{3^r-1}$ *for $r > 1$;* (iii) $\dfrac{N^\sim(q,r)}{q^r+1} \geqslant \dfrac{N^\sim(3,r)}{3^r+1}$.

PROOF. (i) Suppose $r = 2^b$ is a power of 2. Then Lemma 7.7(i) implies that

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

This is an increasing function of $q$. Hence Part (i) holds for such $r$. A straightforward calculation shows the result when $r = 3$, so assume that $r \geqslant 5$. Using Lemma 7.7(ii),

$$4r\frac{D(q,r)}{q^{2r}-1} \geqslant \frac{q^{2r}-2q^r-\frac{1}{q^2-1}q^r}{q^{2r}-1} = 1-\frac{2q^r+\frac{1}{q^2-1}q^r-1}{q^{2r}-1} \geqslant 1-\frac{\frac{49}{24}q^r}{q^{2r}-1} \geqslant 1-\frac{9q^r}{4(q^{2r}-1)}.$$

Using Lemma 7.7(ii) again gives

$$4r\frac{D(3,r)}{3^{2r}-1} \leqslant \frac{3^{2r}-3^r+\frac{4}{3}3^{r/3}}{3^{2r}-1} = 1-\frac{3^r-\frac{4}{3}3^{r/3}-1}{3^{2r}-1} \leqslant 1-\frac{1}{2\cdot 3^r}.$$

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

(ii) The result is immediate from Theorem 7.1 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 $rN^*(q^2,r) = q^r - q^{r/p}$, and the result can be verified by direct calculation. So let $p_2 < p_3$ be the two smallest odd primes dividing $r$, then Lemma 7.2(iii) states that $rN^*(q^2,r) \geqslant q^r - q^{r/p_2} - \frac{5}{4}q^{r/p_3}$ and $rN^*(3^2,r) \leqslant 3^r - 3^{r/p_2} - \frac{1}{2}3^{r/p_3}$. 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 $(3q)^{r/p_2}$ yields a contradiction. Hence the result holds for all $r$ and $q$.

(iii) The arguments here are similar to the previous two parts. By Theorem 7.1, the result is immediate if $r$ is even or if $r = 1$. Assume that $r > 1$ is odd, so that $N^{\sim}(q,r) = N(q,r)$.

Let $p$ be a prime divisor of $r$. We digress to prove

(11) $$\frac{q^r-q^{r/p}}{q^r+1} \geqslant \frac{3^r-3^{r/p}}{3^r+1} \text{ or equivalently } \frac{(q^r+1)-(q^{r/p}+1)}{q^r+1} \geqslant \frac{(3^r+1)-(3^{r/p}+1)}{3^r+1}.$$

It suffices to prove $(q^{r/p}+1)(3^r+1) \leqslant (3^{r/p}+1)(q^r+1)$. This is true if $q^{r/p}3^r \leqslant q^r 3^{r/p}$ and $q^{r/p}+3^r \leqslant q^r+3^{r/p}$. The first inequality is true as $3^{r(1-1/p)} \leqslant q^{r(1-1/p)}$. The second inequality is $3^r - 3^{r/p} \leqslant q^r - q^{r/p}$ or $x_0^p - x_0 \leqslant x^p - x$ where $x_0 = 3^{r/p} \leqslant q^{r/p} = x$. However, the function $x^p - x$ is increasing for $x > 1$, so the second inequality holds. This proves (11).

If $r = p^a$ is a prime power, then $rN(q,r) = q^r - q^{r/p}$. Thus Part (iii) is true by (11). Suppose now that $r$ has distinct prime divisors $p_1 < p_2$. Thus $p_1 \geqslant 3$, $p_2 \geqslant 5$ and so $r \geqslant 15$.

Then as in (10) we see that $rN(q,r) = q^r - q^{r/p_1} - \delta q^{r/p_2}$, where $2 - q/(q-1) < \delta < q/(q-1)$. Hence

$$\frac{rN(q,r)}{q^r+1} > \frac{q^r - q^{r/p_1}}{q^r+1} - \frac{\frac{3}{2}q^{r/p_2}}{q^r+1} \quad \text{and} \quad \frac{3^r - 3^{r/p_1}}{3^r+1} - \frac{\frac{1}{2}3^{r/p_2}}{3^r+1} > \frac{rN(3,r)}{3^r+1}.$$

Using (11), it suffices to show that

$$\frac{3^{r/p_2}}{3^r+1} > \frac{3q^{r/p_2}}{q^r+1} \qquad \text{or equivalently} \qquad (q^r+1)3^{r/p_2} > 3q^{r/p_2}(3^r+1).$$

As $q^r + 1 > q^r$ and $2 \cdot 3^r > 3^r + 1$, it suffices to show that $3^{r/p_2}q^r > (6 \cdot 3^r)q^{r/p_2}$. This is true because $(q/3)^{r(1-1/p_2)} \geqslant (5/3)^{15(1-1/5)} = (5/3)^{12} > 6$. This concludes the proof. □

## 8. The generating function $R_{\mathsf{U}}(q,u)$

In this section, we define a key generating function, analyse its convergence and bound its coefficients. We continue to assume throughout that $q$ is an odd prime power.

### 8.1. Introducing $R_{\mathsf{U}}(q,u)$.

Recall the definition of $\Delta_{\mathsf{U}}(2n,q)$ from (4).

Definition 8.1. We shall consider the 'weighted proportions'

$$r_{\mathsf{U}}(2n,q) := \frac{|\Delta_{\mathsf{U}}(2n,q)|}{|\mathrm{GU}_{2n}(q)|} \quad \text{for } n \geqslant 1, \text{ letting } r_{\mathsf{U}}(0,q) = 1,$$

and define the generating function $R_{\mathsf{U}}(q,u) = \sum_{n=0}^{\infty} r_{\mathsf{U}}(2n,q)u^n$.

Recall Types A to D from Proposition 4.3, and that we use these types to describe $\mathsf{U}*$-irreducible polynomials. Recall also Definition 6.1.

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

$$\frac{1}{\left(\prod_{f\in\mathcal{A}_g}(q^{\deg f}-1)\right)\left(\prod_{f\in\mathcal{B}_g}(q^{\deg f}+1)\right)\left(\prod_{f\in\mathcal{C}_g}(q^{\deg f}+1)\right)\left(\prod_{f\in\mathcal{D}_g}(q^{2\deg f}-1)\right)}.$$

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

$$\sum_{n=0}^{\infty}\left(\sum_{g\,\in\,\mathcal{U}_n}\frac{u^n}{\left(\prod_{f\in\mathcal{A}_g}(q^{\deg f}-1)\right)\left(\prod_{f\in\mathcal{B}_g\cup\mathcal{C}_g}(q^{\deg f}+1)\right)\left(\prod_{f\in\mathcal{D}_g}(q^{2\deg f}-1)\right)}\right).$$

Theorem 8.2. *$R_{\mathsf{U}}(q,u)$ is equal as a complex function to $S_0(q,u)S(q,u)$, where $S_0(q,u)$ equals $\left(1+\frac{u}{q-1}\right)^{-1}\left(1+\frac{u}{q+1}\right)^{-3}$ and $S(q,u)$ is the infinite product*

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

*Furthermore, $R_{\mathsf{U}}(q,u)$ is absolutely and uniformly convergent on the open disc $|u| < 1$.*

PROOF. Let

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

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

The contribution of each term of this infinite product depends only on the degree of the corresponding polynomial $f$, and so $R'_{\mathsf{U}}(q,u)$ is equal, as a complex function, to (12)

$$R''_{\mathsf{U}}(q,u)=\prod_{r\text{ even}}\left(1+\frac{u^r}{q^r-1}\right)^{A(q,r)}\prod_{r\text{ odd}}\left(1+\frac{u^r}{q^r+1}\right)^{B(q,r)+C(q,r)}\prod_{\text{all }r}\left(1+\frac{u^{2r}}{q^{2r}-1}\right)^{D(q,r)}.$$

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

We now consider convergence of $S(q,u)$. By [4, Corollary 1.3.2], each of

the product $\displaystyle\prod_{r\geqslant 1}\left(1+\frac{u^r}{q^r-1}\right)^{\frac{1}{2}N^*(q^2,r)}$ and the sum $\displaystyle\sum_{r\geqslant 1}\frac{1}{2}N^*(q^2,r)\frac{|u^r|}{q^r-1}$

is absolutely and uniformly convergent if and only if the other has these properties. Now, by [4, 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 $r\geqslant 3$ is odd, so the displayed sum is absolutely and uniformly convergent for $|u|<1$. Similarly, for the product

$\displaystyle\prod_{r\geqslant 1}\left(1+\frac{u^r}{q^r+1}\right)^{N^{\sim}(q,r)}$ we consider the sum $\displaystyle\sum_{r\geqslant 1}N^{\sim}(q,r)\frac{|u^r|}{q^r+1}$.

By [4, Lemma 1.3.12(a)], $N^{\sim}(q,r)=r^{-1}q^r-O(q^{r/3})$ 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 $\prod_{r\geqslant 1}(1+\frac{u^{2r}}{q^{2r}-1})^{\frac{1}{2}M^*(q^2,r)-\frac{1}{2}N^{\sim}(q,r)}$, 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 $|u|<1$. □

THEOREM 8.3. *The limit* $\lim_{n\to\infty} r_{\mathsf{U}}(2n,q)$ *exists and is equal to*

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

PROOF. Consider the expression $R_{\mathsf{U}}(q,u)=S_0(q,u)S(q,u)$ 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

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

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

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

Since $R_{\mathsf{U}}(q,u)$ is uniformly convergent, we can rearrange the infinite product. Substituting the above displayed expression into $R_{\mathsf{U}}(q,u)$ gives

$$R_{\mathsf{U}}(q,u) = \frac{(1+\frac{u^2}{q^2-1})^{3/2}}{1+\frac{u}{q+1}} \prod_{r\geqslant 1}\left(1+\frac{u^{2r}}{q^{2r}-1}\right)^{\frac{1}{2}(N^*(q^2,2r)+M^*(q^2,r)-N^{\sim}(q,r))} \prod_{r\geqslant 1\text{ odd}}\left(1+\frac{u^r}{q^r+1}\right)^{N(q,r)}.$$

In the first infinite product, we rewrite the exponents using Lemma 7.3, then replace $2r$ by $r$, and finally we combine the two infinite products to obtain

$$R_{\mathsf{U}}(q,u) = \left(1+\frac{u}{q+1}\right)^{-1} \prod_{r\geqslant 1}\left(1+\frac{u^r}{q^r-(-1)^r}\right)^{N(q,r)}. \tag{13}$$

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 $|u|<1$,

$$\frac{1-u/q}{1-u}\prod_{r\geqslant 1}\left(1-\frac{u^r}{q^r}\right)^{N(q,r)} = 1.$$

Multiplying this by our expression for $R_{\mathsf{U}}(q,u)$ gives that for $|u|<1$

$$\begin{aligned} R_{\mathsf{U}}(q,u) &= \frac{1-\frac{u}{q}}{(1-u)(1+\frac{u}{q+1})}\prod_{r\geqslant 1}\left(\left(1+\frac{u^r}{q^r-(-1)^r}\right)\left(1-\frac{u^r}{q^r}\right)\right)^{N(q,r)} \\ &= \frac{1-\frac{u}{q}}{(1-u)(1+\frac{u}{q+1})}\prod_{r\geqslant 1}\left(1-\frac{u^r(u^r-(-1)^r)}{q^r(q^r-(-1)^r)}\right)^{N(q,r)}. \end{aligned} \tag{14}$$

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

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

Using the bound $N(q,r) < q^r/r$ 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], $\lim_{n\to\infty} r_{\mathsf{U}}(2n,q) = H(1)$, and the result follows. □

### 8.2. Upper and lower bounds on $r_{\mathsf{U}}(2n,q)$.

NOTATION 8.4. If $f(z) := \sum_{n\geqslant 0} f_n z^n$ is a power series, we write $[z^n]f(z)$ to denote the coefficient $f_n$ of $z^n$, and we write $|f|(z)$ for the power series $\sum_{n\geqslant 0}|f_n|z^n$. Let $g(z) := \sum_{n\geqslant 0} g_n z^n$. We write $f(z) \ll g(z)$ if $f_n \leqslant g_n$ for all $n$.

Definition 8.5. Recall (14), and define $R_{\mathsf{U}}(q,u) = A_{\mathsf{U}}(q,u)B_{\mathsf{U}}(q,u)$, where

$$A_{\mathsf{U}}(q,u) = \sum_{n\geqslant 0} a_n u^n := \frac{1-\frac{u}{q}}{(1-u)(1+\frac{u}{q+1})}, \quad \text{and}$$

$$B_{\mathsf{U}}(q,u) = \sum_{n\geqslant 0} b_n u^n := \prod_{r\geqslant 1}\left(1-\frac{u^r(u^r-(-1)^r)}{q^r(q^r-(-1)^r)}\right)^{N(q,r)}.$$

We let $B_{\mathsf{U}}(q,u) = \prod_{r\geqslant 1} B_{\mathsf{U}}(r,q,u)$, where

$$B_{\mathsf{U}}(r,q,u) = \left(1-\frac{u^r(u^r-(-1)^r)}{q^r(q^r-(-1)^r)}\right)^{N(q,r)}.$$

We shall bound $r_{\mathsf{U}}(2n,q)$ by first bounding the $b_n$.

Lemma 8.6. *For all $n$, the absolute value $|b_n| \leqslant \beta q^{-n/2}$, where $\beta := q/(q-1)$. In particular, $B_{\mathsf{U}}(q,u)$ is absolutely convergent for all $|u| < q^{1/2}$.*

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

$$|B_{\mathsf{U}}|(r,q,u) \ll \left(1+\frac{u^r(u^r+1)}{q^r(q^r-1)}\right)^{N(q,r)}. \tag{15}$$

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

$$B_{\mathsf{U}}(r,q,u) = \left(1-\frac{u^r(u^r+1)}{q^r(q^r+1)}\right)^{N} = \sum_{n=0}^{2N}\left(\sum_{n/2\leqslant j\leqslant n}(-1)^j\binom{N}{j}\binom{j}{n-j}\frac{1}{(q^r(q^r+1))^j}\right)u^{rn},$$

and hence when $r$ is even

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

It is shown in [3, p. 433] that when $r$ is odd

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

Hence (15) holds for all values of $r$.

Now, from Definition 8.5, we deduce from (15) that

$$|B_{\mathsf{U}}|(q,u) \ll \prod_{r\geqslant 1}|B_{\mathsf{U}}|(r,q,u) \ll \prod_{r\geqslant 1}\left(1+\frac{u^r(u^r+1)}{q^r(q^r-1)}\right)^{N(q,r)}.$$

Comparing the expression for $B_{\mathsf{U}}(q,u)$ with that for $B(q,u)$ in [3, Equation (8)], we can reason just as in the proof of Lemma 4.1 in [3, p. 434] that the bound in [3, Equation (10)] is valid for $|B_{\mathsf{U}}|(q,u)$. This is precisely the bound in the current lemma.

The convergence claims are clear. □

THEOREM 8.7. *Let* $\alpha = (q^2-1)/(q^2+2q)$. *Then* $B_{\mathsf{U}}(q,1) = \sum_{n\geqslant 0} b_n$ *converges and* $\lim_{n\to\infty} r_{\mathsf{U}}(2n,q)$ *equals* $\alpha B_{\mathsf{U}}(q,1)$. *Furthermore*

$$\varepsilon_n := |r_{\mathsf{U}}(2n,q) - \alpha B_{\mathsf{U}}(q,1)| < \frac{\alpha q^{1/2}+2}{q^{(n-1)/2}(q-1)(q^{1/2}-1)} = O(q^{-(n-1)/2}).$$

PROOF. By Definition 8.5, the coefficient $r_{\mathsf{U}}(2n,q) = \sum_{k=0}^{n} a_{n-k}b_k$. Notice that

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

Hence $a_n = \frac{q^2-1}{q^2+2q} + c_n$, where $c_n := (-1)^n\frac{2q+1}{q(q+2)(q+1)^n}$. By Lemma 8.6, $B_{\mathsf{U}}(q,1)$ converges. Therefore

$$r_{\mathsf{U}}(2n,q) - \alpha B_{\mathsf{U}}(q,1) = \sum_{k=0}^{n}(\alpha + c_{n-k})b_k - \alpha\sum_{k\geqslant 0} b_k = \sum_{k=0}^{n} c_{n-k}b_k - \alpha\sum_{k>n} b_k. \tag{16}$$

We bound the terms on the right side of (16) as follows. Using $(2q+1)/(q(q+2)) < 2/(q+1)$ gives

$$|c_n| = (2q+1)(q(q+2)(q+1)^n)^{-1} < 2(q+1)^{-n-1} < 2q^{-n-1}.$$

Hence, by Lemma 8.6,

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

Similarly, from Lemma 8.6, we deduce that

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

Substituting the previous two displayed equations into (16), and setting $\beta = q/(q-1)$, gives

$$|r_{\mathsf{U}}(2n,q) - \alpha B_{\mathsf{U}}(q,1)| < \frac{(\alpha q^{1/2}+2)\beta}{q^{(n+1)/2}(q^{1/2}-1)} = \frac{\alpha q^{1/2}+2}{q^{(n-1)/2}(q-1)(q^{1/2}-1)}.$$

Therefore $r_{\mathsf{U}}(2n,q) \to \alpha B_{\mathsf{U}}(q,1)$ as $n\to\infty$ as claimed. □

We next record a technical lemma.

LEMMA 8.8. *Let* $a, b \in \mathbb{R}_{>0}$ *such that* $b > 1$ *and* $ab < 1$. *Then* $(1-a)^b \geqslant 1 - ab$.

PROOF. It suffices to show that $b\log(1-a) \geqslant \log(1-ab)$. We use the expansion $\log(1-x) = -\sum_{n=1}^{\infty} x^n/n$, valid for $0 < x < 1$. Notice that

$$b\log(1-a) = -ab - a^2b\left(\frac{1}{2}+\frac{a}{3}+\cdots\right), \quad \log(1-ab) = -ab - a^2b\left(\frac{b}{2}+\frac{ab^2}{3}+\cdots\right).$$

Since $b > 1$, it follows that $a^ib^{i+2}/(i+2) > a^i/(i+2)$ for all $i$, from which the result follows. □

THEOREM 8.9. *Let*

$$\mu = \frac{q^2-1}{q^2+2q}\left(1-\frac{2}{q(q+1)}\right)^{q-1},$$

*let* $\delta = 1 - 3/(4q^3)$*, and let* $\varepsilon_n$ *be as in Theorem 8.7. Then* $\mu\delta - \varepsilon_n < r_{\mathsf{U}}(2n,q) < \mu + \varepsilon_n$*. In particular,* $r_{\mathsf{U}}(2,3) = 0.25$*, and* $0.3433 < r_{\mathsf{U}}(2n,3) < 0.3795$ *for* $n \geqslant 2$*.*

PROOF. We first bound $B_{\mathsf{U}}(q,1)$. It follows from Definition 8.5 that

$$B_{\mathsf{U}}(q,1) = \prod_{r\,\geqslant\,1\text{ odd}} \left(1-\frac{2}{q^r(q^r+1)}\right)^{N(q,r)} \leqslant \left(1-\frac{2}{q(q+1)}\right)^{N(q,1)}.$$

By Theorem 7.1, the upper bound above is $\gamma := (1-2/(q(q+1)))^{q-1}$. For a lower bound, note that $1-2/(q^r(q^r+1)) > 1-2/q^{2r}$, and $N(q,r) \leqslant q^r/r$ by Lemma 7.2(i). Hence

$$B_{\mathsf{U}}(q,1) = \gamma \prod_{r\geqslant 3\text{ odd}} \left(1-\frac{2}{q^r(q^r+1)}\right)^{N(q,r)} \geqslant \gamma \prod_{r\geqslant 3\text{ odd}} \left(1-\frac{2}{q^{2r}}\right)^{q^r/r}.$$

Lemma 8.8 with $a = 2q^{-2r}$ and $b = q^r/r$ gives $(1-2q^{-2r})^{q^r/r} \geqslant 1-2/(rq^r)$, and by induction

$$B_{\mathsf{U}}(q,1) \geqslant \gamma \prod_{r\geqslant 3\text{ odd}} \left(1-\frac{2}{rq^r}\right) \geqslant \gamma\left(1-\sum_{r\geqslant 3\text{ odd}}\frac{2}{rq^r}\right).$$

However,

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

and so $B_{\mathsf{U}}(q,1) > \gamma\,(1-3/(4q^3))$. Setting $\delta = 1-3/(4q^3)$ and

$$\mu = \alpha\gamma = \frac{q^2-1}{q(q+1)}\left(1-\frac{2}{q(q+1)}\right)^{q-1}$$

gives $\mu\delta < \alpha B_{\mathsf{U}}(q,1) < \mu$. The main claim follows from Theorem 8.7. When $q=3$, this becomes $0.3601 < \alpha B_{\mathsf{U}}(3,1) < 0.3704$.

Finally, we estimate $r_{\mathsf{U}}(2n,3)$ for $n \geqslant 3$. We compute the values of $r_{\mathsf{U}}(2n,q)$ directly for $n \leqslant 20$, using the expression for $R_{\mathsf{U}}(q,u)$ given in (13), and we find that $r_{\mathsf{U}}(0,q)$ and $r_{\mathsf{U}}(2,q)$ are as given, and that for $n \geqslant 2$ we can bound $0.3433 < r_{\mathsf{U}}(2n,q) < 0.3795$. Assume therefore that $n \geqslant 21$. For $q=3$, Theorem 8.7 simplifies to

$$|r_{\mathsf{U}}(2n,3) - \alpha B_{\mathsf{U}}(3,1)| \leqslant \varepsilon_n = \frac{27+19\sqrt{3}}{30}3^{-(n-1)/2}.$$

However, $(27+19\sqrt{3})/30 < 2$ and $3^{-(n-1)/2} \leqslant 3^{-10}$, and so

$$\alpha B_{\mathsf{U}}(3,1) - 2/3^{10} \leqslant r_{\mathsf{U}}(2n,3) < \alpha B_{\mathsf{U}}(3,1) + 2/3^{10}.$$

The bounds for $n \geqslant 3$ now follow from $0.3601 < \alpha B_{\mathsf{U}}(3,1) < 0.3704$. □

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

We wish to estimate the proportion of pairs $(t, y) \in \Delta_{\mathsf{U}}(2n, q)$ for which $\mathrm{inv}(y)$ induces a strong involution on one of the $t$-eigenspaces. A central issue underpinning this is the link between the eigenspaces of $\mathrm{inv}(y)$ and the characteristic polynomial of $y$ (acting on some $U \leqslant V$). 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 $2^B$, and
(b) the restriction $y^+ := y|_{U^+}$ is guaranteed to have 2-part order strictly less than $2^B$.

The $\varepsilon$-eigenspace of $\mathrm{inv}(y)|_U$ is $U^\varepsilon$, and it is possible to detect whether conditions (a,b) hold from the characteristic polynomial of $y|_U$. In Subsections 9.1 and 9.2 we introduce functions $G_{\mathsf{U},b}(q, u)$, $R_{\mathsf{U},b}(q, u)$ and $G^-_{\mathsf{U},b}(q, u)$, each related to $R_{\mathsf{U}}(q, u)$, for certain non-negative integers $b$. These three functions will help detect these properties. We will see that $G^-_{\mathsf{U},b}(q, u)$ counts pairs $(t^-, y^-)$ for which the 2-part order of $y^-$ equals $2^{b-1}(q^2 - 1)_2$, while the pairs $(t^+, y^+)$ counted by $R_{\mathsf{U},b}(q, u)$ are such that the 2-part order of $y^+$ is less than $2^{b-1}(q^2-1)_2$. Thus properties (a) and (b) are determined by the characteristic polynomials of $y^\pm$.

The functions $G^-_{\mathsf{U},b}(q, u)$ and $R_{\mathsf{U},b}(q, u)$ are therefore crucial. In particular we will need lower bounds on the sizes of the coefficients of their power series. In Subsection 9.1 we define functions $T_{\mathsf{U},b}(q, u)$, for positive integers $b$, and prove that $R_{\mathsf{U},b}(q, u) = R_{\mathsf{U}}(q, u)T_{\mathsf{U},b}(q, u)^{-1}$ (Theorem 9.2). The 2-part orders of the roots will play a critical role. In Subsection 9.2, we introduce a truncated version $F_{\mathsf{U},b}(q, u)$ of $G^-_{\mathsf{U},b}(q, u)$ from which it is easier to deduce lower bounds for the coefficients of $G^-_{\mathsf{U},b}(q, u)$. We also prove the fundamental Lemma 9.5 that links the number of pairs $(t, y)$ in $\Delta_{\mathsf{U}}(2n, q)$, where $y$ has a particular type of characteristic polynomial, with products of certain coefficients of $R_{\mathsf{U},b}(q, u)$ and $G^-_{\mathsf{U},b}(q, u)$. In the remaining two technical subsections (9.3 and 9.4) we obtain the required lower bounds: for the coefficients of $T_{\mathsf{U},b}(q, u)^{-1}$ (in 9.3), then for $R_{\mathsf{U},b}(q, u)$ and $F_{\mathsf{U},b}(q, u)$ (in 9.4). These bounds are used in §10 to prove Theorem 1.

Our methods in this section are guided by the work of Dixon, Praeger and Seress in [**3**], and we have used similar notation to facilitate comparisons between the two analyses. However, the results of [**3**] unfortunately do not carry over without careful re-analysis.

We shall continue to assume that $q$ is an odd prime power.

**9.1. Related functions $G_{\mathsf{U},b}(q, u)$, $R_{\mathsf{U},b}(q, u)$ and $T_{\mathsf{U},b}(q, u)$.** Recall from Theorem 8.2 that $R_{\mathsf{U}}(q, u) = S_0(q, u)S(q, u)$. Recall also the relationships between the power series given in Lemma 7.5. For each $b \geqslant 0$, we now define an infinite series $G_{\mathsf{U},b}(q, u) = \sum_{n\geqslant 0} g_b(2n, q)u^n$ as follows. First define

$$
\begin{aligned}
G_{\mathsf{U},0}(q, u) &:= \prod_{r\geqslant 1}\left(1 + \tfrac{u^r}{q^r-1}\right)^{A(q,r)} \prod_{r\geqslant 1}\left(1 + \tfrac{u^r}{q^r+1}\right)^{B(q,r)+C(q,r)} \\
&= S_0(q, u)\prod_{r\geqslant 1}\left(1 + \tfrac{u^r}{q^r-1}\right)^{\frac{1}{2}N^*(q^2,r)} \prod_{r\geqslant 1}\left(1 + \tfrac{u^r}{q^r+1}\right)^{N^\sim(q,r)}.
\end{aligned}
\tag{17}
$$

It follows from §8 that $g_0(2n, q)|\mathrm{GU}_{2n}(q)|$ is equal to the number of pairs $(t, y) \in \Delta_{\mathsf{U}}(2n, q)$ for which each factor in the $\mathsf{U}*$-factorisation of $c_y(X)$ is of type A, B or C.

For the infinite product $S(q,u) = R_{\mathsf{U}}(q,u)/S_0(q,u)$, the terms are labelled 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 $m \geqslant 1$" simply as "$m$ odd". For each $b \geqslant 1$, define

$$G_{\mathsf{U},b}(q,u) := \prod_{m \text{ odd}} \left(1 + \frac{u^{2^b m}}{q^{2^b m} - 1}\right)^{D(q,2^{b-1}m)}, \tag{18}$$

and so by Lemma 7.5

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

It follows from §8 that for $b \geqslant 1$ the quantity $[u^n]G_{\mathsf{U},b}(q,u)\,|\mathrm{GU}_{2n}(q)|$, that is to say, $g_b(2n,q)\,|\mathrm{GU}_{2n}(q)|$, is equal to the number of pairs $(t,y) \in \Delta_{\mathsf{U}}(2n,q)$ for which each factor in the $\mathsf{U}*$-factorization of $c_y(X)$ is of type D, and each $\mathsf{U}*$-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 $\mathsf{U}*$-irreducible polynomial $g(X)$ has degree $4r = 2^{b+1}m$ with $m$ odd, and $\omega_2(g) \leqslant (q^{2r}-1)_2 = 2^{b-1}(q^2-1)_2$; 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 $b \geqslant 1$, we now define an ascending chain of subsets $\Delta_{\mathsf{U},b}(2n,q)$ of $\Delta_{\mathsf{U}}(2n,q)$. Let $\Delta_{\mathsf{U},b}(2n,q)$ consist of those $(t,y) \in \Delta_{\mathsf{U}}(2n,q)$ such that each $\mathsf{U}*$-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 $2^b$. Thus in particular $\Delta_{\mathsf{U},1}(2n,q)$ contains only those $(t,y)$ where each $\mathsf{U}*$-irreducible factor of $c_y(X)$ is of type A, B, or C; whilst $\Delta_{\mathsf{U},2}(2n,q)$ also allows factors of type D, provided that their degree is $4m$ for some odd $m$.

Definition 9.1. For $b \geqslant 1$, let $r_{\mathsf{U},b}(2n,q) := |\Delta_{\mathsf{U},b}(2n,q)|\,/|\mathrm{GU}_{2n}(q)|$ for $n > 0$, and let $r_{\mathsf{U},b}(0,q) := 1$. We define $R_{\mathsf{U},b}(q,u) := \sum_{n=0}^\infty r_{\mathsf{U},b}(2n,q)u^n$, and for $b \geqslant 1$, set $T_{\mathsf{U},b}(q,u) := \prod_{k \geqslant b} G_{\mathsf{U},k}(q,u)$.

Theorem 9.2. *The power series $R_{\mathsf{U}}(q,u)$, and $G_{\mathsf{U},b}(q,u)$ (for $b \geqslant 0$), and $R_{\mathsf{U},b}(q,u)$ and $T_{\mathsf{U},b}(q,u)^{-1}$ (for $b \geqslant 1$) all converge absolutely and uniformly in the open disc $|u| < 1$. In this disc,*

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

Proof. By Theorem 8.2, $R_{\mathsf{U}}(q,u)$ converges absolutely and uniformly in the disc $|u| < 1$. A similar argument shows that the $G_{\mathsf{U},b}(q,u)$ converge absolutely and uniformly for $|u| < 1$. Hence $T_{\mathsf{U},b}(q,u)$ is also absolutely convergent for each $b$. Since convergent products converge to nonzero limits, it follows that $T_{\mathsf{U},b}(q,u)^{-1}$ is also absolutely convergent.

From (12), we see that the terms of $R_{\mathsf{U}}(q,u)$ are a permutation of the terms of $\prod_{b=0}^{\infty} G_{\mathsf{U},b}(q,u)$. 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 $b \geqslant 1$. Since $0 < r_{\mathsf{U},b}(2n,q) < r_{\mathsf{U}}(2n,q)$ for all $n$, $R_{\mathsf{U},b}(q,u)$ converges absolutely and uniformly for $|u|<1$. It follows from the discussion after (18), and Definition 9.1, that $R_{\mathsf{U},b}(q,u)$ is a product of a permutation of the terms of $\prod_{k=0}^{b-1} G_{\mathsf{U},k}(q,u)$. The absolute convergence for $|u|<1$ of each infinite expression in the second displayed equality in the statement implies the equality of these functions. The final equality is now immediate. □

**9.2. Truncations of the power series $G_{\mathsf{U},b}(q,u)$.** For the definitions of the subset $\mathcal{D}_{4r}^-$ of $\mathcal{D}_{4r}$ and the quantity $N_{\mathsf{U}}^-(q,4r)$, see Definition 4.9.

Definition 9.3. For $b \geqslant 1$, we 'truncate' the infinite product defined by (18) by reducing the exponent of each term, and hence removing some of the factors. We set

$$G_{\mathsf{U},b}^-(q,u) = \sum_{n\geqslant 0} g_{\mathsf{U},b}^-(2n,q)u^n := \prod_{m \text{ odd}} \left(1+\frac{u^{2^b m}}{q^{2^b m}-1}\right)^{N_{\mathsf{U}}^-(q,2^{b+1}m)}. \tag{19}$$

Remark 9.4. For $b>1$ the product expression for $G_{\mathsf{U},b}^-(q,u)$ is a truncation of the one for $G_{\mathsf{U},b}$, because $\mathcal{D}_{4r}^- \subset \mathcal{D}_{4r}$. For $b=1$ notice that replacing the exponent $D(q,m)$ in (18) by the exponent $N_{\mathsf{U}}^-(q,2m)$ either preserves or decreases exponents, even for the term $m=1$, as the exponent of $(1+\frac{u^2}{q^2-1})$ in $G_{\mathsf{U},1}(q,u)$ is

$$(3/2) + M^*(q^2,1)/2 - N^{\sim}(q,1)/2 = D(q,1) = (q-1)^2/4 \geqslant (q^2-1)/8,$$

since $q \geqslant 3$. Theorem 9.2 shows that each $G_{\mathsf{U},b}^-(q,u)$ is absolutely convergent for $|u|<1$.

We do not know the precise value of $N_{\mathsf{U}}^-(q,2^{b+1}m)$, but we found a lower bound for it in Lemma 4.10(iii). Hence, rather than calculate $G_{\mathsf{U},b}^-(q,u)$ it is simpler to compute

$$F_{\mathsf{U},b}(q,u) = \sum_{n=0}^{\infty} f_{\mathsf{U},b}(2n,q)u^n := \prod_{m \text{ odd}} \left(1+\frac{u^{2^b m}}{q^{2^b m}-1}\right)^{\left\lceil \frac{1}{8}N(q^2,2^{b-1}m)\right\rceil}. \tag{20}$$

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

Lemma 9.5. *Fix $b>1$, let $k \geqslant \ell \geqslant 0$ with $k>0$, and let $a_{k\ell} := r_{\mathsf{U},b}(2k-2\ell,q)g_{\mathsf{U},b}^-(2\ell,q)$. Then $a_{k\ell}|\mathrm{GU}_{2k}(q)|$ is equal to the number of pairs $(t,y) \in \Delta_{\mathsf{U}}(2k,q)$ such that the characteristic polynomial $c_y(X)$ for $y$ has the form $c_y(X) = c_y^-(X)c_y^+(X)$, where:*

- (i) *$c_y^-(X)$ is the product of the $\mathsf{U}*$-irreducible factors $g(X)$ of $c_y(X)$ which lie in the set $\bigcup_{m \text{ odd}} \mathcal{D}_{2^{b+1}m}^-$; 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, $\deg c_y^-(X) = 2\ell$.*
- (ii) *$c_y^+(X)$ is a product of $\mathsf{U}*$-irreducible polynomials $g(X)$ which are either not of type D or have degree with 2-part dividing $2^b$, and satisfy $\omega_2(g) \leqslant 2^{b-2}(q^2-1)_2$.*

(iii) *If* $\ell > 0$ *then* $inv(y)$ *is of type* $(2k-2\ell, 2\ell)$.
(iv) $0 \ll F_{\mathsf{U},b}(q,u) \ll G^{-}_{\mathsf{U},b}(q,u)$, *and if* $f_{\mathsf{U},b}(2n,q) \neq 0$ *then* $2^b$ *divides* $n$.
(v) $[u^n]F_{\mathsf{U},b}(q,u)\,|\mathrm{GU}_{2n}(q)|$ *is at most the number of pairs* $(t,y)$ *in* $\Delta_{\mathsf{U}}(2n,q)$ *such that each* $\mathsf{U}*$*-irreducible factor* $g(X)$ *of* $c_y(X)$ *satisfies* $\omega_2(g) = 2^{b-1}(q^2-1)_2$.

Proof. Recall that $r_{\mathsf{U},b}(2k-2\ell,q)|\mathrm{GU}_{2k-2\ell}(q)|$ counts certain pairs $(t,y) \in \Delta_{\mathsf{U}}(2k-2\ell,q)$ (Definition 9.1). By Lemma 4.10(i)(ii), it follows from $b \geqslant 2$ that $|y|_2 \leqslant 2^{b-2}(q^2-1)_2$.

By construction, $g^{-}_{\mathsf{U},b}(2\ell,q)\,|\mathrm{GU}_{2\ell}(q)|$ is the number of pairs $(t,y) \in \Delta_{\mathsf{U}}(2\ell,q)$ such that each $\mathsf{U}*$-irreducible factor of $c_y(X)$ lies in $\bigcup_{m\ odd}\mathcal{D}^{-}_{2^{b+1}m}$. Such a $y$ satisfies $|y|_2 = 2^{b-1}(q^2-1)_2$, and the 2-part of the degree of each $\mathsf{U}*$-irreducible factor is $2^{b+1}$. Notice that

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

By Lemma 6.2, to count the pairs $(t,y) \in \Delta_{\mathsf{U}}(2k,q)$ 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, and $\dim(U) = 2k-2\ell$: this is

$$\frac{|\mathrm{GU}_{2k}(q)|}{|\mathrm{GU}_{2k-2\ell}(q) \times \mathrm{GU}_{2\ell}(q)|}.$$

We then multiply by the number of possible actions of $t|_U$ and $y|_U$ such that all $\mathsf{U}*$-irreducible factors of $y$ are of type A, B or C, or of type D with 2-part of the degree at most $2^b$: this is exactly $r_{\mathsf{U},b}(2k-2\ell)|\mathrm{GU}_{2k-2\ell}(q)|$. Finally we multiply by $g^{-}_{\mathsf{U},b}(2\ell,q)|\mathrm{GU}_{2\ell}(q)|$ for the number of choices of $t|_W$ and $y|_W$ that ensure that each irreducible factor $g(X)$ of $c_{y|_W}(X)$ lies in $\mathcal{D}^{-}_{2^{b+1}m}$ 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), $\omega_2(c^{+}_y(X)) \leqslant 2^{b-2}(q^2-1)_2$. Hence if $\ell > 0$ then $\mathrm{inv}(y)$ has $(-1)$-eigenspace of dimension $\deg(c^{-}_y) = 2\ell$, and $\mathrm{inv}(y)$ has type $(2k-2\ell, 2\ell)$.

For Part (iv) it is immediate from (20) that each coefficient $f_{\mathsf{U},b}(2n,q)$ of $F_{\mathsf{U},b}(q,u)$ is non-negative, and from Lemma 4.10(iii) that $g^{-}_{\mathsf{U},b}(2n,q) \geqslant f_{\mathsf{U},b}(2n,q)$ for all $n$. For the final claim, notice that if $f_{\mathsf{U},b}(2n,q) > 0$ then $g^{-}_{\mathsf{U},b}(2n,q) > 0$, and so, as argued for Part (i) above, there exists $(t,y) \in \Delta_{\mathsf{U}}(2n,q)$ such that each $\mathsf{U}*$-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). □

**9.3. Bounding the coefficients of $T_{\mathsf{U},b}(q,u)^{-1}$.** Recall the power series $T_{\mathsf{U},b}(q,u)$, see Definition 9.1. We will use the bounds derived for $r_{\mathsf{U}}(2n,q)$ in Theorem 8.9, together with bounds we shall derive in this subsection for the coefficients of $T_{\mathsf{U},b}(q,u)^{-1}$, to obtain bounds for the coefficients of $R_{\mathsf{U},b}(q,u)$. It will suffice to consider only $b \geqslant 3$. Now

$$(21)\quad T_{\mathsf{U},b}(q,u)^{-1} = \prod_{k=b}^{\infty}\prod_{m\,\mathrm{odd}}\left(1+\frac{u^{2^k m}}{q^{2^k m}-1}\right)^{-D(q,2^{k-1}m)} = \prod_{m=1}^{\infty}\left(1+\frac{u^{2^b m}}{q^{2^b m}-1}\right)^{-D(q,2^{b-1}m)}$$

where the second rearrangement is permissible in the disc $|u| < 1$ due to Theorem 9.2.

Fix a value of $b \geqslant 3$ and define $d := 2^b$, $U := u^{2^b}$ and $Q := q^{2^b}$. We will now bound the coefficients $t_n := [U^n]T_{\mathsf{U}}(U)$ of the power series $T_{\mathsf{U}}(U)$, where

$$1 - T_{\mathsf{U}}(U) := \prod_{m=1}^{\infty} \left(1 + \frac{U^m}{Q^m - 1}\right)^{-D(q,dm/2)}. \tag{22}$$

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

LEMMA 9.6. *Assume that $b \geqslant 3$, that is, $d \geqslant 8$, and define*

$$W_{\mathsf{U}}(U) = \sum_{n \geqslant 0} w_n U^n := -\log\left(1 - T_{\mathsf{U}}(U)\right) + \frac{1}{2d}\log(1-U).$$

(i) *$T_{\mathsf{U}}(U)$ and $W_{\mathsf{U}}(U)$ are absolutely and uniformly convergent in the open disc $|U| < 1$.*
(ii) *In this disc, $1 - T_{\mathsf{U}}(U) = T_{\mathsf{U},b}(q,u)^{-1}$.*
(iii) *$w_0 = 0$, and $|w_n| < 2d^{-1}n^{-1}(Q-1)^{-n/2}$ for all $n \geqslant 1$.*

PROOF. (i) Notice that the product in (22) converges absolutely and uniformly if and only if the product $\prod_{m=1}^{\infty}(1 + U^m/(Q^m-1))^{D(q,dm/2)}$ does so too. By [4, Lemma 1.3.1], this happens if and only if $\sum_{m=1}^{\infty} D(q,dm/2)|U^m|/(Q^m-1)$ converges absolutely and uniformly. By Lemma 7.7(ii), $D(q,dm/2) < (q^{dm}-1)/2dm < Q^m/2dm$, so the result follows.

(ii) This is now immediate from (21) and (22).

(iii) We follow the same strategy (but with $W_{\mathsf{U}}(U)$ in place of $W(U)$) as in the proof of [3, Lemma 4.2], to write $W_{\mathsf{U}}(U) = W_{\mathsf{U},1}(U) + W_{\mathsf{U},2}(U)$ where

$$W_{\mathsf{U},1}(U) := \sum_{m=1}^{\infty}\left\{D(q,dm/2)\frac{U^m}{Q^m-1} - \frac{U^m}{2dm}\right\} = \sum_{n=1}^{\infty} w_{1,n}U^n, \text{ say}$$

$$W_{\mathsf{U},2}(U) := \sum_{m=1}^{\infty}\sum_{k=2}^{\infty}(-1)^{k+1}D(q,dm/2)\frac{U^{mk}}{k(Q^m-1)^k} = \sum_{n=2}^{\infty} w_{2,n}U^n, \text{ say.}$$

Notice that $w_0 = 0$. In order to treat the $w_{1,n}$, we use Lemma 7.7(iii) to get

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

where $1 - 2Q^{-m/3} \leqslant \eta(q, \frac{md}{2}) < 2.2$. Thus for all $n \geqslant 1$,

$$|w_{1,n}| = \left|\frac{D(q,dn/2)}{Q^n-1} - \frac{1}{2dn}\right| = \left|\frac{-\eta(q,dn/2)}{2dn(Q^{n/2}+1)}\right| \leqslant \frac{1}{2dn}\cdot\frac{2.2}{Q^{n/2}+1} \leqslant \frac{1.1(Q-1)^{-n/2}}{dn}.$$

Since $D(q,dm/2) \leqslant (Q^m-1)/2dm$, we can mimic the proof of [3, Lemma 4.2] to deduce that

$$|w_{2,n}| < (2dn)^{-1}(Q-1)^{-n/2}\left(1-(Q-1)^{-1}\right)^{-1} \leqslant (2dn)^{-1}1.0002(Q-1)^{-n/2}.$$

Hence $|w_n| \leqslant |w_{1n}| + |w_{2n}| < 2d^{-1}n^{-1}(Q-1)^{-n/2}$ for all $n \geqslant 1$ as required. □

Let $W_{\mathsf{U}}(U)$ be as in Lemma 9.6, and let $E(U) := \exp(-W_{\mathsf{U}}(U)) - 1 = \sum_{n=1}^{\infty} e_n U^n$. Let $h(U) = \sum_{k=1}^{\infty} h_k U^k$, say, be the series for $1-(1-U)^{1/2d}$. Then

$$1 - T_{\mathsf{U}}(U) = (1-U)^{1/2d}(1+E(U)) = (1-h(U))\,(1+E(U)). \tag{23}$$

Comparing (23) 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 $k \geqslant 2$

$$1 > 2dkh_k > \exp\left(\frac{-(1+\log k)}{2d-1}\right). \tag{24}$$

We use this to estimate the values of the coefficients $e_n$ and $t_k$.

Lemma 9.7. *Let $d = 2^b \geqslant 8$, and let $\gamma = (1+d^{-1})(Q-1)^{-1/2}$.*

(i) *$|e_n| \leqslant \frac{2}{1+d}\gamma^n$ for all $n \geqslant 1$. In particular, $\gamma \leqslant 0.014$ and $d\,|e_1| < 0.025$.*
(ii) *$dkt_k < 0.5065$ for $k \geqslant 1$, whenever $dk \leqslant e^{d/2}$.*

Proof. (i) Lemma 9.6 shows that $|w_n| \leqslant 2d^{-1}(Q-1)^{-n/2}$ for all $n \geqslant 1$. Let $\beta = (Q-1)^{-1/2}$ and $\alpha = 2d^{-1}\beta$, so that $|w_n| \leqslant \alpha\beta^{n-1}$ for all $n \geqslant 1$, and $\gamma := \alpha/2 + \beta = (1+d^{-1})(Q-1)^{-1/2} \leqslant 1$. Thus [**3**, Lemma 3.4] applies to $-W_{\mathsf{U}}(U)$ with this $\alpha$ and $\beta$, and yields $|e_n| \leqslant \alpha\gamma^{n-1} = \frac{2}{1+d}\gamma^n$ for all $n \geqslant 1$. From $q^d \geqslant 3^8$ we see that $\gamma \leqslant 0.014$, and that $d\,|e_1| \leqslant \frac{2d}{1+d}\gamma = 2(Q-1)^{-1/2} < 0.025$.

(ii) The proof is similar to that of the upper bound in [**3**, Lemma 4.4], and we only give the necessary details. First let $k=1$. From (22) we see that $t_1 = D(q,d/2)(q^d-1)^{-1} = 0.5d^{-1}(q^{d/2}-1)/(q^{d/2}+1)$ by Lemma 7.7(i), and so $t_1 \leqslant 0.5d^{-1}$. Suppose therefore that $k \geqslant 2$.

Equations (23) and (24) show that $t_k = h_k - e_k + \sum_{i=1}^{k-1} e_{k-i}h_i$ and $0 < h_k < 1$. Thus Part (i) gives

$$t_k - h_k \leqslant -e_k + \sum_{i=1}^{k-1}\frac{e_{k-i}}{2di} \leqslant \frac{2}{1+d}\left\{\gamma^k + \frac{1}{2d}\sum_{i=1}^{k-1}\frac{1}{i}\gamma^{k-i}\right\} \text{ for } k \geqslant 2$$

where $\gamma \leqslant 1.125(q^d-1)^{-1/2}$. Hence $dk\gamma \leqslant 1.125e^4(3^8-1)^{-1/2} < 0.759$.

Part (i) yields $(1-\gamma)^{-2} < 1.0295$. Hence, as in the proof of [**3**, Lemma 4.4],

$$t_k - h_k \leqslant \frac{2}{1+d}\left(\gamma^k + \frac{\gamma}{2d(k-1)(1-\gamma)^2}\right) < 3.577\gamma d^{-2}k^{-1}.$$

Since $3.577\gamma d^{-1} < 0.0065$ we have $t_k - h_k < 0.0065d^{-1}k^{-1}$ for $2 \leqslant k \leqslant e^{d/2}d^{-1}$. It is immediate from (24) that $dkh_k < 0.5$, so we conclude that $dkt_k = dk(t_k-h_k) + dkh_k < 0.5065$ for $2 \leqslant k \leqslant e^{d/2}d^{-1}$, as required. □

**9.4. Bounding the coefficients of $R_{\mathsf{U},b}(q,u)$ and $F_{\mathsf{U},b}(q,u)$.** Recall from Definitions 8.1 and 9.1 that $R_{\mathsf{U}}(q,u) = \sum_{n=0}^{\infty} r_{\mathsf{U}}(2n,q)u^n$ and $R_{\mathsf{U},b}(q,u) = \sum_{n=0}^{\infty} r_{\mathsf{U},b}(2n,q)u^n$. We now prove a lower bound on the coefficients $r_{\mathsf{U},b}(2n,q)$, provided that $n$ is not too large.

Lemma 9.8. *For all $b \geqslant 1$, $0 \ll R_{\mathsf{U}}(3,u) \ll R_{\mathsf{U}}(q,u)$ and $0 \ll R_{\mathsf{U},b}(3,u) \ll R_{\mathsf{U},b}(q,u)$. Furthermore, for $b \geqslant 2$, $R_{\mathsf{U},b-1}(3,u) \ll R_{\mathsf{U},b}(3,u)$.*

Proof. First we claim that $0 \ll G_{\mathsf{U},0}(3,u) \ll G_{\mathsf{U},0}(q,u)$. Recall (17). From Theorem 7.1 we find that $N^*(q^2,1) = 2$ and $N^\sim(q,1) = q+1$, and so

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

It is clear that $0 \ll (1 + \frac{u}{3+1})^{3-2} \ll (1 + \frac{u}{q+1})^{q-2}$, so consider next the $r$th term of the first infinite product. Since $\frac{1}{2}N^*(q^2,r) = A(q,r)$ counts certain polynomials over $\mathbb{F}_{q^2}$, it is an integer, and so it follows from Lemma 7.8(ii) and [**3**, Lemma 3.1] (with $N = \frac{1}{2}N^*(3^2,r)$, $M = \frac{1}{2}N^*(q^2,r)$, $a = (q^r-1)^{-1}$ and $b = (3^r-1)^{-1}$) 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 $r > 1$. Next consider the $r$th term of the second infinite product. As in the previous paragraph, from Lemma 7.8(iii) and [**3**, Lemma 3.1] we deduce that

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

The claim now follows by multiplying all of these terms together.

Now we claim that $0 \ll G_{\mathsf{U},b}(3,u) \ll G_{\mathsf{U},b}(q,u)$ for $b \geqslant 1$. This follows for all $m \geqslant 1$ from (18), Lemma 7.8(i) and [**3**, Lemma 3.1]:

$$\left(1 + \frac{u^{2m}}{3^{2m} - 1}\right)^{D(3,m)} \ll \left(1 + \frac{u^{2m}}{q^{2m} - 1}\right)^{D(q,m)}.$$

Now we prove the lemma. For the first two bounds on $R_{\mathsf{U}}(3,u)$ and $R_{\mathsf{U},b}(3,u)$, recall that $R_{\mathsf{U}}(q,u) = \prod_{b=0}^{\infty} G_{\mathsf{U},b}(q,u)$, and $R_{\mathsf{U},b}(q,u) = \prod_{k=0}^{b-1} G_{\mathsf{U},k}(q,u)$, so the results follow immediately from the bounds on $G_{\mathsf{U},b}(3,u)$.

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

Lemma 9.9. *Let $b \geqslant 3$ and $d = 2^b$. Then $r_{\mathsf{U},b}(2n,q) > 0.247$ for all $n \leqslant e^{d/2}$.*

Proof. The proof of this lemma is similar to that of [**3**, Lemma 4.5], so we indicate only the relevant earlier results. By Lemma 9.8, we may assume that $q = 3$. The values of $r_{\mathsf{U},3}(2n,3)$ for $1 \leqslant n < 24$ may be computed: they are all at least 0.25. Lemma 9.8 then shows that if $b \geqslant 3$ then $r_{\mathsf{U},b}(2n,3) \geqslant r_{\mathsf{U},3}(2n,3) \geqslant 0.25 > 0.247$ for all $n < 24$.

Hence, using Lemma 9.8, it suffices to show that $r_{\mathsf{U},b}(2n,3) > 0.247$ for each consecutive $b$, and $n$ in the range $3 \cdot 2^b \leqslant n \leqslant e^{2^{b-1}}$. Using (21) and (22), and setting $k_0 = \lfloor n/d \rfloor \geqslant 3$, we get $r_{\mathsf{U},b}(2n,3) = r_{\mathsf{U}}(2n,3) - \sum_{1 \leqslant k \leqslant k_0} r_{\mathsf{U}}(2(n-kd),3)t_k$.

Using Theorem 8.9 in place of [**3**, Lemma 4.1], we deduce that $r_{\mathsf{U}}(2n,3) > 0.3433$ for $n \geqslant d$; $r_{\mathsf{U}}(2(n-k_0d),3) \leqslant 1$; and $r_{\mathsf{U}}(2(n-kd),3) \leqslant 0.3795$ for $1 \leqslant k \leqslant k_0 - 1$. Since $kdt_k \leqslant 0.5065$ for all $k$ such that $dk \leqslant e^{d/2}$ by Lemma 9.7, we proceed as in the proof of [**3**, Lemma 4.5], but with $(0.3433, 0.5065, 0.3795)$ in place of $(0.4346, 1.02, 0.4543)$, to deduce that $r_{\mathsf{U},b}(2n,3) \geqslant 0.3433 - 0.5065 \cdot 0.3795/2 > 0.247$. $\square$

Finally, we find a lower bound for certain coefficients of $F_{\mathsf{U},b}(q,u)$. Setting $b \geqslant 3$, $d := 2^b \geqslant 8$, $U = u^d$ and $Q = q^d$, (20) becomes

$$F_{\mathsf{U},b}(q,u) = F_b(U) := \prod_{m \text{ odd}} \left(1 + \frac{U^m}{Q^m - 1}\right)^{\left\lceil \frac{1}{8} N(q^2, md/2) \right\rceil}.$$

Recall from Lemma 9.5(v) that $[u^n]F_{\mathsf{U},b}(q,u)\,|\mathrm{GU}_{2n}(q)|$ is a lower bound on the number of pairs $(t,y) \in \Delta_{\mathsf{U}}(2n,q)$ such that the 2-part of the order of each eigenvalue of $y$ is $2^{b-1}(q^2-1)_2$.

Lemma 9.10. *Assume $b \geqslant 3$, so $d = 2^b \geqslant 8$. Then for all $k$ such that $kd \leqslant e^{d/2}$*

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

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 $\lceil N(q,md)/4 \rceil$, and the bounds

$$\frac{N(q,md)}{4} \geqslant \frac{(q^{md} - 2q^{md})}{4md} \quad \text{and} \quad \frac{N(q,md)}{4} \geqslant \frac{0.956(q^{md}-1)}{4md}$$

are used. Our exponent is $N(q^2, md/2)/8$, and Lemma 7.2(i) gives

$$\frac{N(q^2,md/2)}{8} \geqslant \frac{2(q^{md} - 2q^{md})}{8md} \quad \text{and} \quad \frac{N(q^2,md/2)}{8} > \frac{2 \times 0.956(q^{md}-1)}{8md}$$

for $md/2 \geqslant 5$. 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

Definition 10.1. Suppose that $0 \leqslant \alpha < \beta \leqslant 1$, and let $J_{\mathsf{U}}(2m,q;\alpha,\beta)$ be the set of all $(t,y) \in \Delta_{\mathsf{U}}(2m,q)$ for which $\mathrm{inv}(y)$ is $(\alpha,\beta)$-balanced. Set

$$j_{\mathsf{U}}(2m,q;\alpha,\beta) := |J_{\mathsf{U}}(2m,q;\alpha,\beta)| \,/\, |\mathrm{GU}_{2m}(q)|\,. \tag{25}$$

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

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

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

Proof. If $c_y(X) \in \Pi_{\mathsf{U}}(2m,q)$ is the characteristic polynomial for $y$ and $c_y^-(X)$ is the polynomial as in Lemma 9.5, then by Lemma 9.5(iii), $\mathrm{inv}(y)$ has $(-1)$-eigenspace of dimension $\deg c_y^-(X)$, and so $\mathrm{inv}(y)$ is $(\alpha,\beta)$-balanced if and only if $2m(1-\beta) \leqslant \deg c_y^-(X) \leqslant 2m(1-\alpha)$. It follows from Lemma 9.5 that we may bound $j_{\mathsf{U}}(2m,q;\alpha,\beta)$ by summing the coefficients of $u^m z^\ell$ in the power series $R_{\mathsf{U},b}(q,u)F_{\mathsf{U},b}(q,uz)$, over $b > 1$, and over $\ell$ in the range $[m(1-\beta), m(1-\alpha)]$ (and we recall that non-zero summands in $F_{\mathsf{U},b}(q,uz) = \sum_{\ell\geqslant 0} f_{\mathsf{U},b}(2\ell,q)(uz)^\ell$ occur only if $2^b$ divides $\ell$). □

LEMMA 10.4. *Let $a, c$ be real with $0 < a < c$. Then*

$$\sum_{a\leqslant k\leqslant c,\, k\in\mathbb{Z}} \frac{1}{k} \geqslant \log\left(\frac{c}{a}\right) - \frac{1}{a}.$$

PROOF. The proof is similar to that of [**3**, Lemma 3.8], so we only sketch the details. Each non-negative integer $\ell$ satisfies $1/\ell \geqslant \int_\ell^{\ell+1} x^{-1}dx$. Set $\ell_0 := \lceil a\rceil$ and $\ell_1 := \lfloor c\rfloor$. The sum in question equals

$$\sum_{\ell=\ell_0}^{\ell_1} \frac{1}{\ell} \geqslant \int_{\ell_0}^{\ell_1+1} x^{-1}dx \geqslant \int_{\ell_0}^{c} x^{-1}dx = \log\left(\frac{c}{a}\right) - \log\left(\frac{\ell_0}{a}\right).$$

From $\ell_o/a < 1{+}1/a$ we deduce that $\log(\ell_0/a) < 1/a$, so the required inequality follows. □

LEMMA 10.5. *Let $b \geqslant 3$ and $d := 2^b$. Then for all $\alpha$ and $\beta$ with $0 \leqslant \alpha < \beta < 1$ and positive integers $m \leqslant e^{d/2}$,*

$$j_{\mathsf{U}}(2m,q;\alpha,\beta) \geqslant \frac{0.05228}{d}\left(\log\left(\frac{1-\alpha}{1-\beta}\right) - \frac{d}{m(1-\beta)}\right).$$

PROOF. We mimic the proof of [**3**, Lemma 5.1]. First we use Lemma 9.10 bounding $f_{\mathsf{U},b}(2dk,q) \geqslant 0.2117/dk$ in place of their Lemma 4.6. Next, we use Lemma 9.5(iv) to see that if $f_{\mathsf{U},b}(2n,q) \neq 0$ then $n = dk$ for some $k$. We let $s$ be the sum of the coefficients of $F_{\mathsf{U},b}(q,u)$ for terms with degrees between $m(1-\beta)$ and $m(1-\alpha)$. We then use Lemma 10.4, Lemma 9.9 and Lemma 10.3 to see that $j_{\mathsf{U}}(2m,q;\alpha,\beta) \geqslant 0.247\, s$, so the result follows. □

DEFINITION 10.6. Let

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

be the proportion of pairs in $K_{\mathsf{U},s} \times K_{\mathsf{U},s}$ which lie in $L_{\mathsf{U}}(n,s,q;\alpha,\beta)$ (as in Definition 3.3).

We define

$$\varphi_{\mathsf{U}}(m,z) = \prod_{i=1}^{m}(1-(-1)^i z^{-i}),\ \text{for } z>1 \text{ and } m\in\mathbb{N} \tag{26}$$

and note that $|\mathrm{GU}_m(q)| = q^{m^2}\varphi_{\mathsf{U}}(m,q)$.

LEMMA 10.7. *Let $2n/3 \geqslant s \geqslant n/2 \geqslant 2$, let $j_{\mathsf{U}}(2n-2s,q;\alpha,\beta)$ be as in (25), and let*

$$\theta(n,s,q) = \frac{\varphi_{\mathsf{U}}(n-s,q)^2\varphi_{\mathsf{U}}(s,q)^2}{\varphi_{\mathsf{U}}(n,q)\varphi_{\mathsf{U}}(2s-n,q)}.$$

*Then $\ell_{\mathsf{U}}(n,s,q;\alpha,\beta) = \theta(n,s,q)j_{\mathsf{U}}(2n-2s,q;\alpha,\beta)$, and $\theta(n,s,q) > \frac{81}{98}$.*

PROOF. For the main claim, we mimic the proof of [**3**, Lemma 5.3], but modify to count decompositions into non-degenerate unitary subspaces. Let $h := 2s - n$, and let $\Omega_{\mathsf{U}}$ be the set of pairs $(V_1, V_2)$ of non-degenerate subspaces of $V$, of dimensions $h, n-h$ respectively, such that $V_1^{\perp} = V_2$. Then for each $(V_1, V_2) \in \Omega_{\mathsf{U}}$, and each $(t_2, y_2) \in \Delta_{\mathsf{U}}(n-h, q)$ acting on $V_2$ such that $\mathrm{inv}(y_2)$ is $(\alpha, \beta)$-balanced, there is (see Lemma 2.9) a unique pair $(t, t')$ of involutions in $\mathrm{GU}_n(q)$ such that $t_{|V_2} = t_2$, $t'_{|V_2} = t_2 y_2$, and $t_{|V_1} = t'_{|V_1} = I$. It follows from Definition 3.3 and [**3**, Lemma 2.2] that $(t, t') \in L_{\mathsf{U}}(n, s, q; \alpha, \beta)$.

Conversely, for each $(t, t') \in L_{\mathsf{U}}(n, s, q; \alpha, \beta)$, relative to $V_1, V_2$ as in Definition 3.3, the pair $(t_{|V_2}, tt'_{|V_2}) \in \Delta_{\mathsf{U}}(n-h, q)$. Thus by (25) and Definition 10.6, we conclude that

$$\ell_{\mathsf{U}}(n, s, q; \alpha, \beta) = |\Omega_{\mathsf{U}}|\, |\mathrm{GU}_{n-h}(q)|\, j_{\mathsf{U}}(n-h, q; \alpha, \beta) / |K_{\mathsf{U},s}|^2 .$$

Using the obvious expressions for $|\Omega_{\mathsf{U}}|$ and $|K_{\mathsf{U},s}|$, and recalling from (26) that $|\mathrm{GU}_n(q)| = q^{n^2}\varphi_{\mathsf{U}}(n, q)$, we obtain the expression for $\theta(n, s, q)$ given in the statement.

To prove that $\theta(n, s, q) > 81/98$, we use [**13**]. For $1 \leqslant k \leqslant n, 1 \leqslant r < n$, 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 $2s - n \leqslant n/3$ by assumption), $\theta(n, s, q) = \Omega(2s-n+1, n; -q)/\Delta(s, n; -q)^2$. 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 $1 - q^{-2s+n-1} \geqslant 8/9$ if $n$ is odd. Hence $\theta(n, s, q) > \left(\frac{27}{28}\right)^2 \left(\frac{8}{9}\right)$. □

PROOF OF THEOREM 1. We shall prove this theorem first for uniformly distributed random elements of $\mathrm{GU}_n(q)$, then generalise to nearly uniformly distributed elements.

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

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

If we choose $\alpha$ and $\beta$ as in Lemma 3.5, we see from Lemma 3.5(ii) that the restriction of $\mathrm{inv}(tt')$ to $E_+(t)$ is $(1/3, 2/3)$-balanced whenever $(t, t') \in L_{\mathsf{U}}(n, s, q; \alpha, \beta)$. It is immediate from Definition 10.6 that $\pi_+ \geqslant \ell_{\mathsf{U}}(n, s, q; \alpha, \beta)$.

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

$$(27)\qquad j_{\mathsf{U}}(2(n-s),q;\alpha,\beta) \geqslant \frac{0.05228}{d}\left(\log\left(\frac{1-\alpha}{1-\beta}\right) - \frac{d}{(n-s)(1-\beta)}\right).$$

Using the definitions of $\alpha$ and $\beta$ from Lemma 3.5, we first deduce that

$$(n-s)(1-\beta) = (n-s)\frac{s}{3(n-s)} = \frac{s}{3} \geqslant \frac{n}{6}$$

so that $1/((n-s)(1-\beta)) \leqslant 6/n$. We also see that

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

which implies that $\log((1-\alpha)/(1-\beta)) \geqslant \log 3/2 > 0.4054$. Substituting into (27) we get

$$j_{\mathsf{U}}(2(n-s),q;\alpha,\beta) \geqslant 0.05228 d^{-1}(0.4054 - 6d/n) = 0.05228\,(0.4054/d - 6/n),$$

so let $\zeta_1(n,d) = 0.05228\,(0.4054/d - 6/n)$. Elementary calculus shows that $\zeta_1(n,d)\log n$ increases with $n$, for fixed $d > 0$ and $n \geqslant 3$. First consider $b = 4$ (so $54 = \lfloor e^4 \rfloor < n \leqslant 2980 = \lfloor e^8 \rfloor$). Since $\zeta_1(250,16)\log 250 > 0.0003$, we have $\zeta_1(n,16)\log n > 0.0003$ for all $n \geqslant 250$. Conversely, when $b \geqslant 5$, $d := 2^b$ and $e^{d/4} < n \leqslant e^{d/2}$,

$$d/n < e^{-d/4}d \leqslant 32e^{-8} < 0.01074 \text{ and } \log n > d/4.$$

Thus

$$\zeta_1(n,d)\log n > 0.05228d^{-1}\cdot(0.4054 - 6\cdot 0.01074)\cdot d/4 > 0.0044$$

in this case. Hence $j_{\mathsf{U}}(2(n-s),q;\alpha,\beta) > 0.0003/(\log n)$ holds for all $n \geqslant 250$. Finally, applying Lemma 10.7, for all $n \geqslant 150$

$$\begin{aligned}\pi_+ \geqslant \ell_{\mathsf{U}}(n,s,q;\alpha,\beta) &= \theta(n,s,q)j_{\mathsf{U}}(n-h,q,\alpha,\beta)\\ &> (81/98)\times 0.0003/\log n > 0.0002/\log n.\end{aligned}$$

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

The proof of Part (ii) is similar. We take $\alpha = 1/3$ and $\beta = 2/3$ since Lemma 3.5 (ii) shows that $z_{|V_2}$ is of type $(2k_+, 2k_-)$ and $z_{|E_-(t)}$ is of type $(k_+, k_-)$ so the former is strong exactly when the latter is. We make a similar estimate using Lemma 10.5 for $j_{\mathsf{U}}(2(n-s),q;1/3,2/3)$ (noting that now $1/((n-s)(1-\beta)) = 3/(n-s) \leqslant 9/n$). This shows that, for all $n \geqslant 250$, and $d$ chosen as the power of 2 such that $e^{d/4} < n \leqslant e^{d/2}$

$$j_{\mathsf{U}}(2(n-s),q;1/3,2/3) \geqslant 0.05228d^{-1}(\log 2 - 9d/n) = \zeta_2(n,d), \text{ say.}$$

We calculate that $\zeta_2(250,16)\log 250 > 0.00211$ and hence $\zeta_2(n,16)\log n > 0.00211$ for $n \geqslant 250$. Furthermore an argument similar to the one above shows that if $b \geqslant 5$ and $e^{d/4} \leqslant n \leqslant e^{d/2}$ then

$$\zeta_2(n,d)\log n > \frac{0.05228}{d}(\log 2 - 9\times 0.01074)\frac{d}{4} > 0.0077.$$

Hence for all $n \geqslant 250$, we get $j_{\mathsf{U}}(2(n-s),q;1/3,2/3) > 0.00211/\log n$ and so

$$\pi_- \geqslant \ell_{\mathsf{U}}(n,s,q;1/3,2/3) > (81/98)0.00211/\log n > 0.00174/\log n.$$

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

For nearly uniformly distributed random elements $g$ of $G$, let $\pi_+$ be the probability that the restriction of $\mathrm{inv}(tt^g)$ to $E_+(t)$ is $(1/3, 2/3)$-balanced. It follows from Definition 1.2 that $\pi_+ > \ell_{\mathsf{U}}(n, s, q; \alpha, \beta)/2$. The rest of the proof follows as before, but the final value of $\kappa$ is halved. The argument for $\pi_-$ is similar. ☐

## 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 $Y$ be the results of three independent trials. Then $\mathbb{P}(g \in Y) \geqslant 1/|G|$ for all $g \in G$.*

PROOF. The result is trivially true if $|G| = 1$. Suppose now that $|G| \geqslant 2$. By definition of nearly uniform, $\mathbb{P}(X = g) > \rho$ where $\rho = 1/(2|G|)$. Then

$$\mathbb{P}(g \notin Y) = (1 - \mathbb{P}(X = g))^3 < (1 - \rho)^3 \text{ so } \mathbb{P}(g \in Y) > 3\rho - 3\rho^2 + \rho^3 = 2\rho + \rho\left(1 - 3\rho + \rho^2\right).$$

However, $0 < \rho < (3 - \sqrt{5})/2$ as $|G| \geqslant 2$, so $1 - 3\rho + \rho^2 > 0$ and $\mathbb{P}(g \in Y) > 2\rho = 1/|G|$. ☐

DEFINITION 11.2. (See [**13**]). Let $H$ be a group, and let $\mathcal{H} = (\mathcal{C}_1, \ldots, \mathcal{C}_c)$ be a sequence of conjugacy classes of $H$. 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 $\mathcal{C}_i$ for all $i$, and the $h_i$ are independent.

PROOF OF THEOREM 2. By Lemma 11.1, it suffices to prove the theorem for uniform random elements. We first consider $G = \mathrm{GU}_n(q)$, and address $\mathrm{GL}_n(q)$ at the end.

Let $V_\varepsilon = E_\varepsilon(t)$ for $\varepsilon \in \{+, -\}$. We construct involutions $\mathrm{inv}(tt^g)$ which have determinant 1 and hence lie in $\mathrm{SU}_n(q)$. However their restrictions $\mathrm{inv}(tt^g)|_{V_\varepsilon}$ are guaranteed to lie only in the subgroup $\mathrm{SU}(V_\varepsilon).2$ of $\mathrm{GU}(V_\varepsilon)$ consisting of elements with determinant $\pm 1$.

We shall now choose an $n_1$, as in the statement of the theorem, and then show that the result holds for all $n \geqslant n_1$. Let $\kappa$ and $n_0$ be as in Theorem 1. In [**13**, Theorem 1.1] it is shown that there exist constants $c$ and $n_2$ such that for $\ell \geqslant n_2$ and for every sequence $\mathcal{H}$ of $c$ conjugacy classes of strong involutions of $\mathrm{SU}_\ell(q).2$, a class-random sequence from $\mathcal{H}$ generates a group containing $\mathrm{SU}_\ell(q)$ with probability at least $1 - q^{-\ell}$. We let $n_1 = \max\{3n_2, n_0\}$.

By Theorem 1, since $n \geqslant n_1 \geqslant n_0$, the probability that a sequence of $N = \lceil \kappa^{-1} \log n \rceil$ random elements $g$ do not produce at least one strong involution $\mathrm{inv}(tt^g)|_{V_+}$ and at least one strong involution $\mathrm{inv}(tt^g)|_{V_-}$ is at most

$$\left(1 - \frac{\kappa}{\log n}\right)^N \leqslant \left(1 - \frac{1}{N}\right)^N < e^{-1}.$$

Let $m \in \mathbb{Z}$. Then the probability that $mN$ random elements $g$ do not produce at least one strong involution $\mathrm{inv}(tt^g)|_{V_+}$ and at least one strong involution $\mathrm{inv}(tt^g)|_{V_-}$ is at most $e^{-m} \leqslant (3/8)^m$. This can be made as small as required, by choosing $m$ sufficiently large. Furthermore, each such strong involution $\mathrm{inv}(tt^g)|_{V_\varepsilon}$ is class-random in $\mathrm{SU}(V_\varepsilon).2$.

We now define the sequence $A$ and constant $\lambda$ from the statement of the theorem. The sequence $A$ will be thought of as the concatenation of three disjoint subsequences, $A_+$, $A_-$ and $B$, and will have total length $\lceil \lambda \log n \rceil$. The constant $\lambda > 0$ is chosen such that, with (combined) probability at least 0.9, all of the following three independent events occur: (i) the subsequence $A_+$ contains at least $c$ elements $g$ such that $\mathrm{inv}(tt^g)|_{V_+}$ is a strong involution; (ii) the subsequence $A_-$ contains at least $c$ elements $g$ such that $\mathrm{inv}(tt^g)|_{V_-}$ is a strong involution; (iii) the subsequence $B$ contains at least one $g \in G$ such that $z = \mathrm{inv}(tt^g)$ is an additional strong involution on $V_+$. Assume now that all three of these events occur.

Let $s = \dim(V_+)$, so that $\dim(V_-) = n - s$. Let $K_1 = \langle \mathrm{inv}(tt^g) \mid g \in A_+ \rangle$, and $K_2 = \langle \mathrm{inv}(tt^g) \mid g \in A_- \rangle$. Set $K = \langle K_1, K_2 \rangle$ and $H = \langle \mathrm{inv}(tt^g) \mid g \in A \rangle$, so that

$$K \leqslant H \leqslant (\mathrm{SU}_s(q) \times \mathrm{SU}_{n-s}(q)) .2 \leqslant C_{\mathrm{GU}_n(q)}(t)$$

where $(\mathrm{SU}_s(q) \times \mathrm{SU}_{n-s}(q)).2 = \mathrm{SU}_n(q) \cap (\mathrm{SU}_s(q).2 \times \mathrm{SU}_{n-s}(q).2)$.

Since $t$ is a strong involution in $\mathrm{GU}_n(q)$, and $n \geqslant n_1 \geqslant 3n_2$, both $\dim(V_+) = s \geqslant n/3 \geqslant n_2$ and $\dim(V_-) = n - s \geqslant n/3 \geqslant n_2$. It therefore follows from [**13**, Theorem 1.1] that $\mathbb{P}(K_1|_{V_+}$ contains $\mathrm{SU}(V_+)) \geqslant 1 - q^{-s}$, and independently $\mathbb{P}(K_2|_{V_-}$ contains $\mathrm{SU}(V_-)) \geqslant 1 - q^{-(n-s)}$. Hence the probability that both $K|_{V_+} \geqslant \mathrm{SU}(V_+)$ and $K|_{V_-} \geqslant \mathrm{SU}(V_-)$ is at least $(1-q^{-s})(1-q^{-(n-s)})$, and since this expression is increasing as $s$ goes from $n/3$ to $n/2$, this probability is at least $1-q^{-n/3}-q^{-2n/3}+q^{-n}$. Suppose then that both $K|_{V_+} \geqslant \mathrm{SU}(V_+)$ and $K|_{V_-} \geqslant \mathrm{SU}(V_-)$.

If $s \neq n/2$ then every subdirect subgroup of $\mathrm{SU}_s(q)\times\mathrm{SU}_{n-s}(q)$ is the full direct product, and therefore $K$, and hence also $H$, contains $\mathrm{SU}_s(q)\times\mathrm{SU}_{n-s}(q)$. Suppose now that $s = n/2$. We show that, with high probability, in this case also $H$ contains $\mathrm{SU}_{n/2}(q) \times \mathrm{SU}_{n/2}(q)$. Suppose that $K$ does not contain $\mathrm{SU}_{n/2}(q) \times \mathrm{SU}_{n/2}(q)$. Then $K \cong K|_{V_\varepsilon} \cong \mathrm{SU}_{n/2}(q)$ or $\mathrm{SU}_{n/2}(q).2$, and $K$ is a diagonal subgroup of $K|_{V_+} \times K|_{V_-}$, with isomorphism $\phi : K|_{V_+} \to K|_{V_-}$.

Recall the element $z$ defined by the final subsequence $B$ of $A$. Let $z_+ = z|_{V_+}$ and $z_- = z|_{V_-}$, so that $z_+$ is a strong involution on $V_+$, with 1-eigenspace of dimension $a$ and $(-1)$-eigenspace of dimension $b$, where $(1/3)(n/2) \leqslant a \leqslant (2/3)(n/2)$ and $a+b = n/2$. If $H$ is also a diagonal subgroup of $H|_{V_+} \times H|_{V_-}$ then $\phi$ naturally extends to $H|_{V_+}$, and $\phi(z_+) = z_-$. Hence $z_-$ acting on $V_-$ also has $(\pm 1)$-eigenspaces of dimensions $a, b$, respectively. As we noted in the Introduction, $z$ is a uniformly distributed random element of its conjugacy class $\mathcal{C}$ in $C_G(t) = C_{\mathrm{GU}_n(q)}(t)$, and the members of $\mathcal{C}$ are elements $z'$ such that $z'|_{V_+}$, $z'|_{V_-}$ are $\mathrm{GU}_{n/2}(q)$-conjugate to $z_+, z_-$ respectively. In particular, for a given $z_+ = z|_{V_+}$, each element of the $\mathrm{GU}_{n/2}(q)$-conjugacy class of $z_-$ would occur as $z|_{V_-}$ with equal probability (which we show is very small). Using [**13**, Table 4], the $\mathrm{GU}_{n/2}(q)$-conjugacy class of $z_-$ has size

$$\frac{|\mathrm{GU}_{n/2}(q)|}{|\mathrm{GU}_a(q) \times \mathrm{GU}_b(q)|} \geqslant \frac{9}{16} q^{(n/2)^2 - a^2 - b^2} = \frac{9}{16} q^{2ab} \geqslant \frac{9}{16} q^{n^2/9}.$$

Hence $\mathbb{P}(z|_{V_-} = \phi(z_+)) < (16/9)q^{-n^2/9}$. Drawing everything together, $\mathbb{P}(H$ contains $\mathrm{SU}_{n/2}(q) \times \mathrm{SU}_{n/2}(q))$ is greater than

$$0.9(1 - q^{-n/3} - q^{-2n/3} + q^{-n})(1 - \frac{16}{9}q^{-n^2/9}) > 0.9(1 - q^{-n/3} - q^{-2n/3})$$

where we increase $n_1$ if necessary so that the final inequality holds.

For $\mathrm{GL}_n(q)$, [**3**, Theorem 1.1] states a similar result to our Theorem 1 for uniformly distributed random elements. An argument identical to the final paragraph of our proof of Theorem 1 upgrades [**3**, Theorem 1.1] to nearly uniformly random elements, and then the remainder of the proof is identical, but with linear groups in place of unitary groups. □

Proof of Theorem 3. By [**9**, Theorem 1.1], there exists an absolute constant $c$ such that $\mathbb{P}(g$ powers to a strong involution$) \geqslant c/\log n$, for $g$ a uniformly distributed random element of $G$. So there exists a constant $\delta_1$ such that $\delta_1 \log n$ independent uniform random elements suffice to produce such a strong involution $t$ with probability at least 0.89/0.9. We first run this random process to produce such a $t$.

For $n \geqslant n_1$, we now apply Theorem 2, with this known strong involution $t$, to see that a further $\lambda \log n$ random elements of $G$ will suffice to produce generators for a subgroup of $C_G(t)$ that contains the last term, $C_G(t)^\infty$, in the derived series of $C_G(t)$. This step succeeds with probability at least $0.9(1 - q^{-n/3} - q^{-2n/3})$. Thus we set $\mu_1 = \delta_1 + \lambda$, to get that the overall probability of success in this case is at least $(0.89/0.9) \cdot 0.9(1 - q^{-n/3} - q^{-2n/3})$.

Assume instead therefore that $n < n_1$. By [**12**, Theorem 2], there is a positive constant $a$ such that if $t_1$ is any involution in $G$, then the proportion of ordered pairs $(t_1, t_1^g)$ such that $t_1 t_1^g$ has odd order is bounded below by $an^{-1}$. We set $t_1$ to be our known strong involution $t$. 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**, Theorem 3.1]). Since the probability that two random elements of $S = \mathrm{SL}_m(q)$ or $\mathrm{SU}_m(q)$ generate $S$ is greater than 1/2 (see [**10**, Theorem 1.1]), reasoning as in the case $n \geqslant n_1$, there is a constant $\delta_2$ such that if $A$ is a sequence of $\delta_2 \log n$ uniformly distributed random elements $g \in G$ then the probability that $\langle R(g,t) \mid g \in A\rangle$ contains $C_G(t)^\infty$ is greater than $0.9(1 - q^{-n/3} - q^{2n/3})$. We therefore may set $\mu_2 = \delta_1 + \delta_2$ to get that the overall probability of success in this case is at least $0.89(1 - q^{-n/3} - q^{2n/3})$.

Finally, we set $\mu = \max\{\mu_1, \mu_2\}$, and the result follows. □

**11.2. Proof of Theorem 5.** The proof of the following lemma is similar to that of [**14**, Lemma 4.1(b)]. We assume that the Gram matrix of the unitary form is the identity matrix. Recall (26). We let $\varphi_{\mathsf{U}}(z) = \lim_{m\to\infty} \varphi_{\mathsf{U}}(m,z)$, and define $\varphi_{\mathsf{U}}(0,z) = 1$.

Lemma 11.3. *Let $\Phi_{\mathsf{U}}(m,q) = \varphi_{\mathsf{U}}(m,q)^4/\varphi_{\mathsf{U}}(2m,q)$. Then for $m \geqslant 1$, $\iota_{\mathsf{U}}(2m,q)$ equals $r_{\mathsf{U}}(2m,q)\Phi_{\mathsf{U}}(m,q)$, and*

$$\iota_{\mathsf{U}}(2m+1,q) = \iota_{\mathsf{U}}(2m,q)\frac{(1-(-1)^{m+1}q^{-m-1})^2}{(1+q^{-2m-1})(1+q^{-1})} = r_{\mathsf{U}}(2m,q)\frac{\varphi_{\mathsf{U}}(m,q)^2\varphi_{\mathsf{U}}(m+1,q)^2}{(1+1/q)\varphi_{\mathsf{U}}(2m+1,q)}.$$

Proof. First let $n = 2m$ be even, and let $x \in \mathcal{C}_{\mathsf{U}}(V)$ (see Definition 1.4). Then $|\mathcal{C}_{\mathsf{U}}(V)| = |\mathrm{GU}_{2m}(q)| \cdot |\mathrm{GU}_m(q)|^{-2}$. Hence, by (1),

$$\begin{aligned}
\iota_{\mathsf{U}}(2m,q) &= \frac{|\mathbf{I}_{\mathsf{U}}(V)|}{|\mathcal{C}_{\mathsf{U}}(V)|^2} = \frac{|\Delta_{\mathsf{U}}(V)|}{|\mathcal{C}_{\mathsf{U}}(V)|^2} \qquad \text{(by Lemma 2.9)}\\
&= |\Delta_{\mathsf{U}}(V)|\frac{|\mathrm{GU}_m(q)|^4}{|\mathrm{GU}_{2m}(q)|^2} = r_{\mathsf{U}}(2m,q)\frac{|\mathrm{GU}_m(q)|^4}{|\mathrm{GU}_{2m}(q)|} \qquad \text{(by Definition 8.1)}\\
&= r_{\mathsf{U}}(2m,q)\frac{\left(q^{m^2}\varphi_{\mathsf{U}}(m,q)\right)^4}{q^{4m^2}\varphi_{\mathsf{U}}(2m,q)} = r_{\mathsf{U}}(2m,q)\frac{\varphi_{\mathsf{U}}(m,q)^4}{\varphi_{\mathsf{U}}(2m,q)}\\
&= r_{\mathsf{U}}(2m,q)\Phi_{\mathsf{U}}(m,q).
\end{aligned}$$

Now let $n = 2m+1$ be odd. Then $|\mathcal{C}_{\mathsf{U}}(V)| = |\mathrm{GU}_{2m+1}(q)|/(|\mathrm{GU}_m(q)|\cdot|\mathrm{GU}_{m+1}(q)|)$. Let $(x,x') \in \mathbf{I}_{\mathsf{U}}(V)$, 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 negate 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 (9), which we can write as $V = V_0 \perp V_\pm$, where $V_0$ is the sum of the $V_f$ for $f$ of Type 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, $x_0, y_0 \in \mathrm{GU}(V_0)$ and so in particular $(x_0,y_0) \in \Delta_{\mathsf{U}}(V_0)$.

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 $x = -I_{V_\pm} \oplus x_0$; and (ii) $y$ fixes $V_\pm$, so $y = I_{V_\pm} \oplus y_0$.

Thus $|\mathbf{I}_{\mathsf{U}}(V)|$ is equal to $|\Delta_{\mathsf{U}}(V_0)| = |\Delta_{\mathsf{U}}(2m,q)|$ times the number of decompositions of $V$ as an orthogonal direct sum of a non-degenerate $2m$-space and a non-degenerate 1-space. The orbit-stabiliser theorem then yields

$$\begin{aligned}
\iota_{\mathsf{U}}(2m+1,q) &= \frac{|\mathbf{I}_{\mathsf{U}}(V)|}{|\mathcal{C}(V)|^2} = \frac{|\mathrm{GU}_{2m+1}(q)|}{|\mathrm{GU}_1(q)|\cdot|\mathrm{GU}_{2m}(q)|}|\Delta_{\mathsf{U}}(2m,q)| \cdot \frac{|\mathrm{GU}_m(q)|^2\cdot|\mathrm{GU}_{m+1}(q)|^2}{|\mathrm{GU}_{2m+1}(q)|^2}\\
&= r_{\mathsf{U}}(2m,q)\cdot\frac{|\mathrm{GU}_m(q)|^2\cdot|\mathrm{GU}_{m+1}(q)|^2}{(q+1)|\mathrm{GU}_{2m+1}(q)|}\\
&= r_{\mathsf{U}}(2m,q)\cdot\frac{\left(q^{m^2}\varphi_{\mathsf{U}}(m,q)\right)^2\cdot\left(q^{(m+1)^2}\varphi_{\mathsf{U}}(m+1,q)\right)^2}{(q+1)q^{(2m+1)^2}\varphi_{\mathsf{U}}(2m+1,q)}\\
&= r_{\mathsf{U}}(2m,q)\cdot\frac{\varphi_{\mathsf{U}}(m,q)^2\varphi_{\mathsf{U}}(m+1,q)^2}{(1+1/q)\varphi_{\mathsf{U}}(2m+1,q)}\\
&= \iota_{\mathsf{U}}(2m,q)\cdot\frac{\varphi_{\mathsf{U}}(2m,q)}{\varphi_{\mathsf{U}}(m,q)^4}\cdot\frac{\varphi_{\mathsf{U}}(m,q)^2\varphi_{\mathsf{U}}(m+1,q)^2}{(1+1/q)\varphi_{\mathsf{U}}(2m+1,q)}\\
&= \iota_{\mathsf{U}}(2m,q)\cdot\frac{(1-(-1)^{m+1}q^{-m-1})^2}{(1+q^{-2m-1})(1+q^{-1})} \qquad \text{as required.} \qquad \square
\end{aligned}$$

Theorem 8.3 showed that $r_{\mathsf{U}}(\infty,q) := \lim_{m\to\infty} r_{\mathsf{U}}(2m,q)$ exists.

Corollary 11.4. *The limits as $m \to \infty$ of $\iota_{\mathsf{U}}(2m,q)$ and $\iota_{\mathsf{U}}(2m+1,q)$ satisfy*

$$\lim_{m\to\infty} \iota_{\mathsf{U}}(2m,q) = r_{\mathsf{U}}(\infty,q)\cdot\varphi_{\mathsf{U}}(q)^3, \qquad \lim_{m\to\infty} \iota_{\mathsf{U}}(2m+1,q) = r_{\mathsf{U}}(\infty,q)\cdot\varphi_{\mathsf{U}}(q)^3/(1+q^{-1}).$$

Proof of Theorem 5. By Lemma 9.8, $r_{\mathsf{U}}(2m,q) \geqslant r_{\mathsf{U}}(2m,3)$. Hence by Theorem 8.9, $r_{\mathsf{U}}(2m,q) \geqslant 0.3433$ for $m \geqslant 2$, whilst $r_{\mathsf{U}}(2,q) \geqslant 0.25$.

We first claim that for $m \geqslant 1$,

$$\Phi_{\mathsf{U}}(m,q) = \frac{\varphi(m,q)^4}{\varphi(2m,q)} > 1$$

To see this, first note that

$$\Phi_{\mathsf{U}}(1,q) = \frac{(1+q^{-1})^4}{(1+q^{-1})(1-q^{-2})} = \frac{(1+q^{-1})^2}{(1-q^{-1})} > 1.$$

Similarly, for $m = 2$,

$$\Phi_{\mathsf{U}}(2,q) = \frac{(1+q^{-1})^4(1-q^{-2})^4}{(1+q^{-1})(1-q^{-2})(1+q^{-3})(1-q^{-4})} = \frac{(1+q^{-1})^2(1-q^{-2})^2}{(1-q^{-1}+q^{-2})(1+q^{-2})} > 1$$

since $(1+q^{-1})^2 > 1+q^{-2}$ and $(1-q^{-2})^2 > 1-q^{-1}+q^{-2}$ for $q \geqslant 3$. So assume that $m \geqslant 3$. If $m$ is odd then an easy calculation shows that

$$\Phi_{\mathsf{U}}(m,q) = \Phi_{\mathsf{U}}(m-1,q)\cdot\frac{(1+q^{-m})^4}{(1+q^{-2m+1})(1-q^{-2m})} > \Phi_{\mathsf{U}}(m-1,q).$$

Thus it is sufficient to prove that $\Phi_{\mathsf{U}}(m,q) \geqslant \Phi_{\mathsf{U}}(m-2,q)$ for even $m \geqslant 4$: from this we shall conclude that, for $m \geqslant 2$, $\Phi_{\mathsf{U}}(m,q) \geqslant \Phi_{\mathsf{U}}(2,q) > 1$. For $m \geqslant 4$ even,

$$\Phi_{\mathsf{U}}(m,q) = \Phi_{\mathsf{U}}(m-2,q)\cdot\frac{(1+q^{-m+1})^4(1-q^{-m})^4}{(1+q^{-2m+3})(1-q^{-2m+2})(1+q^{-2m+1})(1-q^{-2m})}.$$

The largest of the four terms in the denominator is $1+q^{-2m+3} < (1+q^{-m+1})(1-q^{-m})$. Thus $\Phi_{\mathsf{U}}(m,q) > \Phi_{\mathsf{U}}(m-2,q)$, and the claim is proved.

Hence by Lemma 11.3 we find that $\iota_{\mathsf{U}}(2m,q) > r_{\mathsf{U}}(2m,q) \geqslant 0.3433$ for $m \geqslant 2$, whilst $\iota(2,q) > r_{\mathsf{U}}(2,q) \geqslant 0.25$. This concludes the arguments for even dimension.

Let

$$\delta(m,q) = \frac{(1-(-q)^{-m-1})^2}{(1+q^{-2m-1})(1+q^{-1})}.$$

Then $\delta(1,q) > 1-q^{-1}-q^{-2}$, and $\delta(1,3) = 4/7$. For $q \geqslant 5$ our bound shows that $\delta(1,q) > 19/25 > 4/7$, so $\delta(1,q) > 4/7$ for all $q$. If $m \geqslant 2$ then performing the division shows that $\delta(m,q) > 1-q^{-1}+q^{-2}-q^{-3} \geqslant 20/27$. The result for $\iota(2m+1,q)$ follows from Lemma 11.3 and our bounds for $\iota(2m,q)$. □

## References


[1] László Babai, Simon Guest, Cheryl E. Praeger, and Robert A. Wilson, *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, 45

[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. ↑2, 3, 8, 10, 21, 29, 32, 36, 37, 38, 39, 40, 41, 45

[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. ↑9, 20, 21, 27, 28, 36

[5] B. Huppert, *Endliche Gruppen. I*, Die Grundlehren der Mathematischen Wissenschaften, Band 134, Springer-Verlag, Berlin-New York, 1967 (German). ↑11, 13, 15

[6] Irving Kaplansky, *Linear Algebra and Geometry: A Second Course*, 2nd edition, Chelsea Publishing Company, New York, 1974. ↑12

[7] C.R. Leedham-Green and E.A. O'Brien, *Constructive recognition of classical groups in odd characteristic*, J. Algebra **322** (2009), 833–881. ↑2, 3

[8] Martin W. Liebeck and E. A. O'Brien, *Finding the characteristic of a group of Lie type*, J. Lond. Math. Soc. (2) **75** (2007), no. 3, 741–754. ↑2

[9] Frank Lübeck, Alice C. Niemeyer, and Cheryl E. Praeger, *Finding involutions in finite Lie type groups of odd characteristic*, J. Algebra **321** (2009), no. 11, 3397–3417. ↑3, 45

[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. ↑45

[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. ↑12, 15

[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. ↑1, 2, 45

[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. ↑41, 43, 44

[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. ↑2, 3, 5, 6, 21, 45, 46

[15] A. Voss, *Zur Theorie der orthogonalen Substitutionen*, Math. Ann. **13** (1878), 320–374. ↑12

[16] G. E. Wall, *On the conjugacy classes in the unitary, symplectic and orthogonal groups*, J. Austral. Math. Soc. **3** (1963), 1–62. ↑4


S.P. Glasby & Cheryl E. Praeger: Department of Mathematics and Statistics, UWA, Perth, WA 6009, Australia

Colva M. Roney-Dougal: Mathematical Institute, Univ. St Andrews, KY16 9SS, UK