PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 140, Number 9, September 2012, Pages 3003–3015
S 0002-9939(2012)11491-1
Article electronically published on January 25, 2012

REGULAR SEMISIMPLE ELEMENTS AND INVOLUTIONS IN FINITE GENERAL LINEAR GROUPS OF ODD CHARACTERISTIC

CHERYL E. PRAEGER AND ÁKOS SERESS

(Communicated by Pham Huu Tiep)

Abstract. Chris Parker and Rob Wilson showed that involution-centraliser methods could be used for solving several problems that appeared to be computationally hard and gave complexity analyses for methods to construct involutions and their centralisers in quasisimple Lie type groups in odd characteristic. Crucial to their analyses are conjugate involution pairs whose products are regular semisimple, possibly in an induced action on a subspace. We consider the fundamental case of conjugate involution pairs, in finite general linear groups $\mathrm{GL}(n,q)$ with q odd, for which the product is regular semisimple on the underlying vector space. Such involutions form essentially a single conjugacy class $\mathcal{C}$. We prove that a constant proportion of pairs from $\mathcal{C}$ have regular semisimple product. Moreover we show that for a fixed parity of n, this proportion converges exponentially quickly to a limit, as n approaches ∞, the limit being $(1-q^{-1})^2\Phi(q)^3$ for even n and $(1-q^{-1})\Phi(q)^3$ for odd n, where $\Phi(q)=\prod_{i=1}^{\infty}(1-q^{-i})$.

1. Introduction

An $n\times n$ matrix y over a finite field $\mathbb{F}_q$ of order q is said to be *regular semisimple* if its characteristic polynomial $c_y(t)$ is multiplicity-free, that is, not divisible by the square of any irreducible polynomial. Regular semisimple matrices are central to analyses in [1, 13] of algorithms for computing with finite groups of Lie type, which in turn underpin new recognition algorithms in [9] for finite classical groups over fields of odd order q. Each of these analyses involves estimating the number of pairs (x,x') of involutions, that is, non-identity matrices with $x^2=(x')^2=1$, such that $y:=xx'$ is regular semisimple, possibly in an induced action on a subspace, and often with other conditions imposed. Usually in these applications the involution x' is a random conjugate of an already constructed involution x, and we wish to know the probability that the product $y:=xx'$ is regular semisimple. We make a few more brief background comments in Subsection 1.1.

We consider here the basic case where the regular semisimple action is on the underlying vector space $V=\mathbb{F}_q^n$. It turns out that essentially all such pairs of conjugate involutions in $\mathrm{GL}(n,q)$ with regular semisimple product come from a single $\mathrm{GL}(n,q)$-conjugacy class, namely the class $\mathcal{C}(V)$ of involutions with fixed point subspace of dimension $\lfloor\frac{n}{2}\rfloor$.

Received by the editors March 28, 2011.
2010 *Mathematics Subject Classification.* Primary 20D06, 20F69.
This work was partially supported by ARC Grants FF0776186 and DP1096525 and by the NSF.

Theorem 1.1. *If $x, x' \in \mathrm{GL}(n,q)$ are conjugate involutions and $y := xx'$ is regular semisimple, then either $x, x' \in \mathcal{C}(V)$ or $-x, -x' \in \mathcal{C}(V)$.*

Thus we wish to understand the proportion $\iota(n,q) = \iota(V) = \frac{|\mathbf{I}(V)|}{|\mathcal{C}(V)|^2}$, where

$$\mathbf{I}(V) = \{(x,x') \in \mathcal{C}(V) \times \mathcal{C}(V) \,|\, y := xx' \text{ regular semisimple}\}. \tag{1}$$

The algorithmic significance of the quantity $\iota(n,q)$ lies in the fact that, for $V = \mathbb{F}_q^n$ and a given $x \in \mathcal{C}(V)$, $\iota(n,q)$ *is the probability that a uniformly distributed random* $x' \in \mathcal{C}(V)$ *produces a regular semisimple* xx' *with* $(x,x') \in \mathbf{I}(V)$. Theorem 1.1 follows from Lemma 3.1, where we also show that either n is even and $c_y(t)$ is coprime to t^2-1 or n is odd, $t-1$ divides $c_y(t)$, and x, x' agree on the 1-dimensional fixed point space of y. This allows us to derive the proportion $\iota(n,q)$ for n odd from the even-dimensional case (see Theorem 1.2 below). We therefore focus on the case $n = 2d$ even, and in that case, by Lemma 3.1, $\mathbf{I}(2d,q) = \mathbf{I}(V)$ is the set

$$\mathbf{I}(V) = \left\{ (x,x') \in \mathcal{C}(V) \times \mathcal{C}(V) \,|\, \begin{array}{l} y := xx' \text{ regular semisimple} \\ \text{with } c_y(t) \text{ coprime to } t^2-1 \end{array} \right\}, \tag{2}$$

which (see Lemma 4.1) is in a natural one-to-one correspondence, under the map $(x,x') \mapsto (xx', x)$, with the set $\mathbf{RI}(2d,q) = \mathbf{RI}(V)$ defined by

$$\mathbf{RI}(V) := \left\{ (y,x) \,|\, \begin{array}{l} y, x \in \mathrm{GL}(V), x \in \mathcal{C}(V), y^x = y^{-1}, y \text{ regular} \\ \text{semisimple, and } c_y(t) \text{ coprime to } t^2-1 \end{array} \right\}. \tag{3}$$

In Section 5 we study the generating function for the 'weighted proportions' $\mathrm{r}(2d,q) := \frac{|\mathbf{RI}(2d,q)|}{|\mathrm{GL}(2d,q)|}$ and determine the limiting value of $\mathrm{r}(2d,q)$ as d increases, and the (exponential) rate of convergence to the limit. The results are expressed in terms of the quantity

$$\Phi(i,j,x) = \prod_{k=i}^{j} (1 - x^{-k}), \text{ for } x > 1 \text{ and integers } 0 < i < j, \tag{4}$$

and its limit $\Phi(x) = \lim_{j\to\infty} \Phi(1,j,x)$.

Theorem 1.2. *Using the notation above, with $d \geq 1$ and q odd,*

$$\begin{array}{rcl} \iota(2d,q) & = & \mathrm{r}(2d,q)\ \frac{\Phi(1,d,q)^4}{\Phi(1,2d,q)}, \\ \iota(2d+1,q) & = & \iota(2d,q)\ \frac{(1-q^{-d-1})^2}{(1-q^{-2d-1})(1-q^{-1})} = \mathrm{r}(2d,q)\ \frac{\Phi(1,d,q)^2\Phi(1,d+1,q)^2}{(1-q^{-1})\Phi(1,2d+1,q)} \end{array}$$

and, as $d \to \infty$, the limits of $\mathrm{r}(2d,q), \iota(2d,q), \iota(2d+1,q)$ exist and satisfy

$$\begin{array}{rcl} \lim_{d\to\infty} \mathrm{r}(2d,q) & = & (1-q^{-1})^2, \\ \lim_{d\to\infty} \iota(2d,q) & = & (1-q^{-1})^2\Phi(q)^3, \\ \lim_{d\to\infty} \iota(2d+1,q) & = & (1-q^{-1})\Phi(q)^3. \end{array}$$

Moreover $|\mathrm{r}(2d,q) - (1-q^{-1})^2| = o(q_0^{-d})$ for any q_0 such that $1 < q_0 < \sqrt{q}$.

Note that, since $(1-q^{-1})^2 < \Phi(q) < 1-q^{-1}$ (see, for example, [12, Lemma 3.5]), the limits of $\iota(2d,q)$ and $\iota(2d+1,q)$ depend only on q and are bounded below by $(1-q^{-1})^8$ and $(1-q^{-1})^7$ and are bounded above by $(1-q^{-1})^5$ and $(1-q^{-1})^4$, respectively.

1.1. **Comments on the algorithmic background.** The 2001 paper of Altseimer and Borovik [1] introduced a new paradigm in computational group theory by using involution centralisers to distinguish between the finite simple Lie type groups $\mathrm{PSp}(2n, q)$ and $\Omega(2n + 1, q)$ with q odd. These simple groups have equal orders, and many measures relating to the statistical distribution of element properties are the same for both groups. The paper [1] formed the 'catalyst' for the seminal paper [13] of Chris Parker and Rob Wilson, which, despite its recent publication, has been highly influential on recent developments of both new algorithms [7, 9, 10] for computing with finite simple Lie type groups and new theory [5, 11, 14] concerning statistical properties of their elements.

Parker and Wilson [13] showed that involution-centraliser methods could be used for solving several problems which appeared to be computationally hard and gave complexity analyses for methods to construct involutions and their centralisers in quasisimple Lie type groups in odd characteristic. Crucial to their analyses are conjugate involution pairs with regular semisimple products (see [13, p. 889]) often requiring the product to have odd order. In particular they discuss an application of the 'base case' we consider here [13, p. 897] (after Corollary 22), giving a heuristic concerning the proportion of odd-order elements of $\mathrm{PSL}(n, q)$ when the 2-part of $q - 1$ is large compared with n.

In forthcoming work we use the methods of this paper to improve the analysis of Bray's algorithm [2] for constructing involution centralisers in finite general linear groups as part of a program to improve the complexity analyses of a number of algorithms for computing with Lie type groups.

2. Self-conjugate polynomials and matrices

Let $G = \mathrm{GL}(n, q)$, acting naturally on the vector space $V = \mathbb{F}_q^d$ of n-dimensional row vectors over a field of odd order q. For $y \in G$ with characteristic polynomial $c_y(t)$ in its action on V, the inverse y^{-1} has characteristic polynomial $c_y^*(t)$, where, for a monic polynomial $f(t)$ over $\mathbb{F}$ of degree d and having non-zero constant coefficient, the conjugate $f^*(t)$ of $f(t)$ is the polynomial

$$f^*(t) := f(0)^{-1} t^d f(t^{-1}).$$

In other words, if $f(t) = \sum_{0 \le i \le d} a_i t^i$ with the $a_i \in \mathbb{F}$, $a_d = 1$, and $a_0 \neq 0$, then

$$f^*(t) = t^d + a_1 a_0^{-1} t^{d-1} + \cdots + a_{d-1} a_0^{-1} t + a_0^{-1}.$$

A monic polynomial $f(t)$ is called *self-conjugate* if $f(t) = f^*(t)$, and we also say that an element $y \in G$ is *self-conjugate* if $c_y(t)$ is self-conjugate.

Recall that y is regular semisimple if $c_y(t)$ is multiplicity free. It follows that a regular semisimple element y is conjugate to its inverse if and only if $c_y(t)$ is self-conjugate, that is to say, if and only if y is self-conjugate. For such elements y there is always a 2-element that inverts y. We are especially interested in the case when y is inverted by an involution.

We comment on the notion of regular semisimplicity. An element y of $\mathrm{GL}(n, q)$ is called *semisimple* if it is diagonalisable over some extension field of $\mathbb{F}_q$ (see [3, p. 11]), and this is equivalent to the minimal polynomial $m_y(t)$ being multiplicity free. Also y is called *regular* if its centraliser in the corresponding general linear group over an algebraic closure of $\mathbb{F}_q$ has minimal possible dimension, namely n (see [3, p. 29]). It turns out that y is regular if and only if $m_y(t) = c_y(t)$. For a

discussion comparing these two conditions for elements of finite classical groups, see [12, Note 8.1]. The regular semisimple elements are those which are both regular and semisimple.

2.1. **The nearly irreducible case.** For self-conjugate regular semisimple elements y, if $c_y(t)$ is divisible by a monic irreducible polynomial $f(t)$, then $f^*(t)$ divides $c_y^*(t) = c_y(t)$ also. By [4, Lemma 1.3.15(c)], if $f(t)$ is a monic irreducible polynomial and $f^*(t) = f(t)$, then either $f(t)$ is $t+1$ or $t-1$, or $\deg f$ is even. Here we study the cases in which $c_y(t)$ is either self-conjugate and irreducible or a product of two conjugate irreducible polynomials. We comment on the $n = 1$ cases in Remark 2.1 and study the case where n is even in Lemmas 2.2 and 2.4.

Remark 2.1. For the exceptional case in which $y \in \mathrm{GL}(1,q)$ acts on $\mathbb{F}_q$ with characteristic polynomial $t-1$ or $t+1$, the element $y = 1$ or -1, respectively, and y is both inverted and centralised by every element of $\mathrm{GL}(1,q)$. Thus $C_{\mathrm{GL}(1,q)}(y) \cong Z_{q-1}$, and the unique involution inverting y is -1.

The field $\mathbb{F}_{q^n}$ may be viewed as an n-dimensional vector space over $\mathbb{F}_q$, and from this point of view, the multiplicative group of $\mathbb{F}_{q^n}$ is a cyclic subgroup of $\mathrm{GL}(n,q)$ of order $q^n - 1$ acting regularly on the non-zero vectors. There is a single conjugacy class of such subgroups in $\mathrm{GL}(n,q)$, and they are called *Singer subgroups* or *Singer cycles*. Thus, if $T := \langle z \rangle \cong Z_{q^n-1}$ is a Singer cycle in $\mathrm{GL}(n,q)$, then we may identify the underlying vector space $\mathbb{F}_q^n$ with the additive group of the field $\mathbb{F}_{q^n}$ and T with the multiplicative group $\mathbb{F}_{q^n}^*$, so that z is a primitive element. Moreover $N_{\mathrm{GL}(n,q)}(T) = \langle z, \sigma \rangle \cong \Gamma\mathrm{L}(1,q^n)$, with $\sigma : u \mapsto u^q$ for $u \in \mathbb{F}_{q^n}$ (see [8, Satz II.7.3]).

Lemma 2.2. *Let $y \in \mathrm{GL}(W)$ be irreducible in its action on $W = \mathbb{F}_q^{2m}$, for some $m \geq 1$ and odd q. Then*

(i) *$T := C_{\mathrm{GL}(W)}(y) = \langle z \rangle \cong Z_{q^{2m}-1}$ is a Singer cycle in $\mathrm{GL}(W)$, and $N_{\mathrm{GL}(W)}(T) = \langle z, \sigma \rangle \cong \Gamma\mathrm{L}(1,q^{2m})$, as above.*

(ii) *y is self-conjugate, that is, y is inverted by some element of $\mathrm{GL}(W)$, if and only if $|y|$ divides $q^m + 1$, and in this case the inverting elements are precisely the elements $z^k\sigma^m$ in $N_{\mathrm{GL}(W)}(T)$; in particular, each such y is inverted by precisely $q^m + 1$ involutions.*

(iii) *Moreover, the involutions in $\mathrm{GL}(W)$ that invert an irreducible $y \in T$ are all conjugate in $N_{\mathrm{GL}(W)}(T)$ to σ^m and have a fixed point subspace of dimension m.*

Proof. (i) This assertion is well known and can be found in Satz II.7.3 on page 187 of [8].

(ii) Suppose that $y = z^i \in T$ is inverted by some element x of $\mathrm{GL}(W)$. Then x normalises $C_{\mathrm{GL}(W)}(y) = T$, and so x lies in $N_{\mathrm{GL}(W)}(T)$. This means that an inverting element x must be of the form $z^k\sigma^j$, inducing a map $\sigma^j : z \mapsto z^{q^j}$ on T, for some positive integer $j < 2m$. Since x inverts z^i we have $z^{i(q^j+1)} = 1$, so $|z^i|$ divides $q^j + 1$, which in turn divides $q^{2j} - 1$. Since also $|z^i|$ divides $|z| = q^{2m} - 1$, the order $|z^i|$ divides $q^{\gcd(2m,2j)} - 1$. However, since z^i is irreducible, $|z^i|$ does not divide $q^\ell - 1$ for any $\ell < 2m$, and hence $\gcd(2m, 2j) = 2m$, whence $j = m$ (since $j < 2m$). Thus $|z^i|$ divides $q^m + 1$. Conversely, if $|z^i|$ divides $q^m + 1$, then any element of $N_{\mathrm{GL}(W)}(T)$ of the form $z^k\sigma^m$ inverts z^i.

Let $T_0 = \langle z_0 \rangle$, where $z_0 = z^{q^m-1}$, the unique subgroup of T of order $q^m + 1$. We have shown that T_0 consists of all the elements of T that are inverted by some

element of $\mathrm{GL}(W)$, and the inverting elements are precisely $z^k\sigma^m$ for $0 \le k < q^{2m}-1$. An inverting element $z^k\sigma^m$ has order 2 if and only if $z^{k(1+q^m)} = 1$ or, equivalently, if and only if $z^k \in T_0$. Thus exactly q^m+1 involutions invert an irreducible self-conjugate element y.

(iii) Since $(z^k\sigma^m)^z = z_0(z^k\sigma^m)$, it follows that these q^m+1 involutions are all conjugate in $N_{\mathrm{GL}(W)}(T)$ to σ^m. Finally we note that the set of fixed points of σ^m in W (identified with the field $\mathbb{F}_{q^{2m}}$) is the subfield $\mathbb{F}_{q^m}$. □

Remark 2.3. We remark that each $N_{\mathrm{GL}(W)}(T)$-conjugacy class of elements inverting y contains a unique element $x(k) = z^k\sigma^m$ with $0 \le k \le q^m-2$, and all elements in the class square to $x(k)^2 = z^{k(q^m+1)}$, which is an $\mathbb{F}_q$-scalar (a central element of $\mathrm{GL}(W)$) if and only if k is a multiple of $(q^m-1)/(q-1)$. The inverting involutions are the class for which $k=0$, and all non-involutory inverting elements fix no non-zero vectors in W.

Our treatment of the non-self-conjugate case involves a wreath product of the form $H \wr S_2$. This is a semidirect product $(H \times H).S_2$, where the generator τ of the top group S_2, of order 2, conjugates each element (h_1, h_2) of $H \times H$ to (h_2, h_1). For a positive integer m, we use $[1,m]$ to denote the set of integers $\{1, 2, \dots, m\}$.

Lemma 2.4. *Let $y \in \mathrm{GL}(U)$ with characteristic polynomial $g(t)g^*(t)$, in its action on $U = \mathbb{F}_q^{2m}$, for some irreducible non-self-conjugate polynomial g of degree $m \ge 1$. Then:*

(i) *$C_{\mathrm{GL}(U)}(y) \cong T \times T = \langle z \rangle \times \langle z \rangle \cong (Z_{q^m-1})^2$ preserving a decomposition $U = W \oplus W$ with T a Singer cycle in $\mathrm{GL}(W)$, and $y = (y_1, y_2)$ such that $c_{y_1}(t) = g(t)$ and $c_{y_2}(t) = g^*(t)$ acting on W; moreover, $N_{\mathrm{GL}(U)}(T \times T) = \langle z, \sigma \rangle \wr \langle \tau \rangle \cong \Gamma\mathrm{L}(1, q^m) \wr S_2$ with $\sigma : z^i \mapsto z^{iq}$ and $\tau : (u, u') \mapsto (u', u)$ for $u, u' \in \langle z, \sigma \rangle$; also, for $(w, w') \in U$, $(w, w')^\tau = (w', w)$.*

(ii) *y is inverted by some element of $\mathrm{GL}(U)$ if and only if $y_2 = y_1^{-q^k}$ for some $k \in [1,m]$, and in this case the inverting elements are the elements $(z^i\sigma^k, z^j\sigma^{-k})\tau$ of $N_{\mathrm{GL}(U)}(T \times T)$; in particular, each such y is inverted by precisely q^m-1 involutions.*

(iii) *Moreover, all involutions in $\mathrm{GL}(U)$ that invert such an element y are conjugate in $N_{\mathrm{GL}(U)}(T \times T)$ to τ and have fixed point subspaces of dimension m.*

Proof. Since $c_y(t) = g(t)g^*(t)$ for some irreducible non-self-conjugate polynomial $g(t)$, the element y leaves invariant a unique decomposition $U = W_1 \oplus W_2$ such that $y_i := y|_{W_i}$ is irreducible with characteristic polynomial $g(t), g^*(t)$ for $i = 1, 2$ respectively, and the centralisers $C_{\mathrm{GL}(W_1)}(y|_{W_1}) \cong C_{\mathrm{GL}(W_2)}(y|_{W_2}) \cong Z_{q^m-1}$ are Singer cycles for the $\mathrm{GL}(W_i)$. Since all Singer cycles of $\mathrm{GL}(W_i)$ are conjugate, we may identify W_1 and W_2 with a single m-dimensional vector space W over $\mathbb{F}_q$ in such a way that $C_{\mathrm{GL}(W_1)}(y|_{W_1})$ and $C_{\mathrm{GL}(W_2)}(y|_{W_2})$ are identified with the same Singer cycle $T = \langle z \rangle$ in $\mathrm{GL}(W)$. Then, as above, we identify W with the additive group of the field $\mathbb{F}_{q^m}$ in such a way that T acts as field multiplications with z a primitive element and $N_{\mathrm{GL}(U)}(T \times T) = \langle z, \sigma \rangle \wr \langle \tau \rangle \cong \Gamma\mathrm{L}(1, q^m) \wr S_2$, where σ, τ are as in (i).

The element y is then equal to (y_1, y_2) with y_1 and y_2 irreducible on W and with characteristic polynomials $g(t), g^*(t)$, respectively. Since $g(t) \ne g^*(t)$, the elements y_1, y_2 are not inverted by any element of $\mathrm{GL}(W)$, since y_1^{-1}, y_2^{-1} have characteristic

polynomials $g^*(t)$, $g(t)$ respectively. Suppose that y is inverted by an element $x \in \mathrm{GL}(U)$. Then x normalises $C_{\mathrm{GL}(U)}(y) = T \times T$, so x lies in $N_{\mathrm{GL}(U)}(T \times T)$ and $x = (z^i\sigma^k, z^j\sigma^\ell)\tau^\delta$, for some i, j, k, ℓ, δ. Since x inverts y and no element of $\Gamma\mathrm{L}(1, q^m)$ inverts y_1, it follows that $\tau^\delta = \tau$. Thus $y^{-1} = y^x = (y_2^{q^\ell}, y_1^{q^k})$, and we have $y_1^{-1} = y_2^{q^\ell}$ and $y_2^{-1} = y_1^{q^k}$, whence $y_1^{q^{k+\ell}} = y_1$, so $|y_1|$ divides $q^{k+\ell} - 1$. Since y_1 is irreducible this implies that m divides $k + \ell$ so that $\sigma^\ell = \sigma^{-k}$. Thus $y_2 = y_1^{-q^k}$ and $x = (z^i\sigma^k, z^j\sigma^{-k})\tau$. Conversely, each element $x = (z^i\sigma^k, z^j\sigma^{-k})\tau$ inverts each element of the form $(y_1, y_1^{-q^k})$. Thus there are $(q^m - 1)^2$ inverting elements x, and $x^2 = (z^{i+jq^{-k}}, z^{j+iq^k}) = 1$ if and only if $j \equiv -iq^k \pmod{q^m - 1}$. Thus exactly $q^m - 1$ inverting elements are involutions.

Since $x^{(1,z)} = (z^{i+q^{-k}}\sigma^k, z^{j-1}\sigma^{-k})\tau$, and since $x^{(\sigma,1)} = (z^{iq}\sigma^{k-1}, z^j\sigma^{-k+1})\tau$, each inverting element x is conjugate in $N_{\mathrm{GL}(U)}(T \times T)$ to $x_i := (z^i, 1)\tau$ for some i such that $0 \le i < q^m - 1$, and x_i inverts precisely the elements of $T \times T$ of the form (u, u^{-1}). Moreover $x_i^2 = (z^i, z^i)$, which is the identity if and only if $i = 0$, that is, $x_i = x_0 = \tau$. Thus each inverting involution is conjugate in $N_{\mathrm{GL}(U)}(T \times T)$ to τ, and the fixed point subspace of τ is $\{(w, w) \mid w \in W\}$, of dimension m. □

Remark 2.5. Each inverting element in Lemma 2.4(ii) was shown to be conjugate in $N_{\mathrm{GL}(U)}(T \times T)$ to $x_i := (z^i, 1)\tau$, for some i such that $0 \le i < q^m - 1$. The square $x_i^2 = (z^i, z^i)$ lies in the centre of $\mathrm{GL}(U)$ if and only if $(q^m - 1)/(q - 1)$ divides i so that $z^i \in \mathbb{F}_q^*$. If moreover $z^i = \mu^2$ for some $\mu \in \mathbb{F}_q^*$, then both the μ-eigenspace and the $(-\mu)$-eigenspace of x_i in $U = W \oplus W$ have dimension m; they are the subspaces $\{(w, \mu w) \mid w \in W\}$ and $\{(w, -\mu w) \mid w \in W\}$, respectively, each of dimension m. In particular, taking $\mu = \pm 1$ we obtain the (± 1)-eigenspaces of $x_0 = \tau$.

3. Inverting involutions

We summarise the situation described in the introduction and introduce notation that will be used throughout the paper. Let $G := \mathrm{GL}(n, q)$ with q odd, and suppose that $y \in G$ is regular semisimple such that $y^x = y^{-1}$ for some involution $x \in G$. Let $c_y(t)$ denote the characteristic polynomial of y in its action on the space $V = \mathbb{F}_q^n$ of n-dimensional row vectors, and consider the factorisation $c_y(t) = \prod_{i=1}^r f_i(t)$, where each of the $f_i(t)$ is monic irreducible over $\mathbb{F}_q$. Since y is regular semisimple, $c_y(t)$ is multiplicity-free. Thus the f_i are pairwise distinct. Also, since $y^x = y^{-1}$, $c_y(t)$ is equal to the characteristic polynomial $c_y^*(t)$ of y^{-1}, that is to say, $c_y(t)$ is self-conjugate. In this situation we also say that y is *self-conjugate*. Thus, for each i, $f_i^*(t)$ divides $c_y(t)$, so either $f_i = f_i^*$ is itself a self-conjugate polynomial or $f_i \ne f_i^*$ and $f_i f_i^*$ divides $c_y(t)$. By [4, Lemma 1.3.15(c)], if $f_i(t)$ is a monic irreducible self-conjugate polynomial, then either $f_i(t)$ is $t + 1$ or $t - 1$, or $\deg f_i$ is even. Therefore we may write $c_y(t)$ as follows:

$$c_y(t) = \left(\prod_{i=1}^{r} f_i(t)\right) \times \left(\prod_{j=1}^{s} g_j(t) g_j^*(t)\right) \times (t-1)^{\delta_-} (t+1)^{\delta_+}, \tag{5}$$

where each $f_i = f_i^*$ with even degree, each $g_j \ne g_j^*$, with the f_i, g_j, g_j^* pairwise distinct monic irreducibles, and $\delta_-, \delta_+ \in \{0, 1\}$.

We consider the primary decomposition of V as an $\mathbb{F}_q\langle y\rangle$-module (see, for example, [6, Lemma 8.10]) and combine the two summands corresponding to each

TABLE 1. Values of $h(t), d, d'$ for Lemma 3.1

$h(t)$	n	d, d' values
1	even	$d = d' = \frac{n}{2}$
$t^2 - 1$	even	$\{d, d'\} = \{\frac{n}{2}, \frac{n+2}{2}\}$ or $\{\frac{n}{2}, \frac{n-2}{2}\}$
$t - 1$	odd	$d = d' \in \{\frac{n-1}{2}, \frac{n+1}{2}\}$
$t + 1$	odd	$\{d, d'\} = \{\frac{n-1}{2}, \frac{n+1}{2}\}$

conjugate pair $\{g_j, g_j^*\}$, to obtain the following uniquely determined y-invariant direct sum decomposition of $V = \mathbb{F}_q^n$:

$$V = \left(\bigoplus_{i=1}^{r} V_i\right) \oplus \left(\bigoplus_{j=1}^{s} U_j\right) \oplus V_{\pm} \tag{6}$$

such that

(2.1a) for each $i \leq r$, the restriction $y_i := y|_{V_i} \in \mathrm{GL}(V_i)$ is irreducible with self-conjugate characteristic polynomial $f_i(t)$ of even degree;

(2.1b) for each $j \leq s$, the restriction $y'_j := y|_{U_j} \in \mathrm{GL}(U_j)$ has characteristic polynomial $g_j(t)g_j^*(t)$; and

(2.1c) $\dim V_{\pm} \in \{0, 1, 2\}$; if $\dim V_{\pm} = 1$, then $y|_{V_{\pm}}$ has characteristic polynomial $t + 1$ or $t - 1$; if $\dim V_{\pm} = 2$, then $V_{\pm} = V_+ \oplus V_-$, and $y|_{V_+}, y|_{V_-}$ has characteristic polynomial $t - 1, t + 1$ respectively.

Moreover, the uniqueness of (6) implies that x must also leave this direct decomposition of V invariant. Thus x induces an element $x_i \in \mathrm{GL}(V_i)$ that inverts y_i in (2.1a), an element $x'_j \in \mathrm{GL}(U_j)$ that inverts y'_j in (2.1b), and if $V_{\pm} \neq 0$, then x fixes or negates each 1-dimensional y-eigenspace in $V_{\pm}$.

In Subsection 2.1 we studied the centralisers of the self-conjugate regular semisimple elements induced by y on the V_i and U_j. We use the results proved there to prove Lemma 3.1 mentioned in the introduction concerning the eigenspace dimensions of the inverting involution x. Let $\mathcal{C}(V)$ denote the $\mathrm{GL}(n, q)$-conjugacy class of involutions with fixed point subspace of dimension $\lfloor \frac{n}{2} \rfloor$. If an involution x inverts an element y, note that $x' := xy$ is also an involution inverting y.

Lemma 3.1. *Let $x, y \in \mathrm{GL}(n, q)$ with q odd, such that y is regular semisimple with characteristic polynomial $c_y(t)$ and associated decomposition (6) of $V = \mathbb{F}_q^n$, and x is an involution inverting y with fixed point subspace of dimension d. Let $h(t) := \gcd(c_y(t), t^2 - 1)$, and let $x' := xy$ with fixed point subspace of dimension d'. Then $h(t), d, d'$ are as in one of the lines of Table 1. Moreover,*

(a) *If $h(t) = 1$, then all involutions inverting y lie in $\mathcal{C}(V)$, while if $h(t) \neq 1$, then exactly half the involutions inverting y lie in $\mathcal{C}(V)$.*

(b) *If $x \in \mathcal{C}(V)$, then x' also lies in $\mathcal{C}(V)$ if and only if either*
   (i) *n is even, $h(t) = 1$, and $V_{\pm} = 0$ or*
   (ii) *n is odd, $h(t) = t - 1$, and x, x' both negate $V_{\pm}$.*

(c) *If x, x' are conjugate in $\mathrm{GL}(n, q)$, then either $x, x' \in \mathcal{C}(V)$ or $-x, -x' \in \mathcal{C}(V)$.*

Proof. As noted above, x' is an involution inverting y. The elements y, x, x' all leave invariant the direct decomposition of V in (6) with direct factors $V_i, U_j, V_\pm$ as in (2.1a), (2.1b), and (2.1c), respectively, the fixed point subspace of x is a direct sum of the fixed point subspaces of the $x|_{V_i}$, $x|_{U_j}$, and $x|_{V_\pm}$, and similarly for x'. For each summand $W = V_i$ or U_j, it follows from Lemmas 2.2 and 2.4 that the dimension of W is even, say $2m$, and the fixed point subspaces of $x|_W$ and $x'|_W$ both have dimension m. Write $V_0 = (\bigoplus_{i=1}^r V_i) \oplus (\bigoplus_{j=1}^s U_j)$. Then $V = V_0 \oplus V_\pm$, and the fixed point subspaces of $x|_{V_0}$ and $x'|_{V_0}$ both have dimension $\frac{1}{2}\dim(V_0)$. Thus if $h(t) = 1$, or equivalently if $V_\pm = 0$, the dimension n is even and $d = d' = \frac{n}{2}$ as in line 1 of Table 1. In this case $x, x' \in \mathcal{C}(V)$, and all assertions are proved.

Suppose now that $V_\pm \neq 0$, equivalently $h(t) \neq 1$. Then each y-eigenspace W in $V_\pm$ corresponds to a factor $t-1$ or $t+1$ of $c_y(t)$. Since x, x' are involutions, each of $x|_W$ and $x'|_W$ fixes or negates W, and $x'|_W = x|_W$ or $-x|_W$ according as W corresponds to $t-1$ or $t+1$ respectively.

Suppose next that n is odd, so that $V_\pm$ has dimension 1 and $h(t) = t \pm 1$. If $h(t) = t+1$, or equivalently if y negates $V_\pm$, then $\{d, d'\}$ is $\{\frac{n-1}{2}, \frac{n+1}{2}\}$, as in line 4 of Table 1. In this case x, x' are not conjugate and exactly one lies in $\mathcal{C}(V)$. On the other hand if $h(t) = t-1$, or equivalently if y fixes $V_\pm$, then $d = d'$ and can be either $\frac{n-1}{2}$ or $\frac{n+1}{2}$, as in line 3 of Table 1. In this case x, x' are conjugate and either both lie in $\mathcal{C}(V)$ or both $-x$ and $-x'$ lie in $\mathcal{C}(V)$. Also, if $x, x' \in \mathcal{C}(V)$, then both negate $V_\pm$. Finally, for n odd, the map $f : x \mapsto f(x)$ on the set of involutions inverting y, defined by $f(x)|_{V_0} = (xy)|_{V_0}$, $f(x)|_{V_\pm} = -(x|_{V_\pm})$, interchanges the inverting involutions which lie in $\mathcal{C}(V)$ with those which do not lie in $\mathcal{C}(V)$, so exactly half the inverting involutions lie in $\mathcal{C}(V)$.

Now suppose that n is even. Then $h(t) = t^2 - 1$, $V_\pm$ has two summands of dimension 1, and x, x' agree on the summand corresponding to $f(t) = t-1$ and disagree on the other summand. If they both fix the former summand, then $\{d, d'\} = \{\frac{n}{2}, \frac{n}{2}+1\}$, while if they both negate that summand, then the dimensions are $\{\frac{n}{2}, \frac{n}{2}-1\}$. Thus line 2 of Table 1 holds, and in either case x, x' are not conjugate and exactly one lies in $\mathcal{C}(V)$. Finally, the map $f : x \mapsto f(x)$ defined by $f(x) = xy$ interchanges the inverting involutions which lie in $\mathcal{C}(V)$ with those which do not lie in $\mathcal{C}(V)$, and again exactly half the inverting involutions lie in $\mathcal{C}(V)$. □

For $g \in \mathrm{GL}(V)$, write $\mathrm{Cent}(g) := |C_{\mathrm{GL}(V)}(g)|$. Then for $c_y(t)$ as in (5),

$$C_{\mathrm{GL}(V)}(y) = \left(\prod_{i=1}^r C_{\mathrm{GL}(V_i)}(y_i)\right)\left(\prod_{j=1}^s C_{\mathrm{GL}(U_j)}(y_j')\right) C_{\mathrm{GL}(V_\pm)}(y|_{V_\pm})$$

and the results of Subsection 2.1 enable us to compute both $\mathrm{Cent}(y)$ and the contribution to $|\mathbf{RI}(V)|$ from pairs (y', x') with y' conjugate to a given regular semisimple y.

Lemma 3.2. *Let $y \in \mathrm{GL}(n,q) = \mathrm{GL}(V)$ (with q odd) be regular semisimple and self-conjugate with characteristic polynomial $c_y(t)$ as in* (5)*. Then:*

(a) $$\mathrm{Cent}(y) = \left(\prod_{i=1}^r (q^{\deg f_i} - 1)\right)\left(\prod_{j=1}^s (q^{\deg g_j} - 1)^2\right)(q-1)^{\delta_+ + \delta_-}.$$

(b) *The number of involutions in* $\mathcal{C}(V)$ *that invert* y *is equal to*

$$\left(\prod_{i=1}^{r}(q^{\frac{1}{2}\deg f_i}+1)\right)\left(\prod_{j=1}^{s}(q^{\deg g_j}-1)\right)\varepsilon(y),$$

where $\varepsilon(y)=2$ *if* t^2-1 *divides* $c_Y(t)$*, and* $\varepsilon(y)=1$ *otherwise.*

(c) *If* $n=2d$ *is even and* $c_y(t)$ *is coprime to* t^2-1*, then the number of pairs* $(y',x)\in\mathbf{RI}(V)$ *such that* y' *has characteristic polynomial* $c_y(t)$ *is*

$$\frac{|\mathrm{GL}(2d,q)|}{\left(\prod_{i=1}^{r}(q^{\frac{1}{2}\deg f_i}-1)\right)\left(\prod_{j=1}^{s}(q^{\deg g_j}-1)\right)}.$$

Proof. Part (a) follows from the remarks before the lemma together with Remark 2.1 and Lemmas 2.2 and 2.4. From these results we also find that the number of involutions $x|_{V_i}$, $x|_{U_j}$ inverting y_i and y'_j are $q^{\frac{1}{2}\deg f_i}+1$ and $q^{\deg g_j}-1$ respectively. For an involution x inverting y, the restriction $x|_{V_\pm}$ may have order 1 or 2, and so there are $2^{\delta_+ + \delta_-}$ possibilities for $x|_{V_\pm}$. By Lemma 3.1, if $V_\pm\neq 0$, then exactly half of these lead to involutions in $\mathcal{C}(V)$. This proves (b). Finally if $n=2d$ and $c_y(t)$ is coprime to t^2-1 (so that $\delta^+ + \delta- = 0$), then the number of pairs $(y',x)\in\mathbf{RI}(V)$ with characteristic polynomial $c_y(t)$ is the number $|\mathrm{GL}(2d,q)|/\mathrm{Cent}(y)$ of conjugates of y times the number of $x\in\mathcal{C}(V)$ inverting y. Thus part (c) follows from parts (a) and (b). □

4. Links between various proportions

First we prove the assertions in Theorem 1.2 concerning $\iota(2d,q)$ and $\iota(2d+1,q)$ and verify the claimed bijection between the sets in (2) and (3).

Lemma 4.1. *For* $d\geq 1$ *and* q *odd,*

(a) *the map* $(x,x')\mapsto(xx',x)$ *defines a bijection between the sets* $\mathbf{I}(2d,q)$ *and* $\mathbf{RI}(2d,q)$ *defined in* (2) *and* (3)*,*

(b)
$$\begin{aligned}\iota(2d,q) &= \mathrm{r}(2d,q)\,\tfrac{\Phi(1,d,q)^4}{\Phi(1,2d,q)};\ \textit{and}\\ \iota(2d+1,q) &= \iota(2d,q)\,\tfrac{(1-q^{-d-1})^2}{(1-q^{-2d-1})(1-q^{-1})} = \mathrm{r}(2d,q)\,\tfrac{\Phi(1,d,q)^2\Phi(1,d+1,q)^2}{(1-q^{-1})\Phi(1,2d+1,q)}.\end{aligned}$$

Proof. Let $V=\mathbb{F}_q^{2d}$ and let $(x,x')\in\mathcal{C}(V)\times\mathcal{C}(V)$ such that $y:=xx'$ is regular semisimple with $c_y(t)$ coprime to t^2-1, that is to say, $(x,x')\in\mathbf{I}(V)$. (Note that by Lemma 3.1, $\dim(V)$ must be even.) Also $y^x=(xx')^x=x'x=y^{-1}$, so $(y,x)\in\mathbf{RI}(V)$. Clearly the map is injective. Conversely if $(y,x)\in\mathbf{RI}(V)$, then $x':=xy$ is an involution inverting y, and by Lemma 3.1(b), x' also lies in $\mathcal{C}(V)$, so the map is onto and hence is a bijection. Thus $|\mathbf{RI}(2d,q)|=|\mathbf{I}(2d,q)|$.

By definition, $\mathrm{r}(2d,q)=\frac{|\mathbf{RI}(2d,q)|}{|\mathrm{GL}(2d,q)|}$. Also, for $x\in\mathcal{C}(V)$, $C_{\mathrm{GL}(2d,q)}(x)\cong\mathrm{GL}(d,q)\times\mathrm{GL}(d,q)$, so $|\mathcal{C}(V)|=|\mathrm{GL}(2d,q)|/|\mathrm{GL}(d,q)|^2$. Hence

$$\begin{aligned}\iota(2d,q) &= \frac{|\mathbf{I}(2d,q)|}{|\mathcal{C}(V)|^2}=|\mathbf{RI}(2d,q)|\cdot\frac{|\mathrm{GL}(d,q)|^4}{|\mathrm{GL}(2d,q)|^2}\\ &= \mathrm{r}(2d,q)\cdot\frac{|\mathrm{GL}(d,q)|^4}{|\mathrm{GL}(2d,q)|}=\mathrm{r}(2d,q)\cdot\frac{\Phi(1,d,q)^4}{\Phi(1,2d,q)}.\end{aligned}$$

Now we consider the case where $n = 2d+1$ is odd and redefine $V = \mathbb{F}_q^{2d+1}$. Then for $x \in \mathcal{C}(V)$, $C_{\mathrm{GL}(2d+1,q)}(x) \cong \mathrm{GL}(d,q) \times \mathrm{GL}(d+1,q)$, so $|\mathcal{C}(V)| = |\mathrm{GL}(2d+1,q)|/(|\mathrm{GL}(d,q)| \cdot |\mathrm{GL}(d+1,q)|)$. Let $(x,x') \in \mathbf{I}(V)$ with, this time, $\mathbf{I}(V)$ as in (1). So $x, x' \in \mathcal{C}(V)$, $y := xx'$ is regular semisimple and inverted by x, and so by Lemma 3.1(b), $\gcd(c_y(t), t^2-1) = t-1$, and x, x' both negate the 1-dimensional fixed point space $V_\pm$ of y. The element y, and therefore also the pair (x,x'), determines a decomposition of V as in (6), which we write as $V = V_0 \oplus V_\pm$, where V_0 is the sum of the V_i and the U_j in (6). Define $x_0 := x|_{V_0}$ and $y_0 := y|_{V_0}$ in $\mathrm{GL}(V_0)$. Then $(y_0, x_0) \in \mathbf{RI}(V_0)$ since $x_0 \in \mathcal{C}(V_0)$, y_0 is regular semisimple with $c_{y_0}(t)$ coprime to t^2-1, and x_0 inverts y_0. Conversely the decomposition $V = V_0 \oplus V_\pm$, together with the pair (y_0, x_0), uniquely determines (y,x) and hence also (x,x'), since by Lemma 3.1(b), firstly, x must negate $V_\pm$ and so $x = -I_{V_\pm} \oplus x_0$, and secondly, y must fix $V_\pm$, so $y = I_{V_\pm} \oplus y_0$, and $x' = xy$. Thus $|\mathbf{I}(V)|$ is the number of decompositions times $|\mathbf{RI}(V_0)| = |\mathbf{RI}(2d,q)|$, so

$$\begin{aligned}
\iota(2d+1,q) &= \frac{|\mathbf{I}(V)|}{|\mathcal{C}(V)|^2} \\
&= \frac{|\mathrm{GL}(2d+1,q)|}{(q-1)|\mathrm{GL}(2d,q)|} \cdot |\mathbf{RI}(2d,q)| \cdot \frac{|\mathrm{GL}(d,q)|^2|\mathrm{GL}(d+1,q)|^2}{|\mathrm{GL}(2d+1,q)|^2} \\
&= \frac{\mathrm{r}(2d,q)}{q-1} \cdot \frac{|\mathrm{GL}(d,q)|^2|\mathrm{GL}(d+1,q)|^2}{|\mathrm{GL}(2d+1,q)|} \\
&= \mathrm{r}(2d,q) \cdot \frac{\Phi(1,d,q)^2\Phi(1,d+1,q)^2}{(1-q^{-1})\Phi(1,2d+1,q)} \\
&= \iota(2d,q) \cdot \frac{\Phi(1,2d,q)}{\Phi(1,d,q)^4} \cdot \frac{\Phi(1,d,q)^2\Phi(1,d+1,q)^2}{(1-q^{-1})\Phi(1,2d+1,q)} \\
&= \iota(2d,q) \cdot \frac{(1-q^{-d-1})^2}{(1-q^{-2d-1})(1-q^{-1})}.
\end{aligned}$$

□

Now we derive the limits for the quantities $\iota(n,q)$ from the limit results for $\mathrm{r}(2d,q)$, which will be proved in Section 5.

Corollary 4.2. *Suppose that* $\mathrm{r}(\infty,q) := \lim_{d\to\infty} \mathrm{r}(2d,q)$ *exists. Then the limits as* $d \to \infty$ *of* $\iota(2d,q)$ *and* $\iota(2d+1,q)$ *also exist and satisfy*

$$\begin{aligned}
\lim_{d\to\infty} \iota(2d,q) &= \mathrm{r}(\infty,q) \cdot \Phi(1,\infty,q)^3, \\
\lim_{d\to\infty} \iota(2d+1,q) &= \mathrm{r}(\infty,q) \cdot \tfrac{\Phi(1,\infty,q)^3}{1-q^{-1}}.
\end{aligned}$$

Proof. It follows immediately from Lemma 4.1 that $\lim_{d\to\infty} \iota(2d+1,q) = \frac{1}{1-q^{-1}} \lim_{d\to\infty} \iota(2d,q)$ and $\lim_{d\to\infty} \iota(2d,q) = \mathrm{r}(\infty,q)\,\Phi(1,\infty,q)^3$. □

5. Generating function for $\mathrm{r}(2d,q)$

In this section we analyse the generating function $R(u) = \sum_{n=0}^{\infty} \mathrm{r}(2n,q)u^n$ for the proportions $\mathrm{r}(2d,q) = \frac{|\mathbf{RI}(2n,q)|}{|\mathrm{GL}(2n,q)|}$, where we set $\mathrm{r}(0,q) = 1$. It follows from Lemma 3.2 that, for $n \geq 1$, $\mathrm{r}(2n,q)$ is the sum over all monic self-conjugate polynomials $f(t) = c_y(t)$ of degree $2n$, having a factorisation as in (5) with $\delta^+ = \delta^- = 0$, of the expression

$$\frac{1}{\left(\prod_{i=1}^{r}(q^{\frac{1}{2}\deg f_i}-1)\right)\left(\prod_{j=1}^{s}(q^{\deg g_j}-1)\right)}.$$

Thus the generating function $R(u)$ can be expressed as

$$R(u) = \sum_{n=0}^{\infty} \left(\sum_{f=f^*,\ \deg f = 2n} \frac{u^n}{\left(\prod_{i=1}^{r}(q^{\frac{1}{2}\deg f_i}-1)\right)\left(\prod_{j=1}^{s}(q^{\deg g_j}-1)\right)} \right),$$

where the inner summation is over all self-conjugate monic polynomials $f(t)$ of degree $2n$ with a factorisation $f = (\prod_i f_i).(\prod_j (g_j g_j^*))$ as in (5). Moreover, computing the coefficient of u^n in the infinite product

$$R'(u) := \prod_{f=f^*,\,\text{irred.}} \left(1 + \frac{u^{\frac{1}{2}\deg f}}{q^{\frac{1}{2}\deg f}-1}\right) \times \prod_{\{g,g^*\},\, g\neq g^*,\,\text{irred.}} \left(1 + \frac{u^{\deg g}}{q^{\deg g}-1}\right),$$

we see that $R(u) = R'(u)$. Recall that in the first product each self-conjugate polynomial f has even degree. The contribution from each irreducible polynomial f or pair $\{g, g^*\}$ to the infinite product depends only on the degree. As in [4, p. 26] we define the following quantities:

$$\begin{aligned} N(q;m) &= \#\,\text{monic irreducible polynomials over } \mathbb{F}_q \text{ of degree } m, \\ &\quad \text{with non-zero constant term,} \\ N^*(q;m) &= \#\,\text{monic irreducible self-conjugate polynomials over} \\ &\quad \mathbb{F}_q \text{ of degree } m, \\ M^*(q;m) &= \#\ \text{(unordered) conjugate pairs of monic irreducible} \\ &\quad \text{non-self-conjugate polynomials over } \mathbb{F}_q \text{ of degree } m. \end{aligned}$$

As mentioned in Section 3, for each $m \geq 1$, we have $N^*(q; 2m+1) = 0$, so $M^*(q; 2m+1) = \frac{1}{2}N(q; 2m+1)$. Also $M^*(q; 1) = (q-3)/2$, and in general (see [4, Lemma 1.3.16]), for $m \geq 1$,

$$M^*(q;m) = \frac{1}{2}\left(N(q;m) - N^*(q;m)\right) = \frac{1}{2m}q^m + O(q^{m/2}), \tag{7}$$

while for even m, $N^*(q;m) = m^{-1}q^{m/2} + O(q^{m/6})$. Thus we obtain the following more compact expression for $R(u)$:

$$R(u) = \prod_{m\geq 1}\left(1 + \frac{u^m}{q^m-1}\right)^{N^*(q;2m)} \times \prod_{m\geq 1}\left(1 + \frac{u^m}{q^m-1}\right)^{M^*(q;m)}. \tag{8}$$

Moreover it follows from [4, Corollary 1.3.2] and the asymptotic values given above for $N^*(q;2m)$ and $M^*(q;m)$ that each of these infinite products converges absolutely for $|u| < 1$. We use the following lemma to simplify this expression.

Lemma 5.1. *Let q be an odd prime power and let m be a positive integer. Then*

$$N^*(q;2m) + M^*(q;m) = \begin{cases} N(q;m) & m > 1, \\ N(q;m) - 1 & m = 1. \end{cases}$$

Proof. By [4, Lemma 1.3.16(b,c)], if m is even, then $N^*(q;2m) + M^*(q;m) = 2M^*(q;m) + N^*(q;m) = N(q;m)$. By the same lemma, if m is odd and $m > 1$, then $N^*(q;2m) + M^*(q;m) = 2M^*(q;m) = N(q;m)$. Finally, if $m = 1$, then $N^*(q;2m) + M^*(q;m) = 2M^*(q;m) + 1 = q - 2 = N(q;m) - 1$. □

Applying Lemma 5.1 to (8) we obtain

$$R(u) = \frac{1}{1 + u/(q-1)} \times \prod_{m\geq 1}\left(1 + \frac{u^m}{q^m-1}\right)^{N(q;m)}. \tag{9}$$

In the following analysis we employ methods used in [4] to obtain another new expression for $R(u)$ from which we deduce the assertions about $\mathrm{r}(2n,q)$ in Theorem 1.2.

Lemma 5.2. *The limit of* $\mathrm{r}(2n,q)$ *as* $n\to\infty$ *exists and*

$$\mathrm{r}(\infty,q) := \lim_{n\to\infty} \mathrm{r}(2n,q) = (1-q^{-1})^2.$$

Moreover $|\mathrm{r}(2n,q) - \mathrm{r}(\infty,q)| = o(q_0^{-n})$ *for any* q_0 *such that* $1 < q_0 < \sqrt{q}$.

Proof. By [4, Lemma 1.3.10(b)] applied with the variable u replaced by u/q, the following equality holds for $|u|<1$:

$$\prod_{m\geq 1}\left(1-\frac{u^m}{q^m}\right)^{N(q;m)} \times \frac{(1-u/q)}{1-u} = 1.$$

Using this to rewrite the expression for $R(u)$ in (9) we see that, for $|u|<1$,

$$R(u) \;=\; \tfrac{(1-u/q)}{(1-u)(1+u/(q-1))}\textstyle\prod_{m\geq 1}\left((1+\frac{u^m}{q^m-1})(1-\frac{u^m}{q^m})\right)^{N(q;m)}.$$

Multiplying out the individual factors in the infinite product we obtain

$$R(u) \;=\; \tfrac{(1-u/q)}{(1-u)(1+u/(q-1))}\textstyle\prod_{m\geq 1}\left(1-\frac{u^m(u^m-1)}{q^m(q^m-1)}\right)^{N(q;m)}.$$

Thus $R(u)$ has the form $H(u)/(1-u)$ for $|u|<1$, where

$$H(u) \;=\; \tfrac{(1-u/q)}{(1+u/(q-1))}\textstyle\prod_{m\geq 1}\left(1-\frac{u^m(u^m-1)}{q^m(q^m-1)}\right)^{N(q;m)}.$$

Applying [4, Corollary 1.3.2 and Lemma 1.3.10(a)] to the infinite product in the expression for $H(u)$ we deduce that $H(u)$ converges absolutely on the disc $D(\sqrt{q}) = \{u\in\mathbb{C}\,|\,|u|<\sqrt{q}\}$ in the complex plane, and hence $H(u)$ is analytic in $D(\sqrt{q})$. Then, by [4, Lemma 1.3.3] it follows that $\mathrm{r}(\infty,q) := \lim_{n\to\infty}\mathrm{r}(2n,q)$ exists and equals $H(1)$, and moreover, $|\mathrm{r}(\infty,q)-\mathrm{r}(2n,q)| = o(q_0^{-n})$ for any q_0 such that $1<q_0<\sqrt{q}$. Finally, to determine $H(1)$, note that the infinite product in the expression for $H(u)$ takes the value 1 when $u=1$, and hence $H(1) = (1-\frac{1}{q})^2$. □

Proof of Theorem 1.2. The assertions about $\iota(n,q)$ follow from Lemma 4.1, while all assertions about the limiting behaviour of $\mathrm{r}(n,q)$ and $\mathrm{r}(n,q)$ follow from Corollary 4.2 and Lemma 5.2. □

References

[1] C. Altseimer and A. Borovik, Probabilistic recognition of orthogonal and symplectic groups. In: *Groups and Computation III*. Editors: W.M. Kantor and Á. Seress, de Gruyter, Berlin, New York (2001), pp. 1–20. With corrections in http://www.ma.umist.ac.uk/avb/pdf/alt-avb4.pdf. MR1829468 (2002e:20093)

[2] J. N. Bray, An improved method for generating the centralizer of an involution, *Arch. Math. (Basel)* **74** (2000), 241–245. MR1742633 (2001c:20063)

[3] R. W. Carter, *Finite groups of Lie type: Conjugacy classes and complex characters*, Wiley, Chichester, 1993. MR1266626 (94k:20020)

[4] J. E. Fulman, Peter M. Neumann and Cheryl E. Praeger, *A Generating Function Approach to the Enumeration of Matrices in Classical Groups over Finite Fields*, Memoirs of the American Mathematical Society **176** (2005), no. 830, vi+90 pp. MR2145026 (2006b:05125)

[5] Simon Guest and Cheryl E. Praeger, Proportions of 2-part orders of elements in finite classical groups, submitted. Available at arxiv.org/abs/1007.2983

[6] B. Hartley and T. O. Hawkes, *Rings, modules and linear algebra. A further course in algebra describing the structure of abelian groups and canonical forms of matrices through the study of rings and modules*. A reprinting. Chapman & Hall, London-New York, 1980. MR619212 (82e:00001)
[7] P. E. Holmes, S. A. Linton, E. A. O'Brien, A. J. E. Ryba, and R. A. Wilson, Constructive membership in black-box groups. *J. Group Theory* **11** (2008), 747–763. MR2466905 (2009i:20001)
[8] B. Huppert, *Endliche Gruppen I*, Springer, Berlin, 1967. MR0224703 (37:302)
[9] C.R. Leedham-Green and E.A. O'Brien, Constructive recognition of classical groups in odd characteristic, *J. Algebra* **322** (2009), 833–881. MR2531225 (2010e:20075)
[10] M. W. Liebeck and E. A. O'Brien, Finding the characteristic of a group of Lie type, *J. London Math. Soc.* **75** (2007), 741–754. MR2352733 (2008i:20058)
[11] Frank Lübeck, Alice C. Niemeyer, and Cheryl E. Praeger, Finding involutions in finite Lie type groups of odd characteristic, *J. Algebra* **321** (2009), 3397–3417. MR2510054 (2010e:20026)
[12] Peter M. Neumann and Cheryl E. Praeger, Cyclic matrices over finite fields, *J. London Math. Soc. (2)* **52** (1995), 263–284. MR1356142 (96j:15017)
[13] Christopher W. Parker and Robert A. Wilson, Recognising simplicity of black-box groups by constructing involutions and their centralisers, *J. Algebra* **324** (2010), 886–915. MR2659204 (2011j:20032)
[14] Cheryl E. Praeger and Ákos Seress, Probabilistic generation of finite classical groups in odd characteristic by involutions, *J. Group Theory* **14** (2011), 521–545. MR2818948

School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009, Australia
E-mail address: cheryl.praeger@uwa.edu.au

School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009, Australia – and – Department of Mathematics, The Ohio State University, Columbus, Ohio 43210
E-mail address: akos@math.ohio-state.edu