doi:10.1006/jabr.2000.8548, available online at http://www.idealibrary.com on IDEAL®

Cyclic Matrices in Classical Groups over Finite Fields

Peter M. Neumann

The Queen's College, Oxford OX1 4AW, United Kingdom

and

Cheryl E. Praeger

Department of Mathematics, UWA, Perth, Western Australia 6907, Australia

Communicated by Gernot Stroth

Received March 15, 2000

TO HELMUT WIELANDT FOR HIS 90TH BIRTHDAY WITH MUCH RESPECT AND MANY CONGRATULATIONS

1. INTRODUCTION

A $d \times d$ matrix X over a field F is said to be *cyclic* if $m_X(t) = c_X(t)$, where $m_X(t)$ is its minimal polynomial and $c_X(t)$ is its characteristic polynomial $\det(tI - X)$. This condition is equivalent to requiring the vector space F^d of $1 \times d$ row vectors over F to be cyclic as an $F\langle X\rangle$-module. In a previous paper [7] we showed that most $d \times d$ matrices over a finite field F are cyclic. The present work is a continuation of that. Its aim is to obtain good lower bounds on the proportion of cyclic matrices in the general linear group $\mathrm{GL}(d, F)$ and in various important subgroups of it. Although our motivation originated in our work on the design and analysis of algorithms for computing efficiently in matrix groups, the results have turned out to be of independent interest.

Define $\mathrm{Cyc}\,(d, q)$ to be the set of cyclic matrices in $\mathrm{M}(d, q)$, and define $\mathrm{Noncyc}(d, q)$ to be the set of non-cyclic matrices. The proportion $|\mathrm{Noncyc}(d, q)| \div q^{d^2}$ may be naturally thought of as the probability that a randomly chosen $d \times d$ matrix is not cyclic. In [7] we proved that

$$\mathrm{Prob}[X \in \mathrm{M}(d, q) \text{ is non-cyclic}] = q^{-3} + O(q^{-4}),$$

0021-8693/00 $35.00

and that $\mathrm{Noncyc}(d,q)$ is an algebraic subvariety of codimension 3 in $\mathrm{M}(d,q)$. Since many (though certainly not all) of the groups G with which we are concerned are close to being algebraic varieties (in the sense of being the points defined over F of an algebraic variety defined over the prime field), it is quite natural to expect that $G \cap \mathrm{Noncyc}(d,q)$ should be a subvariety of codimension 3 in G. There is no great difficulty dealing with $\mathrm{GL}(d,F)$ itself since it is the complement of the affine algebraic variety given by the polynomial equation $\det(X) = 0$. For other groups it is rather harder to turn geometric intuition into acceptable proof. Indeed, for some of the groups this intuition is misleading—for example, if G is an orthogonal group then $G \cap \mathrm{Noncyc}(d,q)$ is a subvariety of codimension 1. Moreover, some of the estimates that one obtains by geometric methods, although asymptotically very good as $q \to \infty$, tend to depend on d (compare [7, Sect. 7, first paragraph]), while others are inadequate for practical purposes when q is small (see, for example, [5]). Therefore in this paper, as in [7], we shall proceed more directly, using elementary linear algebra.

For ease of reference we shall refer to a group G as being a *classical* group associated with the dimension d and the field-size q if one of the following holds:

$$\mathrm{SL}(d,q) \leqslant G \leqslant \mathrm{GL}(d,q),$$
$$\mathrm{SU}(d,q) \leqslant G \leqslant \mathrm{GU}(d,q),$$
$$\mathrm{Sp}(d,q) \leqslant G \leqslant \mathrm{GSp}(d,q),$$
$$\Omega^{\varepsilon}(d,q) \leqslant G \leqslant \mathrm{GO}^{\varepsilon}(d,q).$$

Here the "general unitary group" $\mathrm{GU}(d,q)$ is the subgroup of $\mathrm{GL}(d,q^2)$ consisting of all matrices that preserve a given non-degenerate hermitian form up to scalar multiplication. The "general symplectic group" $\mathrm{GSp}(d,q)$ and the "general orthogonal group" $\mathrm{GO}^{\varepsilon}(d,q)$ are the subgroups of $\mathrm{GL}(d,q)$ consisting of all matrices that preserve a given symplectic form, or non-degenerate quadratic form, respectively, up to scalar multiplication. Our main results can be summarised as follows:

THEOREM. *If G is a classical subgroup of* $\mathrm{GL}(d,q)$ *and*

$$\nu(G) := \mathrm{Prob}[X \in G \textit{ is non-cyclic}] = |G \cap \mathrm{Noncyc}(d,q)| \div |G|,$$

then

$$\nu(G) \leqslant \begin{cases} q^{-3} + O(q^{-4}) & \textit{if } d \geqslant 3 \textit{ and } \mathrm{SL}(d,q) \leqslant G \leqslant \mathrm{GL}(d,q), \\ q^{-3} + O(q^{-4}) & \textit{if } d \geqslant 3 \textit{ and } \mathrm{SU}(d,q) \leqslant G \leqslant \mathrm{GU}(d,q), \\ (1+t(G))q^{-3} + O(q^{-4}) & \textit{if } d \textit{ is even, } d \geqslant 4, \textit{ and} \\ & \mathrm{Sp}(d,q) \leqslant G \leqslant \mathrm{GSp}(d,q), \\ \frac{1}{2}s(G)q^{-1} + O(q^{-2}) & \textit{if } d \textit{ is even, } d \geqslant 4, \textit{ and} \\ & \Omega^{\varepsilon}(d,q) \leqslant G \leqslant \mathrm{GO}^{\varepsilon}(d,q), \\ q^{-1} + O(q^{-2}) & \textit{if } d \textit{ and } q \textit{ are odd and} \\ & \Omega(d,q) \leqslant G \leqslant \mathrm{GO}(d,q), \end{cases}$$

where the constants implicit in the "Oh" notation depend on the type of the group G, but not on d.

We emphasize that this is only a summary of our main results. In particular, for the symplectic case $t(G)$ is defined in Section 7 and can take values 1 or 2. For example, when d is even and q is odd, $t(\mathrm{Sp}(d,q)) = 2$ and $t(\mathrm{GSp}(d,q)) = 1$. For the orthogonal case in even dimensions $s(G)$ is defined in Section 8 and can take values 1, 2, or 4 if q is odd, and values 1 or 2 if q is even. For example, when d is even and q is odd, $s(\Omega^{\varepsilon}(d,q)) = s(\mathrm{SO}^{\varepsilon}(d,q)) = 4$, $s(\mathrm{O}^{\varepsilon}(d,q)) = 2$, and $s(\mathrm{GO}^{\varepsilon}(d,q)) = 1$. Precise results are formulated as Theorem 3.1 for the general linear case, Theorem 6.1 for the unitary case, Theorem 7.1 for the symplectic case, Theorem 8.1 for even-dimensional orthogonal groups, and Theorem 9.1 for odd-dimensional orthogonal groups. It turns out that small-dimensional groups behave a little differently, interestingly so, from the general case. For the general linear, unitary, and symplectic groups we discuss this point within the relevant section, but small-dimensional orthogonal groups are treated separately in Section 10.

In [7] we gave both upper and lower bounds for the proportion of noncyclic matrices. We have decided to restrict ourselves to upper bounds here. To have included discussion and proofs of appropriate lower bounds would have added too much to the length of the paper. Besides, it is only the upper bounds that are needed for the applications we have in mind. In earlier stages of this work we were unable to prove usable bounds for the probabilities in some of the groups over small fields, especially the orthogonal groups. We have taken care to ensure that the bounds we now give are realistic. We are confident that they are good ones, not merely in the sense that they are of the right order of magnitude with the correct coefficients for the leading terms, but also in the sense that they can actually be used—for example, in the design and analysis of algorithms [9]. Small adjustments of the reasoning will also give the proportions of non-separable matrices, just as they do in [7], and they would give the proportions of non-semisimple matrices also. But again, for reasons of economy, we have left those out. The interested reader should have no difficulty adapting our methods to derive good estimates. Upper bounds for the probabilities of non-semisimple elements are given by Guralnick and Lübeck in [5] but their method does not give usable estimates when the field size q is small.

An alternative approach to the study of these probabilities uses generating functions. This method is used by Wall in [12], by Fulman in [2, 3], and by Fulman et al. in [4]. It gives far more precise results than ours, but unfortunately only for the groups $\mathrm{GL}(d,q)$, $\mathrm{U}(d,q)$, $\mathrm{Sp}(d,q)$, $\mathrm{O}^{\varepsilon}(d,q)$ themselves and not for any others of the related groups. For the applications to the analysis of algorithms in computational algebra that we have in mind, groups such as $\mathrm{SL}(d, q)$, $\mathrm{SU}(d, q)$, $\mathrm{GSp}(d, q)$, $\mathrm{SO}^{\varepsilon}(d, q)$, $\Omega^{\varepsilon}(d, q)$ are equally important, but it is not yet known whether, or how, the generating function methods might be adapted to give good results for them.

We thank Tim Wall and Jason Fulman for their interest and encouragement and many illuminating conversations. We thank Alice Niemeyer for explicit computations in certain small-dimensional orthogonal groups which both guided our thinking for Sections 8–10 and confirmed some of the results of Section 10. We also thank the Australian Research Council, the Engineering and Physical Sciences Research Council of the United Kingdom, and the Royal Society of London for grants which facilitated various stages of our collaboration on this project.

2. CYCLIC MATRICES, CYCLIC VECTORS, AND SOME INEQUALITIES

For the reader's convenience we recall here some of the basic facts about cyclic matrices. A fuller account can be found in [7]. Given a matrix $X \in \mathrm{M}(d, F)$ we define $F\langle X\rangle$ to be the subalgebra of $\mathrm{M}(d, F)$ generated by X, and we define $C_{\mathrm{M}}(X)$ to be its centraliser $\{Y \in \mathrm{M}(d, F) \mid XY = YX\}$. Thus $F\langle X\rangle$ consists of all polynomials in X, and $F\langle X\rangle \leqslant C_{\mathrm{M}}(X)$. The vector space V of $1 \times d$ row vectors over F is an $F\langle X\rangle$-module in a natural way, and may also be thought of as a module for the polynomial ring $F[t]$ (with t acting as right multiplication by X). A *cyclic vector* for X is an element $v_0 \in V$ such that the elements $v_0, v_0X, v_0X^2, \ldots$ span V. Such an element exists if and only if V is cyclic as $F\langle X\rangle$-module (or as $F[t]$-module). As indicated in Section 1, we call X cyclic if $c_X(t) = m_X(t)$. In fact X is cyclic in this sense if and only if there exists a cyclic vector for X in V.

THEOREM 2.1. *For $X \in \mathrm{M}(d, F)$ the following are equivalent*:

(1) $c_X(t) = m_X(t)$;

(2) *there is a cyclic vector for X in V*;

(3) $C(X) = F\langle X\rangle$;

(4) $\dim F\langle X\rangle = d$;

(5) $\dim C(X) = d$.

Let F be a finite field of order q. We will need the following upper bounds for the number of monic irreducible polynomials of a given degree over F.

LEMMA 2.2. *If $n_r := n_r(q) :=$ the number of monic irreducible polynomials of degree r over F, then $n_1 = q$, $n_2 = \frac{1}{2}(q^2 - q)$, $n_3 = \frac{1}{3}(q^3 - q)$, $n_4 = \frac{1}{4}(q^4 - q^2)$, and in general $n_r \leqslant (q^r - q)/r$ for $r \geqslant 2$.*

As in [7] there are some elementary estimates (depending upon the fact that $q \geqslant 2$) that we shall sometimes use without comment. Examples are

$$\sum_{r=m}^{m+k} q^{-r} < 2q^{-m} \leqslant q^{-(m-1)} \quad \text{and} \quad \sum_{r=m}^{n} \frac{1}{rq^r} < \sum_{r=m}^{n} \frac{1}{r(q^r-1)} < \frac{2}{mq^m}. \tag{2.3}$$

3. THE GENERAL LINEAR GROUP

If G is a group such that $\mathrm{SL}(d,F) \leqslant G \leqslant \mathrm{GL}(d,F)$ then it is a normal subgroup of $\mathrm{GL}(d,F)$ and there is a subgroup D of the multiplicative group $F^{\times}$ such that $G = \{X \in \mathrm{GL}(d,F) \mid \det X \in D\}$. Note that

$$|G| = (q^d-1)(q^d-q)(q^d-q^2)\cdots(q^d-q^{d-1})\frac{|D|}{q-1}.$$

In [7, Theorem 4.1] we showed that $q^{-d^2}|\mathrm{Noncyc}(d,q)| < \big((q^2-1)\times(q-1)\big)^{-1}$. The proportion of cyclic matrices in any group containing $\mathrm{SL}(d,q)$ is not much different from this.

THEOREM 3.1. *Suppose that $d \geqslant 3$ and that $\mathrm{SL}(d,q) \leqslant G \leqslant \mathrm{GL}(d,q)$. Define $\nu(G) := |G \cap \mathrm{Noncyc}(d,q)|/|G|$, so that $\nu(G)$ is the probability that a random matrix in G is not cyclic. Then $\nu(G) < 1/q(q^2-1)$.*

Remark 3.2. If $d=2$ then $G \cap \mathrm{Noncyc}(2,q)$ is the set of scalar matrices in G. For $\mathrm{SL}(2,q) \leqslant G \leqslant \mathrm{GL}(2,q)$ define

$$t(G) := \begin{cases} 1 & \text{if } (q-1)/|D| \text{ is odd,} \\ 2 & \text{otherwise.} \end{cases}$$

Then there are $t(G)|D|$ scalar matrices in G and, since $|G| = q(q^2-1)|D|$, we find that $\nu(G) = t(G)/q(q^2-1)$ in this case.

Proof of Theorem 3.1. A square matrix X is non-cyclic if and only if there exists a monic irreducible polynomial $f(t)$ with the property that $\dim \operatorname{Ker} f(X) \geqslant 2 \deg f$. For each r in the range $1 \leqslant r \leqslant \frac{1}{2}d$ we estimate the number of quadruples (f, V_0, X_0, X), in which

f is an irreducible monic polynomial of degree r and $f(0) \neq 0$,

V_0 is a $2r$-dimensional subspace of V,

$X_0 \in \mathrm{GL}(V_0)$ and $f(X_0) = 0$, and

$X \in GL(V)$, $X{\restriction}V_0 = X_0$, and $\det(X) \in D$.

First we count those quadruples that occur when $r = 1$. In this case $f(t) = t - \lambda$ for some $\lambda \in F^{\times}$. Thus the number of possible f is $q - 1$. The number of choices for V_0 is

$$\frac{(q^d - 1)(q^d - q)}{(q^2 - 1)(q^2 - q)}.$$

Given f and V_0, in this case X_0 is uniquely determined (it has to be λI_2). Since $d \geqslant 3$ the number of extensions X of X_0 to an appropriate mapping of the whole of V is

$$(q^d - q^2)(q^d - q^3) \cdots (q^d - q^{d-1}) \frac{|D|}{q - 1}.$$

Thus for $r = 1$ the number of quadruples is

$$(q - 1) \times \frac{(q^d - 1) \cdots (q^d - q^{d-1})}{(q^2 - 1)(q^2 - q)} \times \frac{|D|}{q - 1},$$

which is $|G|/q(q^2 - 1)$.

Next fix r in the range $2 \leqslant r \leqslant \frac{1}{2}d$. By Lemma 2.2, the number of possible f is at most $(q^r - q)/r$. The number of choices for V_0 is $(q^d - 1) \cdots (q^d - q^{2r-1})/|\mathrm{GL}(2r, q)|$. The matrix of the linear transformation X_0 is conjugate to $X_f \otimes I_2$, where X_f is the companion matrix of f. Thus the number of possible X_0 is $|\mathrm{GL}(2r, q) : C_{\mathrm{GL}(2r,q)}(X_f \otimes I_2)|$, which is $|\mathrm{GL}(2r, q)|/|\mathrm{GL}(2, q^r)|$. The number of extensions X of X_0 to the whole of V is then at most $(q^d - q^{2r}) \cdots (q^d - q^{d-1}) \times |D|/(q - 1)$ (it will be exactly this if $2r < d$ or if $|D| = q - 1$, but could be smaller if $2r = d$ and D is a proper subgroup of $F^{\times}$). Multiplying these numbers together and reorganizing the result in an obvious way we get that the number of quadruples is at most

$$|G| \times \frac{q^r - q}{r} \times \frac{1}{(q^{2r} - 1)(q^{2r} - q^r)}.$$

One checks easily that

$$\frac{q^r - q}{(q^{2r} - 1)(q^{2r} - q^r)} < \frac{1}{q^{3r}}.$$

Thus if $2 \leqslant r \leqslant \frac{1}{2}d$ then the number of quadruples is less than $|G|/rq^{3r}$.

Since every non-cyclic matrix appears in at least one quadruple we find that

$$\nu(G) = \frac{|G \cap \mathrm{Noncyc}(d, q)|}{|G|} \leqslant \frac{\text{number of quadruples}}{|G|}$$
$$< \frac{1}{q(q^2 - 1)} + \sum_{2 \leqslant r \leqslant d/2} \frac{1}{rq^{3r}} < \frac{1}{q(q^2 - 1)} + \frac{1}{q^6}.$$

Matrices that have an eigenspace of dimension $\geqslant 3$ will have been counted at least q^2+q+1 times by this method. An argument which we leave to the reader because it is very similar to one explained in [7, Sect. 4] yields that the upper bound can be reduced by more than q^{-6} on this account. Therefore $\nu(G) < 1/(q^3-q)$ as our theorem states.

4. GENERALITIES ABOUT CLASSICAL GROUPS

The theory of classical groups is well known but conventions vary and so we begin by specifying the notation and terminology that we shall use. We need, moreover, to extend some of Wall's theory of conjugacy classes [11] from the classical groups themselves to their "general" versions.

4.1. *Forms and Isometries*

For general theory of the classical groups the reader is referred to [1, 6, 10]. As in previous sections $V = F^d$, the space of $1 \times d$ row vectors. We use φ to denote a sesquilinear or bilinear form on V, and Q to denote a quadratic form. When dealing with quadratic forms Q we maintain the convention that φ is the polar form of Q, that is, that $Q(u+v) = Q(u) + Q(v) + \varphi(u,v)$. For any sesquilinear form with respect to an automorphism σ of F there is a $d \times d$ matrix A over F such that $\varphi(u,v) = uA(v^\sigma)^{\mathrm{tr}}$; for a bilinear form φ on V the equation is $\varphi(u,v) = uAv^{\mathrm{tr}}$; for a quadratic form Q it is $Q(u) = uAu^{\mathrm{tr}}$. Moreover, φ or Q is non-degenerate if and only if the corresponding matrix A is non-singular. We shall often identify forms with their corresponding matrices.

Matrices X in $\mathrm{GL}(d,F)$ act on V by right multiplication. This gives an action of $\mathrm{GL}(d,F)$ on the sets of sesquilinear, bilinear and quadratic forms defined by the formulae $\varphi^X(u,v) = \varphi(uX^{-1}, vX^{-1})$ and $Q^X(u) = Q(uX^{-1})$. Forms φ and φ', or Q and Q' are said to be *equivalent* or *isometric* if they lie in the same orbit. The corresponding matrix equation is $A = XA'X^{\mathrm{tr}}$. An invertible linear transformation T between subspaces U_1, U_2 of V is called an *isometry* if $\varphi(u,v) = \varphi(uT, vT)$, or $Q(u) = Q(uT)$, respectively, for all $u, v \in U_1$.

Let Φ (either φ or Q) be a non-degenerate sesquilinear, alternating bilinear, or quadratic form on V. We shall speak of V, or of the pair (V, Φ), as being a *unitary space*, a *symplectic space*, or an *orthogonal space*, as the case may be. The isometry group $\mathrm{Aut}(V, \Phi)$, usually written simply as $\mathrm{Aut}(V)$, will be one of the classical groups $\mathrm{U}(V)$, $\mathrm{Sp}(V)$, $\mathrm{O}^\varepsilon(V)$ according to the type of Φ. It is well known that if $X \in \mathrm{Sp}(V)$ then $\det X = 1$. The special unitary and special orthogonal groups are defined by

$$\mathrm{SU}(V) := \{X \in \mathrm{U}(V) \mid \det X = 1\},$$
$$\mathrm{SO}(V) := \{X \in \mathrm{O}(V) \mid \det X = 1\}.$$

In the orthogonal case we define $\Omega(V)$ to be the commutator subgroup of $\mathrm{O}(V)$. The reader should beware: notational conventions in respect of the orthogonal groups differ. Our usage follows that of Aschbacher [1, p. 89] and is different from that used by Taylor [10, p. 160].

4.2. *Similarities*

The notion of isometry needs to be extended in the following way. An invertible linear transformation $T\colon U_1 \to U_2$ between subspaces U_1 and U_2 of V will be said to be a *similarity* if there is a multiplier (sometimes called a *scaling factor*) $\mu \in F$ such that $\varphi(uT, vT) = \mu\varphi(u, v)$, or $Q(uT) = \mu Q(u)$, respectively, for all $u, v \in U_1$. Define the similarity group

$$\Delta(V) := \{g \in \mathrm{GL}(V) \mid \Phi(wg) = \mu(g)\Phi(w)\}$$

(where w denotes a pair (u, v) of vectors in the bilinear and unitary cases, a single vector if Φ is a quadratic form). The groups $\mathrm{GU}(V)$, $\mathrm{GSp}(V)$, $\mathrm{GO}^{\varepsilon}(V)$ (sometimes known as the "conformal" groups) are defined to be the similarity groups $\Delta(V)$ when (V, Φ) is a unitary, symplectic, or orthogonal space, respectively. The map $g \mapsto \mu(g)$ from the similarity group to $F^{\times}$ is a homomorphism whose kernel is the isometry group $\mathrm{Aut}(V)$. It is often convenient to define $\Omega(V)$ to be $\mathrm{SU}(V)$ and $\mathrm{Sp}(V)$ in the unitary and symplectic cases (compare [6, Chap. 2]) so that always $\Omega(V) = \mathrm{Aut}(V)'$ and our interest is in groups G such that $\Omega(V) \leqslant G \leqslant \Delta(V)$.

LEMMA 4.2.1. *Let V be a unitary, symplectic, or orthogonal space and let $\mu\colon \Delta(V) \to F^{\times}$ be its multiplier map. Then μ is surjective* **except** *when $\Delta(V) = \mathrm{GO}(V)$ and both d, q are odd, in which case* $\mathrm{Im}\,\mu = \{a^2 \mid a \in F^{\times}\}$.

Sketch proof. The surjectivity of μ can be checked very quickly when V is a two-dimensional symplectic or orthogonal space, or when V is a one-dimensional unitary space. In general, an even-dimensional symplectic or orthogonal space is an orthogonal direct sum of non-degenerate two-dimensional subspaces, and an arbitrary unitary space is an orthogonal direct sum of non-degenerate one-dimensional subspaces, and so the surjectivity of the multiplier map follows easily.

Suppose that both q and d are odd, and let Q be an orthogonal form on V with matrix A. If $X \in \mathrm{GO}(V)$ then $XAX^{\mathrm{tr}} = \mu(X)A$. Therefore $\mu(X)^d = \det(X)^2$, and since d is odd, $\mu(X)$ must be a square in $F^{\times}$. On the other hand, if b is a square in $F^{\times}$, say $b = a^2$, then the scalar matrix aI

is a member of $\mathrm{GO}(V)$ that has multiplier b. Thus if both d and q are odd then $\mathrm{Im}\,\mu = \{a^2 \mid a \in F^\times\}$.

A well-known theorem of Witt [1, p. 81; 10, p. 57] states that if U_1, U_2 are subspaces of V that meet the radical $V^\perp$ trivially, then every isometry $U_1 \to U_2$ may be extended to an automorphism of (V, φ). Its proof needs only very small adjustment to give the following lemma (compare [6, Lemma 4.1.1]).

LEMMA 4.2.2. *Let Φ be a (possibly degenerate) sesquilinear, alternating bilinear, or quadratic form on the vector space V, let U_1, U_2 be subspaces of V such that $U_1 \cap V^\perp = U_2 \cap V^\perp = \{0\}$, and let $\mu \in F^\times$. Suppose that μ is a square if Φ is a quadratic form Q and* $\dim(V)$ *is odd. Then every similarity $T\colon U_1 \to U_2$ with scaling factor μ can be extended to a similarity $X\colon V \to V$ with scaling factor μ.*

We shall also need the following variant of Witt's theorem.

LEMMA 4.2.3. *Let (V, Φ) be a unitary, symplectic, or orthogonal space and define*

$$k := \begin{cases} 1 & \textit{if } \Phi \textit{ is unitary}, \\ 0 & \textit{if } \Phi \textit{ is symplectic}, \\ 2 & \textit{if } \Phi \textit{ is orthogonal}. \end{cases}$$

(1) *If U is a non-degenerate subspace of V of dimension k then* $\mathrm{Aut}(U).\Omega(V) = \mathrm{Aut}(V)$.

(2) *If U a subspace of V of rank m and dimension n, where $2n - m \leqslant d - k$, then every isometry T of U may be extended to an isometry of V that lies in $\Omega(V)$.*

Proof. In (1) we have identified $\mathrm{Aut}(U)$ in the natural way with the subgroup $\{I_{U^\perp}\} \times \mathrm{Aut}(U)$ of $\mathrm{Aut}(V)$. The fact that this group is mapped surjectively by the natural homomorphism $\mathrm{Aut}(V) \to \mathrm{Aut}(V)/\Omega(V)$ is almost trivial in the unitary case, trivial in the symplectic case, and it follows easily in the orthogonal case from Taylor's description [10, p. 163] of $\Omega(V)$.

For (2) we use the fact that a subspace U of rank m and dimension n is contained in a non-degenerate subspace of dimension $2n - m$. (Let U_0 be the radical of U, and $V_0 := U_0^\perp$. Then $\dim U_0 = n - m$, V_0 has codimension $n - m$, and there is a subspace U_1 of dimension $n - m$ that complements V_0 in V. Define $U^* := U + U_1$. It is easy to see that U^* is non-degenerate, and of course $\dim U^* = 2n - m$ since $U \leqslant V_0$.) Then, since $2n - m \leqslant d - k$, there is a non-degenerate subspace W of V such that $U \leqslant W$ and $\dim(W) = d - k$. By Witt's theorem, an isometry T of U can be extended to an isometry of W and then to an isometry T^* of V fixing W setwise. By (1) we may choose $Y \in \mathrm{Aut}(W^\perp)$ (fixing W pointwise) so that Y has the same image as T^* in $\mathrm{Aut}(V)/\Omega(V)$. If $X := T^* Y^{-1}$ then X lies in $\Omega(V)$ and of course X is an extension of T as required.

4.3. *The General Unitary Group*

Recall that in the case of the unitary groups we take F to be $\mathbb{F}_{q^2}$. Define σ to be the automorphism of F of order 2 and $F_0 := \mathrm{Fix}(\sigma)$, so that F_0 may be identified with $\mathbb{F}_q$ and σ is the map $a \mapsto a^q$.

LEMMA 4.3.1. *Let Z be the group of all non-zero $d \times d$ scalar matrices over F. Then* $\mathrm{GU}(d, q) = \mathrm{U}(d, q).Z$.

Proof. Let $X \in \mathrm{GU}(V)$, let $\mu := \mu(X)$, and choose $u, v \in V$ such that $\varphi(u, v) \neq 0$. Then

$$\mu\varphi(u, v) = \varphi(uX, vX) = \varphi(vX, uX)^\sigma = \mu^\sigma \varphi(v, u)^\sigma = \mu^\sigma \varphi(u, v),$$

and so $\mu = \mu^\sigma$; that is, $\mu \in F_0$. For a scalar matrix aI_d, where $a \in F$, the multiplier $\mu(aI_d)$ is a^{1+q}. But the norm map $a \mapsto a^{1+q}$ is surjective from F to F_0, and it follows immediately that $\mathrm{GU}(d, q) = \mathrm{U}(d, q).Z$.

As a consequence of this lemma it will be sufficient for our purposes to consider groups G such that $\mathrm{SU}(V) \leqslant G \leqslant \mathrm{U}(V)$, that is to say, scaling factors will not arise. Let $X \in \mathrm{GL}(d, q)$, and define $\widetilde{X} := (X^\sigma)^{-\mathrm{tr}}$. The matrix X preserves the unitary form with matrix A if and only if $XA(X^\sigma)^{\mathrm{tr}} = A$. Pre-multiplying by A^{-1} and post-multiplying by $\widetilde{X}$ we see that a necessary condition for the existence of an X-invariant form is that X and $\widetilde{X}$ should be similar. In particular, X and $\widetilde{X}$ must have the same characteristic polynomial. For a monic polynomial f of degree d in $F[t]$ with non-zero constant coefficient c_0, define

$$\tilde{f}(t) := c_0^{-\sigma} t^d f^\sigma(t^{-1}).$$

The characteristic polynomial of $\widetilde{X}$ is $\tilde{c}_X(t)$ and so a necessary condition for X to preserve some unitary form is that $c_X(t) = \tilde{c}_X(t)$; it is not hard to see that for cyclic matrices this necessary condition turns out also to be sufficient. We shall therefore be interested in monic polynomials f that are *self-conjugate* in the sense that $f(0) \neq 0$ and $f = \tilde{f}$.

LEMMA 4.3.2. (1) *If f is a self-conjugate irreducible polynomial over F then* $\deg(f)$ *is odd.*

(2) *Let r be an odd positive integer. The number of self-conjugate monic irreducible polynomials $f \in F[t]$ which are of degree r is at most* $(q^r + 1)/r$.

Proof. Let f be a self-conjugate irreducible polynomial over F, and let λ be a root in some splitting field E. Of course $E = F(\lambda)$. Since λ^{-q} is another root of f the prescription $\tau_0\colon \lambda \mapsto \lambda^{-q}$ defines an automorphism of E over F. Now τ_0^2 is the Frobenius automorphism $\lambda \mapsto \lambda^{q^2}$, which, as is well known, generates $\mathrm{Aut}(E/F)$. It follows that the automorphism τ_0 must have odd order, and therefore the degree of f must be odd. This proves (1).

To prove (2) let E be a field extension of F of degree r. If f is to be self-conjugate and irreducible, then it must be the minimal polynomial of some element θ of E which generates E over F, and which has the property that θ^{-q} is an algebraic conjugate of it. The automorphism τ_0 defined above has the property that $\tau_0^2 \colon a \mapsto a^{q^2}$, and it follows that $\tau_0 \colon a \mapsto a^{q^{r+1}}$. Therefore $\theta^{q^{r+1}} = \theta^{-q}$, and so $\theta^{q(q^r+1)} = 1$. The map $a \mapsto a^{q(q^r+1)}$ is a homomorphism $E^\times \to E^\times$ whose kernel has order $q^r + 1$ and whose image therefore has order $q^r - 1$. Thus there are $q^r + 1$ elements θ in E such that $\theta^{q(q^r+1)} = 1$, but it is possible that not all of them generate E over F. Any self-conjugate irreducible polynomial f of degree r over F gives rise to a class of r algebraic conjugates of these elements θ, and therefore the number of such polynomials is at most $(q^r + 1)/r$.

LEMMA 4.3.3. *Let r be an odd positive integer, let V be an r-dimensional vector space over F, and let f be a self-conjugate monic irreducible polynomial of degree r over F.*

(1) *If X is a linear transformation of V with minimal polynomial f then there are unitary forms φ on V that are invariant under X.*

(2) *The general linear group* $\mathrm{GL}(V)$ *acts transitively on pairs (φ, X) where φ is a unitary form on V and X is an isometry of (V, φ) with minimal polynomial f.*

(3) *Let φ be a unitary form on V and let X be an isometry of (V, φ) with minimal polynomial f. If $C := \{Y \in \mathrm{GL}(V) \mid \varphi^Y = \varphi$ and $Y^{-1}XY = X\}$ then $|C| = q^r + 1$.*

Proof. Let X be a linear transformation of V with minimal polynomial f, and let $\Phi(X)$ be the set of sesquilinear forms on V that are preserved by X. Let V' denote the dual space of V and let $\widetilde{X} \colon V' \to V'$ denote the transformation X'^{σ}, where X' is the dual of X. Since $f = \tilde{f}$, V and V' are isomorphic as $F[t]$-modules on which t acts as X and $\widetilde{X}$, respectively. Moreover, since f is irreducible in $F[t]$, X and $\widetilde{X}$ act irreducibly. In particular, V, V' are cyclic modules and so the space $\mathrm{Hom}_{F[t]}(V, V')$ has dimension r. This space of homomorphisms is naturally identifiable with $\Phi(X)$, however, and so $\Phi(X)$ is a vector space of dimension r over F. Notice that since X is irreducible, every non-zero form in $\Phi(X)$ must be non-degenerate.

Let E be the splitting field of f over F (so that $E \cong \mathbb{F}_{q^{2r}}$), and let ξ be a root of f in E. We can identify V with E in such a way that X becomes the multiplication map $u \mapsto u\xi$. Recall that τ_0, the automorphism of F over F_0 defined before the previous lemma, maps ξ to ξ^{-q}. Now the automorphism σ of F over F_0 extends to an automorphism σ (the coincidence of names carries no danger here) of E over F_0, $\sigma \colon a \mapsto a^q$. Let $\tau := \tau_0 \sigma^{-1}$. This automorphism of E over F_0 has three relevant properties. First, the restriction of τ to F is our original automorphism σ. Second, $\xi^\tau = \xi^{-1}$;

that is, $\xi\xi^{\tau} = 1$. Third, $\tau^2 = 1$ because τ^2 fixes F pointwise and also fixes the generator ξ of E over F. For $a \in E$ define $\varphi_a(u, v) := \mathrm{trace}_{E/F}(uav^{\tau})$. From the fact that $\tau \restriction F = \sigma$ we get that φ_a is sesquilinear with respect to σ; it should also be clear that if $a \neq 0$ then φ_a is non-degenerate. Also,

$$\varphi_a(uX, vX) = \mathrm{trace}_{E/F}(u\xi a(v\xi)^{\tau}) = \mathrm{trace}_{E/F}(uav^{\tau}) = \varphi_a(u, v),$$

and so $\varphi_a \in \Phi(X)$. The forms φ_a for a in E form an r-dimensional vector space over F, and it follows that $\Phi(X) = \{\varphi_a \mid a \in E\}$. Now

$$\varphi_a(v, u) = \mathrm{trace}_{E/F}(vau^{\tau}) = \mathrm{trace}_{E/F}((v^{\tau}a^{\tau}u)^{\tau}) = \varphi_{a^{\tau}}(u, v)^{\sigma}$$

and so φ_a is hermitian if and only if $a \in K$, where K is the fixed field of τ. Since $|E : K| = 2$, K is the extension of F_0 of degree r. Thus there are precisely $q^r - 1$ unitary forms that are X-invariant.

The group $\mathrm{GL}(V)$ acts transitively by conjugation on linear transformations X with minimal polynomial f. To demonstrate (2) we need to prove therefore that the centraliser in $\mathrm{GL}(V)$ of such a transformation X is transitive on $\Phi(X)$. The elements of $\mathrm{GL}(V)$ which centralise X are the multiplications $u \mapsto u\alpha$ for $\alpha \in E^{\times}$. A form φ_a is transformed into the form φ_{ab}, where $b := \alpha\alpha^{\tau}$. Now $\alpha\alpha^{\tau}$ ranges over values of the norm map from $E^{\times}$ to $K^{\times}$ and this norm map is surjective. Therefore any two unitary forms that are invariant under X are equivalent under an element of $\mathrm{GL}(V)$ that centralises X. Moreover, $C = \{u \mapsto u\eta \mid \eta \in E^{\times} \text{ and } \eta\eta^{\tau} = 1\}$, and it follows immediately that C is cyclic and of order $q^r + 1$. This completes the proof of the lemma.

4.4. *Similarities of Bilinear Forms*

For $X \in \mathrm{GL}(d, F)$, the bilinear form φ with matrix A is X-invariant up to multiplication by μ if and only if $XAX^{\mathrm{tr}} = \mu A$. It follows that there is some non-degenerate bilinear form preserved by X up to multiplication by μ if and only if X is similar to $\mu X^{-\mathrm{tr}}$. For $\mu \in F^{\times}$ and for a monic polynomial f of degree d and with non-zero constant coefficient c_0 define $f^{*(\mu)}$ by the equation

$$f^{*(\mu)}(t) := c_0^{-1}t^d f(\mu t^{-1}).$$

Note that $(f^{*(\mu)})^{*(\mu)} = f$. Now the characteristic polynomial of $\mu X^{-\mathrm{tr}}$ is $c_X^{*(\mu)}(t)$ and so a necessary condition for X to preserve some non-degenerate bilinear form up to multiplication by the scaling factor μ is that $c_X(t) = c_X^{*(\mu)}(t)$. For preassigned non-zero values of μ we shall therefore be interested in monic polynomials $f \in F[t]$ that satisfy the condition

$$\mathrm{C}(\mu): \qquad f(0) \neq 0 \text{ and } f = f^{*(\mu)}.$$

If f is a polynomial satisfying $\mathrm{C}(\mu)$ and λ is a root of f of multiplicity m then so is μ/λ.

LEMMA 4.4.1. *Let φ be a non-degenerate bilinear form on V and let X be an invertible linear transformation of V which preserves φ up to multiplication by μ. If f is a monic polynomial such that $f(0) = c_0 \neq 0$ then* $\dim \operatorname{Ker} f(X) = \dim \operatorname{Ker} f^{*(\mu)}(X)$.

Proof. Let A be the matrix of φ. From the equation $XAX^{\mathrm{tr}} = \mu A$ it follows that $XA = A(\mu X^{-1})^{\mathrm{tr}}$, then that $X^i A = A((\mu X^{-1})^i)^{\mathrm{tr}}$, and hence that $f(X)A = Af(\mu X^{-1})^{\mathrm{tr}}$. Since A is invertible $f(X)$ and $f(\mu X^{-1})^{\mathrm{tr}}$ have the same rank and nullity. But then also $f(X)$ and $f(\mu X^{-1})$ have the same nullity, and so $\dim \operatorname{Ker} f(X) = \dim \operatorname{Ker} c_0^{-1} X^n f^{*(\mu)}(X)$, where $n :=$ deg (f); that is, $\dim \operatorname{Ker} f(X) = \dim \operatorname{Ker} f^{*(\mu)}(X)$, as required.

COROLLARY. *Let φ be a non-degenerate bilinear form on V and let X be an invertible linear transformation of V which preserves φ up to multiplication by μ. For $a \in F$ define V_a to be the eigenspace $\{v \in V \mid vX = av\}$. Then* $\dim V_\lambda = \dim V_{\mu/\lambda}$ *for all $\lambda \in F^\times$.*

LEMMA 4.4.2. *Let μ be a non-zero member of F, let $f \in F[t]$, and let* $r :=$ deg (f). *Suppose that f satisfies* $\mathrm{C}(\mu)$.

(1) *If f is irreducible then one of the following holds*:

$r = 1$, μ is a square in $F^\times$, and $f(t) = t \pm \lambda$ where $\lambda^2 = \mu$;

$r = 2$, μ is a non-square in $F^\times$, and $f(t) = t^2 - \mu$;

r is even and the roots of f in its splitting field occur in pairs λ, μ/λ.

(2) *If r is odd then $\mu = \lambda^2$ for some $\lambda \in F^\times$, and exactly one of $t - \lambda$, $t + \lambda$ has odd multiplicity as a divisor of $f(t)$.*

Proof. The mapping $\tau \colon \lambda \mapsto \mu/\lambda$ on the set of roots of f (in its splitting field) satisfies $\tau^2 = 1$, and λ is a fixed point of τ if and only if $\lambda^2 = \mu$. Since irreducible polynomials over finite fields are separable (1) follows easily.

Suppose that $f^{*(\mu)} = f$ and that deg f is odd, and let g be an irreducible factor of f in $F[t]$. Then $g^{*(\mu)}$ also divides f in $F[t]$, and with the same multiplicity, say m, as g. Hence, if $g^{*(\mu)} \neq g$ then $(g^{*(\mu)}g)^m$ makes an even contribution to the degree of f. If $g^{*(\mu)} = g$ then by (1), either g has even degree or $g(t) = t - \lambda$ where $\lambda^2 = \mu$. Since deg f is odd, μ must have a square root λ and, moreover, exactly one of $t - \lambda$, $t + \lambda$ must have odd multiplicity as a factor of $f(t)$.

LEMMA 4.4.3. *Let r be an even positive integer and let μ be a non-zero member of F. The number of irreducible monic polynomials $f \in F[t]$ which* *are of degree r and satisfy* C(μ) *is*

$\frac{1}{2}(q-1)$ *if* $r=2$, *q is odd and* μ *is a square in* $F^\times$,

$\frac{1}{2}(q+1)$ *if* $r=2$, *q is odd and* μ *is a non-square in* $F^\times$,

$\frac{1}{2}q$ *if* $r=2$ *and q is even*,

at most $(q^{r/2}+1)/r$ *if* $r>2$.

Proof. Let E be a field extension of F of degree r and let K be the extension of degree $\frac{1}{2}r$ contained in it. If f is to be monic irreducible and satisfy C(μ) then it must be the minimal polynomial of some element ξ of E, which generates E over F, and which has the property that μ/ξ is an algebraic conjugate of it. There is therefore an automorphism τ of E over F such that $\tau\colon \xi \mapsto \mu/\xi$. Then $\tau^2=1$ and so the fixed field of τ is K. Moreover, $N_{E/K}(\xi)=\xi\xi^\tau=\mu$. Now the norm $N_{E/K}$ is a surjective homomorphism from $E^\times$ to $K^\times$ whose kernel has order $q^{r/2}+1$. Therefore the number of elements ξ of E for which $N_{E/K}(\xi)=\mu$ is $q^{r/2}+1$. Perhaps not all of these generate E over F. Those that do may be partitioned into sets of r algebraic conjugates that have the same minimal polynomial. Therefore the number of monic irreducible polynomials satisfying C(μ) is always at most $(q^{r/2}+1)/r$. If $r=2$ then we require ξ such that $\xi^{q+1}=\mu$. Since $E^\times$ is cyclic of order q^2-1 and $\mu^{q-1}=1$ there are $q+1$ such ξ. If q is odd and μ is a square in F then two of these are $\pm\mu^{1/2}$ and the remaining $q-1$ generate E over F, and so the number of irreducible f is $\frac{1}{2}(q-1)$. If q is odd and μ is non-square in F then they all generate E over F, and the number of irreducible f is $\frac{1}{2}(q+1)$. If q is even then one of our ξ is $\mu^{1/2}$ and the remaining q generate E over F, and the number of irreducible f is $\frac{1}{2}q$.

Next we need a description of the bilinear forms preserved by irreducible matrices up to a scaling factor μ. Let r be an even positive integer, say $r=2m$, let V be an r-dimensional vector space over the finite field F, let $\mu\in F^\times$, and let f be a monic irreducible polynomial of degree r satisfying the condition C(μ). Let X be a linear transformation of V with minimal (and characteristic) polynomial f, so that X acts irreducibly on V. Define

$$\begin{aligned}\Phi_{\mathrm{Sp}}(\mu,X) &:= \{\varphi \mid \varphi \text{ is a non-degenerate alternating bilinear}\\ &\qquad\qquad \text{form on } V \text{ and } \varphi^X=\mu\varphi\},\\ \Phi_{\mathrm{O}}(\mu,X) &:= \{\varphi \mid \varphi \text{ is a non-degenerate symmetric bilinear}\\ &\qquad\qquad \text{form on } V \text{ and } \varphi^X=\mu\varphi\}.\end{aligned}$$

It is very easy to see directly that if $f(t) = t^2 - \mu$ (so that μ must be non-square and q must be odd) then $\Phi_{\mathrm{Sp}}(\mu, X) = \{0\}$ and $\Phi_{\mathrm{O}}(\mu, X)$ is a two-dimensional vector space over F: for then X may be taken to be $\begin{pmatrix} 0 & 1 \\ \mu & 0 \end{pmatrix}$ and we find that $X^{\mathrm{tr}}AX = \mu A$ if and only if $A = \begin{pmatrix} a & b \\ b & a/\mu \end{pmatrix}$. As it happens, however, this case is also covered by the following discussion.

To identify $\Phi_{\mathrm{Sp}}(\mu, X)$ and $\Phi_{\mathrm{O}}(\mu, X)$ let $K := \mathbb{F}_{q^m}$ and $E := \mathbb{F}_{q^r}$, so that $F \leqslant K \leqslant E$. Let ξ be a root of f in E and identify V with E in such a way that X becomes multiplication by ξ. Note that since $f(t)$ is irreducible in $F[t]$, ξ generates E over F. The condition $f = f^{*(\mu)}$ guarantees that μ/ξ is also a root of f. Since f is irreducible and $E = F(\xi)$ there is an automorphism τ of E over F mapping ξ to μ/ξ. If $f(t) = t^2 - \mu$ then τ is the identity map on E; otherwise τ is the automorphism of E of order 2 and $K = \mathrm{Fix}(\tau)$. If q is odd define $M := \{a \in E \mid a^\tau = -a\}$. If $f(t) \neq t^2 - \mu$ and q is odd then K is the 1-eigenspace of τ in V (or in E), M is the (-1)-eigenspace, and $V = K \oplus M$. Now for $a \in E$ define a function φ_a by

$$\varphi_a(u, v) := \mathrm{trace}_{E/F}(auv^\tau) \quad \text{for } u, v \in E.$$

LEMMA 4.4.4. *With the above notation*:

(1) *if* $f(t) = t^2 - \mu$ *then* $\Phi_{\mathrm{Sp}}(\mu, X) = \{0\}$ *and* $\Phi_{\mathrm{O}}(\mu, X) = \{\varphi_a \mid a \in E^\times\}$;

(2) *if* q *is odd and* $f(t) \neq t^2 - \mu$ *then* $\Phi_{\mathrm{Sp}}(\mu, X) = \{\varphi_a \mid a \in M^*\}$ *where* $M^* := M \backslash \{0\}$, *and* $\Phi_{\mathrm{O}}(\mu, X) = \{\varphi_a \mid a \in K^\times\}$;

(3) *if* q *is even* (*in which case* μ *has a square root in* F, *so* $f(t) \neq t^2 - \mu$) *then* $\Phi_{\mathrm{Sp}}(\mu, X) = \Phi_{\mathrm{O}}(\mu, X) = \{\varphi_a \mid a \in K\}$.

Proof. Let $\Phi(\mu, X)$ be the set of bilinear forms on V that are preserved by X up to multiplication by μ. Since X acts irreducibly on V, non-zero members of $\Phi_\mu(X)$ are non-degenerate. Let V' denote the dual space of V and let $X^*: V' \to V'$ denote the transformation $\mu X'$, where X' is the dual of X. Since $f = f^{*(\mu)}$, V and V' are isomorphic as $F[t]$-modules on which t acts as X and X^*, respectively. Moreover, being irreducible these are cyclic modules and so the space $\mathrm{Hom}_{F[t]}(V, V')$ has dimension r. This space of homomorphisms is naturally identifiable with $\Phi(\mu, X)$, however, and so $\Phi(\mu, X)$ is a vector space of dimension r over F.

Certainly φ_a, as defined above, is a non-degenerate bilinear form on E, that is, on V. Furthermore,

$$\varphi_a(uX, vX) = \mathrm{trace}(au\xi(v\xi)^\tau) = \mathrm{trace}(\mu auv^\tau) = \mu\varphi_a(u, v),$$

and so $\varphi_a \in \Phi(\mu, X)$. The forms φ_a for a in E form an r-dimensional vector space over F, and it follows that $\Phi(\mu, X) = \{\varphi_a \mid a \in E\}$. Now $\tau^2 = 1$ and therefore

$$\varphi_a(v, u) = \mathrm{trace}(avu^\tau) = \mathrm{trace}(a^\tau v^\tau u^{\tau^2}) = \mathrm{trace}(a^\tau v^\tau u);$$

that is, $\varphi_a(v, u) = \varphi_{a^\tau}(u, v)$. It follows immediately that if $f(t) = t^2 - \mu$ (so that μ must be a non-square, q must be odd, and τ is the identity map on E) then all elements of $\Phi(\mu, X)$ are symmetric and (1) holds; if q is odd and $f(t) \neq t^2 - \mu$ then φ_a is alternating if and only if $a \in M$ and φ_a is symmetric if and only if $a \in K$, so (2) holds, while if q is even then $\Phi_{\mathrm{Sp}}(\mu, X) = \Phi_{\mathrm{O}}(\mu, X) = \{\varphi_a \mid a \in K\}$, so (3) holds.

LEMMA 4.4.5. *Let r be an even positive integer, let V be an r-dimensional vector space over the finite field F, let $\mu \in F^\times$, and let f be a monic irreducible polynomial of degree r satisfying the condition $C(\mu)$. Define*

$$\Phi_{\mathrm{Sp}} := \{ (\varphi, X) \mid X \in \mathrm{GL}(V), f(X) = 0, \text{ and } \varphi \in \Phi_{\mathrm{Sp}}(\mu, X)\},$$

$$\Phi_{\mathrm{O}} := \{ (\varphi, X) \mid X \in \mathrm{GL}(V), f(X) = 0, \text{ and } \varphi \in \Phi_{\mathrm{O}}(\mu, X)\}.$$

If $f(t) \neq t^2 - \mu$ then the natural actions of GL(V) *on Φ_{Sp} and on Φ_{O} are transitive.*

Proof. The actions of $\mathrm{GL}(V)$ on Φ_{Sp} and on Φ_{O} are standard ones: if $Y \in \mathrm{GL}(V)$ then $Y: (\varphi, X) \mapsto (\varphi^Y, Y^{-1}XY)$, where $\varphi^Y(u, v) = \varphi(uY^{-1}, vY^{-1})$ for all $u, v \in V$. Identify V with E (the field $\mathbb{F}_{q^r}$) as above. As has already been used, the conjugation action of $\mathrm{GL}(V)$ is transitive on linear transformations X with minimal polynomial f and allows us to assume that X is multiplication by ξ, where $\xi \in E$ and $f(\xi) = 0$. Define $T := E^\times$ as a subgroup of $\mathrm{GL}(V)$ with action by multiplication. Then T is the centraliser of X in $\mathrm{GL}(V)$.

By the previous lemma, $\Phi(\mu, X) = \{\varphi_a \mid a \in K\}$. For $Y \in T$ we find that $(\varphi_a)^Y = \varphi_b$, where $b = a(YY^\tau)^{-1}$. Now the map $Y \mapsto YY^\tau$ is the norm map $N_{E/K}: E^\times \to K^\times$, which is surjective. Therefore T acts transitively on $\{\varphi_a \mid a \in K^\times\}$ and (if q is odd) on $\{\varphi_a \mid a \in M^*\}$, that is, on $\Phi_{\mathrm{Sp}}(\mu, X)$ and on $\Phi_{\mathrm{O}}(\mu, X)$. Since T centralises X, the actions of $\mathrm{GL}(V)$ on the sets Φ_{Sp} and Φ_{O} are transitive.

4.5. *Irreducible Matrices in General Orthogonal Groups*

It is well known that the orthogonal groups $\mathrm{O}^\varepsilon(d, q)$ contain no irreducible matrices if d is odd or if $\varepsilon = +$. One consequence of the following lemma is that the same is true for $\mathrm{GO}^\varepsilon(d, q)$ except perhaps if $d = 2$ and q is odd. As it happens, this is a genuine exception: the group $\mathrm{GO}^+(2, q)$ does contain irreducible matrices when q is odd—for example, taking $Q(x, y) := xy$ we find that the matrix $\left(\begin{smallmatrix} 0 & 1 \\ \mu & 0 \end{smallmatrix}\right)$ transforms Q to μQ, and is irreducible if μ is a non-square in $F^\times$.

Let r be an even positive integer, let V be an r-dimensional vector space over the finite field F, let $\mu \in F^\times$, and let f be a monic irreducible polynomial of degree r satisfying the condition $\mathrm{C}(\mu)$. Let X be a linear transformation of V with minimal polynomial f and define

$$\Psi(\mu, X) := \{Q \mid Q \text{ is a non-degenerate quadratic form on } V \text{ and } Q^X = \mu Q\}.$$

As in the previous subsection we identify V with E, where E is the splitting field of f over F (so that $|E : F| = \deg f = r$), in such a way that X becomes multiplication by ξ, where ξ is a root of f in E; we define also K to be the subfield of E such that $F \leqslant K \leqslant E$ and $|K : E| = \frac{1}{2}r$. Then for $a \in E$ we define a function Q_a by $Q_a(u) := \mathrm{trace}_{E/F}(auu^\tau)$ for all $u \in E$, where τ is the identity if $f(t) = t^2 - \mu$ and otherwise τ is the involutory automorphism of E whose fixed field is K.

Lemma 4.5.1. *With the above notation*:

(1) *if* $f(t) = t^2 - \mu$ *then* $\Psi(\mu, X) = \{Q_a \mid a \in E^\times\}$ *and* $|\Psi(\mu, X)| = q^r - 1$;

(2) *if* q *is odd and* $f(t) \neq t^2 - \mu$ *then* $\Psi(\mu, X) = \{Q_a \mid a \in K^\times\}$ *and* $|\Psi(\mu, X)| = q^{r/2} - 1$;

(3) *If* q *is even then* $\Psi(\mu, X) = \{Q_a \mid a \notin K\}$, $Q_a = Q_b$ *if and only if* $a - b \in K$, *and* $|\Psi(\mu, X)| = q^{r/2} - 1$.

Proof. By definition (or by polarisation—see, for example, [1, p. 77; 10, p. 54]) each $Q \in \Psi(\mu, X)$ yields a unique non-degenerate symmetric bilinear form in $\Phi_{\mathrm{O}}(\mu, X)$. Conversely, if $\mathrm{char}\, F$ is odd then also each non-zero symmetric bilinear form in $\Phi_{\mathrm{O}}(\mu, X)$ yields a unique quadratic form in $\Psi(\mu, X)$. Therefore (1) and (2) follow immediately from Lemma 4.4.4.

Suppose now that $\mathrm{char}\, F = 2$ (in which case μ is a square and $f(t) \neq t^2 - \mu$), that $Q_1, Q_2 \in \Psi(\mu, X)$, and that Q_1, Q_2 are associated with the same member of $\Phi_{\mathrm{O}}(\mu, X)$. Define $Q_0 := Q_1 - Q_2$. Then $Q_0 : V \to F$, $Q_0(u_1 + u_2) = Q_0(u_1) + Q_0(u_2)$, and $Q_0(au) = a^2 Q_0(u)$ for $a \in F$. A short calculation confirms that if $V_0 := \{u \in V \mid Q_0(u) = 0\}$ then V_0 is a subspace of codimension $\leqslant 1$ in V. Following through the fact that Q_1 and Q_2 are X-invariant up to multiplication by μ we find that V_0 is an X-invariant subspace of V. Since X is irreducible, $V_0 = V$ and hence $Q_1 = Q_2$. Thus each non-zero symmetric bilinear form in $\Phi_{\mathrm{O}}(\mu, X)$ can arise from at most one member of $\Psi(\mu, X)$ and so $|\Psi(\mu, X)| \leqslant |\Phi_{\mathrm{O}}(\mu, X)| = q^{r/2} - 1$. The functions Q_a certainly are quadratic forms and a similar calculation to that given in the proof of Lemma 4.4.4 for φ_a confirms that $Q_a \in \Psi(\mu, X)$. The symmetric bilinear form associated with Q_a is easily found to be $\varphi_{a'}$, where $a' = a + a^\tau$, and it follows immediately that $Q_a = Q_b$ if and only if a, b lie in the same additive coset of $\mathrm{Fix}(\tau)$, that is, of K, in E. Also, Q_a is non-degenerate if and only if $a \notin K$. Since there are therefore $q^{r/2} - 1$ distinct non-degenerate forms Q_a it follows that $|\Psi(\mu, X)| = q^{r/2} - 1$ and that $\Psi(\mu, X) = \{Q_a \mid a \notin K\}$.

LEMMA 4.5.2. *Let r be an even positive integer, let V be an r-dimensional vector space over the finite field F, let $\mu \in F^{\times}$, and let f be a monic irreducible polynomial of degree r satisfying the condition $C(\mu)$. If $f(t) \neq t^2 - \mu$ then*:

(1) *the natural action of* $\mathrm{GL}(V)$ *on pairs* (Q, X), *where X is a linear transformation of V with minimal polynomial f and where* $Q \in \Psi(\mu, X)$, *is transitive*;

(2) $\mathrm{type}(V) = -$ *for all* $Q \in \Psi(\mu, X)$.

Proof. The action of $\mathrm{GL}(V)$ on the set of pairs (Q, X) is a standard one: if $Y \in \mathrm{GL}(V)$ then $Y\colon (Q, X) \mapsto (Q^Y, Y^{-1}XY)$, where $Q^Y(u) = Q(uY^{-1})$ for all $u \in V$. Part (1) follows immediately from Lemma 4.4.5 for odd q. Suppose therefore that q is a power of 2. Identify V with E (the splitting field of f over F) as in the previous lemma, and let $T := E^{\times}$. Then T acts by multiplication on E and may be thought of as a subgroup of $\mathrm{GL}(V)$.

As has already been used, the conjugation action of $\mathrm{GL}(V)$ is transitive on linear transformations X with minimal polynomial f and allows us to assume that $X \in T$, in fact, that X is multiplication by ξ, where $f(\xi) = 0$. From Lemma 4.5.1 we know that $\Psi(\mu, X) = \{Q_a \mid a \notin K\}$ and $Q_a = Q_b$ if and only if $a - b \in K$. For $\eta \in T$ let $c := N_{E/K}(\eta)$. If $Y \in \mathrm{GL}(V)$ is multiplication by η then we find that $(Q_a)^Y = Q_b$, where $b = ac^{-1}$. If $a \in E\backslash K$, $c_1, c_2 \in K^{\times}$, and $c_1 \neq c_2$ then $ac_1 - ac_2 \notin K$. All $c \in K^{\times}$ occur as values of the norm map and so, starting from any $Q_a \in \Psi(\mu, X)$ and applying members of T, we get $q^{r/2} - 1$ distinct quadratic forms; that is, we get all of $\Psi(\mu, X)$. Therefore T acts transitively on $\Psi(\mu, X)$ and $\mathrm{GL}(V)$ acts transitively on the set of pairs (Q, X).

Transitivity implies, of course, that all the forms in $\Psi(\mu, X)$ have the same type. To identify that type we proceed as follows. For $Q \in \Psi(\mu, X)$ define $Z(Q) := \{u \in E^{\times} \mid Q(u) = 0\}$, the set of singular vectors with respect to Q, and for $u \in E^{\times}$ define $\Psi(u) := \{Q \in \Psi(\mu, X) \mid Q(u) = 0\}$. A quick calculation shows that if $\eta \in T$ and $Z(Q)\eta := \{u\eta \mid u \in Z(Q)\}$ then $Z(Q)\eta = Z(Q^Y)$, where $Y \in \mathrm{GL}(V)$ is multiplication by η; similarly, $\Psi(u)^Y = \Psi(u\eta)$. Since T acts transitively on $\Psi(\mu, X)$ it follows that $|Z(Q)|$ is the same number n for all $Q \in \Psi(\mu, X)$. Similarly, there exists m such that $|\Psi(u)| = m$ for all $u \in E^{\times}$. Counting pairs (Q, u) such that $Q \in \Psi(\mu, X)$, $u \in E^{\times}$, and $Q(u) = 0$ we find that $(q^{r/2} - 1)n = (q^r - 1)m$, so that $n = (q^{r/2} + 1)m$. For forms of type $+$ the number of singular vectors is $(q^{r/2} - 1)(q^{r/2-1} + 1)$ (see [10, Theorem 11.5]), which is not divisible by $q^{r/2} + 1$ unless $q = 3$ and $r = 2$. When $r = 2$ and q is odd, however, $Q_a(u) = 2auu^{\tau} \neq 0$, so that there are no non-zero isotropic vectors for Q_a, and this means that the type of Q_a is $-$. Thus Q_a has type $-$ in all cases, and this completes the proof of the lemma.

LEMMA 4.5.3. *Suppose that q is odd. Let μ be a non-square in $F^\times$ and let V be a two-dimensional vector space over F. For $\varepsilon \in \{+,-\}$ and $X \in \mathrm{GL}(V)$ with $X^2 = \mu I_2$ define*

$$\Psi^\varepsilon(\mu, X) := \{Q \in \Psi(\mu, X) \mid \mathrm{type}(Q) = \varepsilon\}.$$

(1) *If $X \in \mathrm{GL}(V)$ and $X^2 = \mu I$ then $|\Psi^+(\mu, X)| = |\Psi^-(\mu, X)| = \frac{1}{2}(q^2 - 1)$.*

(2) *For $\varepsilon \in \{+,-\}$ the natural action of $\mathrm{GL}(V)$ on pairs (Q, X), where $X \in \mathrm{GL}(V)$, $X^2 = \mu I_2$, and $Q \in \Psi^\varepsilon(\mu, X)$, is transitive.*

Proof. As before identify V with the degree-2 field extension E of F and X with multiplication by ξ, where $\xi \in E$ and $\xi^2 = \mu$. Let $T := E^\times$, so that $T \leqslant \mathrm{GL}(V)$ and T is the centraliser of X in $\mathrm{GL}(V)$. We know from Lemma 4.5.1 that $\Psi(\mu, X) = \{Q_a \mid a \in E^\times\}$ and $|\Psi(\mu, X)| = q^2 - 1$. In the natural action of T on $\Psi(\mu, X)$, if $\eta \in T$ and $Y \in \mathrm{GL}(V)$ is multiplication by η, then $(Q_a)^Y = Q_b$ where $b = a\eta^{-2}$. Consequently T has two orbits in $\Psi(\mu, X)$,

$$\{Q_a \mid a \text{ is square in } E^\times\} \text{ and } \{Q_a \mid a \text{ is non-square in } E^\times\},$$

each of size $\frac{1}{2}(q^2 - 1)$. We shall show that these are $\Psi^+(\mu, X)$ and $\Psi^-(\mu, X)$ in one order or the other.

To do this we study the equation $Q_a(u) = 0$, because it has a non-zero solution if and only if $\mathrm{type}(Q_a) = +$. This is the equation $au^2 + a^q u^{2q} = 0$, which may be re-written (for $u \neq 0$) as $(au^2)^{q-1} = -1$. Let ρ be a primitive root in E (i.e., a generator of the cyclic group $E^\times$), and choose k such that $a = \rho^k$. Now $-1 = \rho^{q^2-1)/2}$ and so there is a non-zero solution u to the equation $Q_a(u) = 0$ if and only if $\rho^{(q-1)(q+1)/2-k}$ has a $2(q-1)$th root in E, that is, if and only if $\frac{1}{2}(q+1) - k$ is even. Consequently there are singular vectors with respect to Q_a if and only if either $q \equiv 1 \pmod 4$ and a is a non-square in $E^\times$ or $q \equiv 3 \pmod 4$ and a is a square in $E^\times$. Thus if we define $\varepsilon' := (-1)^{(q-1)/2}$ then

$$\Psi^{-\varepsilon'}(\mu, X) = \{Q_a \mid a \text{ is square in } E^\times\},$$
$$\Psi^{\varepsilon'}(\mu, X) = \{Q_a \mid a \text{ is non-square in } E^\times\}.$$

Both parts of the lemma follow immediately.

LEMMA 4.5.4. *Let r be an even positive integer, let $\mu \in F^\times$, and let f be a monic irreducible polynomial of degree r satisfying the condition $\mathrm{C}(\mu)$.*

Let (V, Q) be an r-dimensional orthogonal space over F, and let X be a linear transformation of V such that $f(X) = 0$ and $Q^X = \mu Q$. Define

$$C := \{\, Y \in \mathrm{GL}(V) \mid Q^Y = Q \text{ and } XY = YX\}.$$

If $f(t) \neq t^2 - \mu$ then $|C| = q^{r/2} + 1$ and if $f(t) = t^2 - \mu$ then $|C| = 2$.

Proof. We use the notation introduced in the previous lemmas, and focus on the group T, the centraliser of X in $\mathrm{GL}(V)$, which is the subgroup of $GL(V)$ consisting of multiplications by elements η of $E^\times$. Now $C = T \cap \mathrm{O}(V) = \mathrm{Stab}_T(Q)$. In the proof of Lemma 4.5.2 it was shown that if $f(t) \neq t^2 - \mu$ then T is transitive on $\Psi(\mu, X)$, and so, since $|T| = q^r - 1$ and $|\Psi(\mu, X)| = q^{r/2} - 1$, it follows that $|C| = q^{r/2} + 1$. A very similar argument shows that if $f(t) = t^2 - \mu$ then $|C| = 2$.

5. RELEVANT PAIRS AND SEQUENCES

Our analysis of non-cyclic matrices in the classical groups will depend upon extending basic non-cyclic linear transformations on subspaces of V to similarities defined on the whole of V. The situation is as follows. Let Φ be a unitary, symplectic, or orthogonal form on V, let r be a positive integer, let $\mu \in F^\times$, and let f be a monic irreducible polynomial of degree r in $F[t]$. A pair (U, T) will be called a *relevant pair* (relative to all this data) if U is a $2r$-dimensional subspace of V and T is a similarity of $(U, \Phi\restriction U)$ with scaling factor μ such that $f(T) = 0$. Note that since f is irreducible and $\dim U = 2r$, non-trivial proper T-invariant subspaces of U are of dimension r; every element of $U\backslash\{0\}$ lies in a unique irreducible T-invariant subspace and therefore the number of such subspaces is $q^r + 1$. Note also that if U is not totally singular then f must be self-conjugate (in the sense that $f = \tilde{f}$ if Φ is unitary and $\mu = 1$, or $f = f^{*(\mu)}$ if Φ is symplectic or orthogonal) if T is to exist. Define $\operatorname{rank} U := 2r - \dim(U^\perp \cap U)$. Since $U^\perp \cap U$ is T-invariant its dimension is 0, r, or $2r$, and $\operatorname{rank} U$ is $2r$, r, or 0 accordingly. If Φ is an orthogonal form Q on V and $\operatorname{rank} U \neq 0$ then there is a naturally induced orthogonal form $\overline{Q}$ on U/U_0, where U_0 is $U \cap U^\perp$, the radical of U. In this case we define $\operatorname{type} U := \operatorname{type}(U/U_0, \overline{Q})$. We define pairs (U, T), (U', T') for the same data r, μ, f to be *similar* if $\operatorname{rank} U = \operatorname{rank} U'$ and (when Φ is an orthogonal form Q on V and U is not totally singular) also $\operatorname{type} U = \operatorname{type} U'$. There is a natural action $(U, T) \mapsto (UY, Y^{-1}TY)$ of the isometry group (indeed, even of the similarity group) of (V, Φ) on the set of relevant pairs. Obviously $\operatorname{rank} U$ is preserved, as also is $\operatorname{type} U$ when Φ is orthogonal and U is not totally singular. The next four lemmas give the basic information about relevant pairs needed later.

LEMMA 5.1. *Let r be an even positive integer, let U be a $2r$-dimensional vector space over F, let Φ be a unitary, symplectic, or orthogonal form on U, and let $T \in \mathrm{GL}(U)$. Suppose that $\Phi^T = \mu\Phi$ where $\mu \in F^\times$ and that $f(T) = 0$, where f is a monic irreducible polynomial of degree r and $f(t) \neq t^2 - \mu$ if Φ is orthogonal. Then there are precisely $q^{r/2} + 1$ totally singular T-invariant subspaces of dimension r.*

Proof. Suppose (seeking a contradiction) that all the irreducible T-invariant subspaces are totally singular. If Φ were a unitary form φ or an orthogonal form Q then there would exist $u \in U$ such that $\phi(u, u) \neq 0$ or $Q(u) \neq 0$, respectively, and the cyclic T-subspace $\langle u \rangle_T$ it generates would not be totally singular. Thus Φ must be a symplectic form φ. Let U_1, U_2 be distinct irreducible T-invariant subspaces and let $u_1 \in U_1$, $u_2 \in U_2$. Then $\langle u_1 + u_2 \rangle_T$ is also totally singular and hence $\varphi(u_1 + u_2, u_1T + u_2T) = 0$. But $\varphi(u_1, u_1T) = \varphi(u_2, u_2T) = 0$ and so $\varphi(u_1, u_2T) + \varphi(u_2, u_1T) = 0$; that is (since φ is alternating), $\varphi(u_1, u_2T) = \varphi(u_1T, u_2)$. Replacing u_2 by u_2T we find that $\varphi(u_1, u_2T^2) = \varphi(u_1T, u_2T) = \mu\varphi(u_1, u_2)$. It follows that $u_2T^2 - \mu u_2 \in U_1^\perp$ for all $u_2 \in U_2$. By Lemma 4.4.4(1), $f(t) \neq t^2 - \mu$ and so the restriction of $T^2 - \mu I$ to U_2 is non-singular. Consequently $U_2 \subseteq U_1^\perp$, which is false since φ is non-degenerate. This contradiction confirms that there must exist irreducible T-invariant subspaces that are not totally singular.

Let U_1 be such a subspace. Then U_1 is non-degenerate and if $U_2 := U_1^\perp$ then U_2 is also T-invariant of dimension r, and since $U = U_1 \oplus^\perp U_2$, also U_2 is non-degenerate. Note that if Φ is a quadratic form then $\operatorname{type} U_1 = \operatorname{type} U_2 = -$ by Lemma 4.5.2 since $f(t) \neq t^2 - \mu$. Suppose first that Φ is a unitary or symplectic form φ, or that q is odd and Φ is a quadratic form Q with associated polar form φ. Then, by Lemmas 4.3.3 and 4.4.4 we can choose $u_1 \in U_1\backslash\{0\}$ and $u_2 \in U_2\backslash\{0\}$ and then identify U_1 with $\{\lambda u_1 \mid \lambda \in E\}$ and U_2 with $\{\lambda u_2 \mid \lambda \in E\}$, where E is the field extension of F of degree r, such that $\varphi(\lambda_1 u_1, \lambda_2 u_1) = \varphi(\lambda_1 u_2, \lambda_2 u_2) = \mathrm{trace}_{E/F}(a\lambda_1\lambda_2^\tau)$, where τ is the involutory automorphism of E and $a \in E^\times$. Now let W_α be the T-invariant subspace generated by $u_1 + \alpha u_2$, where $\alpha \in E$, so that

$$W_\alpha = \{\lambda u_1 + \alpha\lambda u_2 \mid \lambda \in E\}.$$

For the restriction of φ to W_α we find that

$$\begin{aligned}\varphi(\lambda_1 u_1 + \alpha\lambda_1 u_2, \lambda_2 u_1 + \alpha\lambda_2 u_2) &= \varphi(\lambda_1 u_1, \lambda_2 u_1) + \varphi(\alpha\lambda_1 u_2, \alpha\lambda_2 u_2)\\ &= \mathrm{trace}(a\lambda_1\lambda_2^\tau) + \mathrm{trace}(a\alpha\lambda_1\alpha^\tau\lambda_2^\tau)\\ &= \mathrm{trace}(a(1 + \alpha\alpha^\tau)\lambda_1\lambda_2^\tau).\end{aligned}$$

Consequently W_α is totally singular if and only if $1 + \alpha\alpha^\tau = 0$; that is, $\alpha^{q^{r/2}+1} = -1$. Since the multiplicative group $E^\times$ is cyclic of order $q^r - 1$, for every element of the subfield K of index 2, and in particular for -1, the number of $(q^{r/2}+1)$th roots is $q^{r/2}+1$. Therefore precisely $q^{r/2}+1$ of the irreducible T-invariant subspaces are totally singular.

What remains to be dealt with is the case where q is even and Φ is a quadratic form Q. In this case, by Lemma 4.5.1(3), notation may be chosen as above so that $Q(\lambda u_1) = Q(\lambda u_2) = \mathrm{trace}_{E/F}(a\lambda\lambda^\tau)$, where $a \notin K = \mathrm{Fix}\tau$. It emerges as before that W_α is totally singular if and only if $1+\alpha\alpha^\tau = 0$, and hence that precisely $q^{r/2}+1$ of the irreducible T-invariant subspaces are totally singular, as the lemma states.

LEMMA 5.2. *Suppose that q is odd. Let μ be a non-square in $F^\times$, let $f(t) := t^2-\mu$, let (U, Q) be a four-dimensional orthogonal space over F, and let T be a similarity of U with scaling factor μ and minimal polynomial f.*

(1) *If* $\mathrm{type}(U) = +$ *then two of the two-dimensional T-invariant subspaces are totally singular, $\frac{1}{2}(q^2-1)$ are non-degenerate of positive type, and $\frac{1}{2}(q^2-1)$ are non-degenerate of negative type.*

(2) *If* $\mathrm{type}(U) = -$ *then none of the two-dimensional T-invariant subspaces are totally singular, $\frac{1}{2}(q^2+1)$ are non-degenerate of positive type, and $\frac{1}{2}(q^2+1)$ are non-degenerate of negative type.*

Proof. Suppose that $\mathrm{type}(U) = +$. The number of totally singular irreducible T-invariant subspaces may be found using the same method as in the preceding proof; the relevance of the assumption that $\mathrm{type}\, U = +$ is that when U is written as $U_1 \oplus U_2$, where U_1, U_2 are non-degenerate irreducible T-invariant subspaces, $\mathrm{type}\, U_1 = \mathrm{type}\, U_2$. What is different is that τ is the identity automorphism and therefore it emerges that the subspace W_α is totally singular if and only if $1+\alpha^2 = 0$. Since q is odd and $|E| = q^2$ there are precisely two choices for α, hence precisely two totally singular two-dimensional T-invariant subspaces of U. Let n be the number of two-dimensional T-invariant subspaces of positive type. There are $(q+1)(q^2-1)$ singular vectors in V and, since the minimal polynomial of T is irreducible of degree 2, each such vector u lies in a two-dimensional T-invariant subspace, namely $\langle u\rangle_T$. Of these, $2(q^2-1)$ lie in totally singular T-invariant subspaces. The remainder lie in subspaces of positive type, each of which contains $2(q-1)$. Thus $2(q-1)n + 2(q^2-1) = (q+1)(q^2-1)$ and so $n = \frac{1}{2}(q^2-1)$. There remain $(q^2+1) - 2 - \frac{1}{2}(q^2-1)$, that is, $\frac{1}{2}(q^2-1)$, irreducible T-invariant subspaces, which must be those of negative type. This proves (1).

If $\mathrm{type}(U) = -$ then maximal totally singular subspaces have dimension 1 and so there are no two-dimensional ones. Now a similar calculation to that in the preceding paragraph tells us that there are $\frac{1}{2}(q^2+1)$ non-degenerate irreducible T-invariant subspaces of positive type and the same number of negative type.

LEMMA 5.3. *Let (U, T), (U', T') be similar relevant pairs for the same data V, Φ, μ, r, f. Then there exists $Y \in \operatorname{Aut}(V)$ such that $(U, T)^Y = (U', T')$.*

Proof. The crux of the matter is to prove that there exists an isometry $Y_0\colon U \to U'$ such that $Y_0^{-1} T Y_0 = T'$. For, the theorem of Witt referred to in Section 4.2 then guarantees the existence of an isometry Y of (V, Φ) extending Y_0, hence having the required property. Define $r_0 := \operatorname{rank} U = \operatorname{rank} U'$. The proof of the existence of Y_0 is divided into cases according to the value of r_0.

Suppose first that $r_0 = 0$. Since T, T' have the same minimal polynomial f and $\dim U = \dim U'$, there is a linear transformation $Y_0\colon U \to U'$ such that $Y_0^{-1} T Y_0 = T'$, as required.

Suppose now that $r_0 = r$. Let $U_1 := U \cap U^{\perp}$. Then U_1 is T-invariant and irreducible. Choose U_2 to be any other irreducible T-invariant subspace of U. Clearly, $U = U_1 \oplus^{\perp} U_2$ and U_2 is non-degenerate. Similarly, there is a decomposition $U' = U_1' \oplus^{\perp} U_2'$ in which U_1', U_2' are T'-invariant and irreducible, $U_1' = U' \cap (U')^{\perp}$, and U_2' is non-degenerate. Let T_1, T_2 be the restrictions of T to U_1, U_2 and T_1', T_2' the restrictions of T' to U_1', U_2', respectively; also, let Φ_2, Φ_2' be the restrictions of Φ to U_2, U_2', respectively. There certainly exists $Y_1\colon U_1 \to U_1'$ such that $Y_1^{-1} T_1 Y_1 = T_1'$. By Lemmas 4.3.3, 4.4.5, 4.5.2, and 4.5.3 there exists $Y_2\colon U_2 \to U_2'$ such that $\Phi_2^{Y_2} = \Phi_2'$ and $Y_2^{-1} T_2 Y_2 = T_2'$. Then $Y_1 \oplus Y_2$ is an isometry $Y_0\colon U \to U'$ carrying T to T', as required.

When $r_0 = 2r$, that is, U, U' are non-degenerate, one special subcase needs to be distinguished: suppose first that $r = 1$ and Φ is a symplectic form φ. Then $f(t) = t - \lambda$ for some $\lambda \in F^{\times}$ and T, T' are scalar multiplication by λ. Certainly $\operatorname{Sp}(V, \varphi)$ is transitive on non-degenerate 2-spaces and any isometry Y mapping U to U' carries T to T'. Suppose, then, that $r > 1$ or that $r = 1$ and Φ is unitary or orthogonal. From Lemma 5.1 or 5.2 (or the first parts of their proofs) there exist non-degenerate irreducible T-invariant subspaces U_1 of U and U_1' of U'. In the orthogonal case, if $r = 1$ or if $r = 2$ and $f(t) = t^2 - \mu$ then U_1, U_1' may be chosen to have negative type, while if $r \geqslant 2$ and $f(t) \neq t^2 - \mu$ then U_1, U_1' must have negative type by Lemma 4.5.2. Define $U_2 := U \cap U_1^{\perp}$, $U_2' := U' \cap (U_1')^{\perp}$. Then $U = U_1 \oplus^{\perp} U_2$, $U' = U_1' \oplus^{\perp} U_2'$, U_2 U_2' are non-degenerate irreducible T-invariant subspaces, and in the orthogonal case, since $\operatorname{type} U = \operatorname{type} U'$ by assumption and $\operatorname{type} U_1 = \operatorname{type} U_1' = -$, also $\operatorname{type} U_2 = \operatorname{type} U_2'$. By Lemmas 4.3.3, 4.4.5, and 4.5.3 there exist isometries $Y_1\colon U_1 \to U_1'$, $Y_2\colon U_2 \to U_2'$ carrying the relevant restrictions of T to those of T' and we may take $Y_0\colon U \to U'$ to be $Y_1 \oplus Y_2$. This completes the proof of the lemma.

LEMMA 5.4. *Let (U, T) be a relevant pair for the same data V, Φ, μ, r, f, and let C be the centraliser of T in* $\mathrm{Aut}(U, \Phi\restriction U)$. *Define*

$$s := \begin{cases} 2r & \text{if } \Phi \text{ is a unitary form } \varphi, \\ r & \text{otherwise,} \end{cases}$$

so that $|F| = q^s$. Then:

(1) *if U is totally singular then $|C| = q^s(q^s - 1)(q^{2s} - 1)$;*

(2) *if* $\mathrm{rank}(U) = r$ *and in the orthogonal case $f(t) \neq t^2 - \mu$, then $|C| = q^s(q^s - 1)(q^{s/2} + 1)$;*

(3) *if* $\mathrm{rank}(U) = r = 2$, *Φ is an orthogonal form Q, and $f(t) = t^2 - \mu$, then $|C| = 2q^2(q^2 - 1)$;*

(4) *if U is non-degenerate and in the orthogonal case $r \geqslant 2$ and $f(t) \neq t^2 - \mu$, then $|C| = q^{s/2}(q^s - 1)(q^{s/2} + 1)$;*

(5) *if U is non-degenerate, $r = 2$, $f(t) = t^2 - \mu$, and Φ is an orthogonal form Q, then $|C| = 2(q^2 - \varepsilon)$, where $\varepsilon :=$* $\mathrm{type}(U)$.

Proof. (1) If U is totally singular then $\mathrm{Aut}(U, \Phi\restriction U) = \mathrm{GL}(U)$, and so $C \cong \mathrm{GL}(2, q^s)$, whose order is $q^s(q^s - 1)(q^{2s} - 1)$.

(2), (3) Suppose that $\mathrm{rank}(U) = r$. Let $U_1 := U \cap U^{\perp}$, so that U_1 is r-dimensional and T-invariant, and let U_2 be a T-invariant complement for U_1. Thus $U = U_1 \oplus^{\perp} U_2$. Now let W_2 be any T-invariant complement for U_1. There are $|F|^r$, that is, q^s, choices for W_2 and in the orthogonal case they all have the same type. If Y_1: $U_1 \to U_1$ and Y_2: $U_2 \to W_2$ are linear isometries that commute with the action of T then $Y_1 \oplus Y_2 \in C$; moreover, every member of C arises in this way. There are $q^s - 1$ possibilities for Y_1. It follows from Lemmas 4.3.3, 4.4.5, and 4.5.4 that the number of linear isometries $U_2 \to W_2$ commuting with the action of T is $q^{s/2} + 1$ unless Φ is an orthogonal form Q and $f(t) = t^2 - \mu$, in which case it is 2. Therefore $|C| = q^s(q^s - 1)(q^{s/2} + 1)$ in case (2) and $|C| = 2q^2(q^2 - 1)$ in case (3).

(4) Suppose now that U is non-degenerate and if Φ is an orthogonal form Q then $r \geqslant 2$ and $f(t) \neq t^2 - \mu$. There is a decomposition $U = U_1 \oplus^{\perp} U_2$ where U_1, U_2 are T-invariant, r-dimensional, and non-degenerate. By Lemma 4.6.2 there are $(q^s + 1) - (q^{s/2} + 1)$, that is, $q^{s/2}(q^{s/2} - 1)$, non-degenerate r-dimensional T-invariant subspaces. Let W_1 be any such and let $W_2 := U \cap W_1^{\perp}$. By Lemma 4.5.2, if Φ is an orthogonal form Q then $\mathrm{type}(U_1) = \mathrm{type}(U_2) = \mathrm{type}(W_1) = \mathrm{type}(W_2) = -$. We obtain elements of C from linear isometries $U_1 \to W_1$ and $U_2 \to W_2$ that commute with the action of T. By Lemmas 4.3.3, 4.4.5, and 4.5.4 there are $q^{s/2} + 1$ such maps $U_1 \to W_1$ and the same number $U_2 \to W_2$. As we have seen, there are $q^{s/2}(q^{s/2} - 1)$ choices for W_1 (and therefore for the pair W_1, W_2), and so $|C| = q^{s/2}(q^{s/2} - 1)(q^{s/2} + 1)^2 = q^{s/2}(q^s - 1)(q^{s/2} + 1)$.

(5) Suppose lastly that U is non-degenerate, $r = 2$, $f(t) = t^2 - \mu$, and Φ is an orthogonal form Q, and define $\varepsilon := \mathrm{type}(U)$. By Lemma 5.2 there are $\frac{1}{2}(q^2 - \varepsilon)$ two-dimensional T-invariant subspaces of U of type $+$. Let U_1 be one of them and let $U_2 := U \cap U_1^{\perp}$ so that $U = U_1 \oplus^{\perp} U_2$, where U_2 is T-invariant of dimension 2 and $\mathrm{type}(U_2) = \varepsilon$. Now let W_1 be any two-dimensional T-invariant subspace of U of type $+$ and let $W_2 := U \cap W_1^{\perp}$. Then also W_2 is T-invariant, $\mathrm{type}(W_2) = \varepsilon$, and $U = W_1 \oplus^{\perp} W_2$. It follows from Lemma 4.5.4 that there are two linear isometries $U_1 \to W_1$ and two linear isometries $U_2 \to W_2$ that commute with the action of T. Putting such maps together gives a linear isometry $U \to U$ that commutes with T, that is, an element of C, and every element of C arises this way. Thus $|C| = \frac{1}{2}(q^2 - \varepsilon) \times 2 \times 2 = 2(q^2 - \varepsilon)$. This completes the proof of the lemma.

In our theorems we shall have a group G such that $\Omega(V) \leqslant G \leqslant \Delta(V)$, where

$$\Omega(V) := \begin{cases} \mathrm{SU}(d, q) & \text{if } \Phi \text{ is a unitary form } \varphi, \\ \mathrm{Sp}(d, q) & \text{if } \Phi \text{ is a symplectic form } \varphi, \\ \Omega^{\varepsilon}(d, q) & \text{if } \Phi \text{ is an orthogonal form } Q \text{ of type } \varepsilon, \end{cases}$$

and $\Delta(V)$ is the group of all similarities of (V, Φ). The map $\mu\colon \Delta(V) \to F^{\times}$, $X \mapsto \mu(X)$, where, as in Section 4, $\mu(X)$ is the scaling factor associated with X, is a homomorphism. The natural homomorphism $\Delta(V) \to \Delta(V)/\Omega(V)$ will be denoted $X \mapsto \overline{X}$. Note that since $\Omega(V) \leqslant \mathrm{Aut}(V) = \mathrm{Ker}(\mu)$, μ induces a homomorphism $\Delta(V)/\Omega(V) \to F^{\times}$ which will also be denoted by μ. For the proofs of the theorems we shall count sequences $(\rho, r, f, V_0, X_0, X)$ where:

$\rho \in G/\Omega(V)$;

$1 \leqslant r \leqslant \frac{1}{2}d$;

f is a monic irreducible polynomial of degree r;

V_0 is a $2r$-dimensional subspace of V;

X_0 is a similarity of V_0 such that $f(X_0) = 0$ and $\mu(X_0) = \mu(\rho)$; and

X is an extension of X_0 to a similarity of V such that $\overline{X} = \rho$.

These will be called *relevant* sequences. The point is that the last entry of a relevant sequence is non-cyclic, and every non-cyclic matrix appears in at least one such sequence. Therefore

$$|G \cap \mathrm{Noncyc}(d, q)| \leqslant |\{\text{relevant sequences}\}|$$

and we shall seek estimates for the number of relevant sequences. In such a sequence the pair (V_0, X_0) is a relevant pair as defined above. Let (U, T) be a relevant pair for the data μ, r, f. If (V_0, X_0) is similar to (U, T) then we shall say that the sequence $(\rho, r, f, V_0, X_0, X)$, where $\mu(\rho) = \mu$, is *of type* (U, T).

LEMMA 5.5. *Suppose that* $\mu \in F^{\times}$, $1 \leqslant r \leqslant \frac{1}{2}d$, f *is a monic irreducible polynomial of degree* r, *and* (U, T) *is a relevant pair for the data* V, Φ, μ, r, f. *Define*

$$r_0 := \operatorname{rank}(U),$$

$$k := \begin{cases} 1 & \textit{if } \Phi \textit{ is unitary}, \\ 0 & \textit{if } \Phi \textit{ is symplectic}, \\ 2 & \textit{if } \Phi \textit{ is orthogonal}, \end{cases}$$

$$C := \{Y \in \operatorname{Aut}(U, \Phi{\restriction}U) \mid Y^{-1}UY = U\}.$$

Then the number of relevant sequences of type (U, T) *is* $c|\Omega(V)|/|C|$, *where*:

(1) *either* $c = 0$ *or* c *divides* $|\operatorname{Aut}(V) : \Omega(V)|$;

(2) *if* $4r - r_0 \leqslant d - 1$ *and in the orthogonal case, either* $\dim(V)$ *is even or* μ *is a square in* $F^{\times}$, *then* $c = 1$.

Proof. Suppose, for the moment, that relevant sequences $(\rho, r, f, V_0, X_0, X)$ of type (U, T) exist. Lemma 5.3 tells us that $\operatorname{Aut}(V)$ acts transitively on the set of relevant pairs similar to (U, T) and so their number is $|\operatorname{Aut}(V) : H|$, where H is the stabiliser of (U, T) in $\operatorname{Aut}(V)$. Define

$$K := \{Y \in \operatorname{Aut}(V) \mid uY = u \text{ for all } u \in U\}.$$

Then $K \trianglelefteqslant H$ and, by Witt's theorem, $H/K \cong C$. Define $K_0 := K \cap \Omega(V)$. Given a relevant sequence (ρ, r, f, U, T, X), a sequence (ρ, r, f, U, T, X') is another if and only if $\rho(X) = \rho(X')$ and $X{\restriction}U = X'{\restriction}U$, that is, if and only if X, X' lie in the same coset of K_0. Therefore the number of relevant sequences $(\rho, r, f, V_0, X_0, X)$ of type (U, T) is $|\operatorname{Aut}(V) : H| \times |K_0|$. Since

$$|\operatorname{Aut}(V) : H|.|K_0| = \frac{|\operatorname{Aut}(V)|}{|C|} \times \frac{|K_0|}{|K|} = \frac{|\Omega(V)|}{|C|} \times \frac{|\operatorname{Aut}(V)|}{|\Omega(V)|} \times \frac{|K_0|}{|K|}$$

and K/K_0 is isomorphic to a subgroup of $\operatorname{Aut}(V)/\Omega(V)$, the number we are seeking is $c|\Omega(V)|/|C|$, where c is the index $|\operatorname{Aut}(V)/\Omega(V) : K/K_0|$. This proves (1).

Suppose now that $4r - r_0 \leqslant d - 1$ and, in the orthogonal case, that either $\dim(V)$ is even or μ is a square in $F^{\times}$. There exists a non-degenerate subspace W of V containing U and of codimension k. By Lemma 4.2.2, T can be extended to a similarity of W with multiplier $\mu(\rho)$ and then to a similarity Y of V with multiplier $\mu(\rho)$. Define $\rho' := \overline{Y}\rho^{-1}$. Then $\rho' \in \operatorname{Aut}(V)/\Omega(V)$ and by Lemma 4.2.3, there exists $Y' \in \operatorname{Aut}(W^{\perp})$ (thought of as an element of $\operatorname{Aut}(V)$ fixing W pointwise) such that $\overline{Y'} = \rho'$. If $X := Y(Y')^{-1}$ then $\overline{X} = \rho$ and $X{\restriction}U = T$. Therefore $c \neq 0$. Define $L := \operatorname{Aut}(W^{\perp}) \leqslant \operatorname{Aut}(V)$, so that, by Lemma 4.2.3, $\Omega(V).L = \operatorname{Aut}(V)$. Since $L \leqslant K$ this implies that $\Omega(V).K = \operatorname{Aut}(V)$, hence that $K/K_0 = \operatorname{Aut}(V)/\Omega(V)$. Thus $c = 1$, as required.

6. NON-CYCLIC MATRICES IN UNITARY GROUPS

Recall notation from Section 4.3: throughout this section we take F to be $\mathbb{F}_{q^2}$. We take σ to be the involutory automorphism of F and F_0 to be its fixed field, so that $F_0 = \mathbb{F}_q$. We take V to be the F-vector space F^d, φ to be a unitary form on V, and G to be a group such that $\mathrm{SU}(d, q) \leqslant G \leqslant \mathrm{GU}(d, q)$; that is, $\mathrm{SU}(V) \leqslant G \leqslant \mathrm{GU}(V)$.

THEOREM 6.1. *Suppose that $d \geqslant 3$. If $\mathrm{SU}(d, q) \leqslant G \leqslant \mathrm{GU}(d, q)$ and $\nu(G)$ is the probability that a random matrix in G is not cyclic, then*

$$\nu(G) < \begin{cases} \dfrac{q+3}{q^2(q^2-1)} & \textit{if } d = 3, \\ \dfrac{q^2+2}{q^2(q-1)(q^2+1)} & \textit{if } d \geqslant 4. \end{cases}$$

In particular, $\nu(G) < q^{-3} + O(q^{-4})$.

Remark 6.2. As in the case of the general linear group, the situation for $d = 2$ is different. In fact, if $\mathrm{U}(2, q) \leqslant G \leqslant \mathrm{GU}(2, q)$ then $\nu(G) = |Z \cap G|/|G|$, where Z is the group of non-zero scalar matrices, and so we find that $\nu(G) = t(G)/q(q^2 - 1)$, where $t(G) = 1$ if q is even or G contains matrices with non-square determinant, and $t(G) = 2$ if q is odd and all elements of G have square determinant.

The remainder of this section is devoted to the proof of Theorem 6.1. By Lemma 4.3.1, $\mathrm{GU}(d, q) = \mathrm{U}(d, q).Z$ where Z is the group of all non-zero $d \times d$ scalar matrices over F. Therefore

$$\nu(G) = \nu(G.Z) = \nu(H.Z) = \nu(H),$$

where $H := G.Z \cap \mathrm{U}(d, q)$, and so we may (and shall) assume that $G \leqslant \mathrm{U}(d, q)$.

Let D be the image of the determinant map $G \to F^\times$, so that D is a subgroup of Z_{q+1}, where $Z_{q+1} := \{a \in F^\times \mid a^{1+q} = 1\}$. Relevant sequences as described in Section 5 take the form (a, r, f, V_0, X_0, X) where $a \in D$, $\det(X) = a$, and otherwise the entries are as specified there. Given r and r_0 let k_{r, r_0} be the number of monic irreducible polynomials f that can arise if relevant pairs (U, T) for the data r, r_0, f are to exist. If $r_0 = 0$, so that U is totally singular, then this is simply the number of monic irreducible polynomials $f(t)$ of degree r over F with $f(0) \neq 0$; thus $k_{r,0} \leqslant (q^{2r} - 1)/r$. If $r_0 > 0$ then f must not only be monic and irreducible but must also be self-conjugate (in the sense that $f = \tilde{f}$ as in Section 4.3) and therefore from Lemma 4.3.2 we know that r must be odd and $k_{r, r_0} \leqslant (q^r + 1)/r$. By Lemma 5.5, if a, r, r_0, and f are given and U, T, and C are as specified there, then the number of relevant sequences is at most $c_{r, r_0}|\mathrm{SU}(d, q)|/|C|$, where $c_{r,r_0} := 1$ if $4r - r_0 < d$ and $c_{r,r_0} := q+1$ if $4r - r_0 = d$. Since there are $|D|$ choices for a and $|D|\,|\mathrm{SU}(d,q)| = |G|$, for given r, r_0, and f the number of relevant sequences is at most $c_{r,r_0}|G|/|C|$. Thus

$$|\text{relevant sequences}| \leqslant |G| \sum_{r,r_0} \frac{k_{r,r_0} c_{r,r_0}}{|C|},$$

and so $\nu(G) \leqslant \sum_{r,r_0} k_{r,r_0} c_{r,r_0}/|C|$, where the sum is over pairs r, r_0 such that r_0 is $2r$, r, or 0. Using Lemma 4.5.4 and our bounds for k_{r,r_0} and c_{r,r_0} we therefore have that

$$\begin{aligned}\nu(G) &\leqslant \frac{q+1}{q(q^2-1)(q+1)} + \sum_{\substack{3\leqslant r<d/2,\\ r\,\text{odd}}} \frac{q^r+1}{rq^r(q^{2r}-1)(q^r+1)} \\ &\quad + \sum_{\substack{1\leqslant r<d/3,\\ r\,\text{odd}}} \frac{q^r+1}{rq^{2r}(q^{2r}-1)(q^r+1)} + \sum_{1\leqslant r<d/4} \frac{q^{2r}-1}{rq^{2r}(q^{2r}-1)(q^{4r}-1)} + \nu' \\ &= \frac{1}{q(q^2-1)} + \sum_{\substack{3\leqslant r<d/2,\\ r\,\text{odd}}} \frac{1}{rq^r(q^{2r}-1)} \\ &\quad + \sum_{\substack{1\leqslant r<d/3,\\ r\,\text{odd}}} \frac{1}{rq^{2r}(q^{2r}-1)} + \sum_{1\leqslant r<d/4} \frac{1}{rq^{2r}(q^{4r}-1)} + \nu',\end{aligned}$$

where ν' accounts for terms (if any) for which $4r - r_0 = d$.

Suppose for the moment that $d > 4$. Consider the three summations, including their contributions to ν'. The first is certainly at most $(q+1)/3q^3(q^6-1)$, which is less than $2/3q^8$. The second is at most $1/q^2(q^2-1) + (q+1)/3q^6(q^6-1)$, which is less than $1/q^2(q^2-1) + 1/q^{11}$. And the third is at most $1/q^2(q^4-1) + (q+1)/2q^4(q^8-1)$, which is less than $1/q^2(q^4-1) + 1/q^{11}$. Thus if $d > 4$ then

$$\nu(G) < \frac{1}{q(q^2-1)} + \frac{1}{q^2(q^2-1)} + \frac{1}{q^2(q^4-1)} + \frac{1}{q^8}.$$

If $d = 4$ the first summation disappears, the only term in the second is $1/q^2(q^2-1)$, and the third contributes at most $(q+1)/q^2(q^4-1)$, and so

$$\nu(G) < \frac{1}{q(q^2-1)} + \frac{1}{q^2(q^2-1)} + \frac{q+1}{q^2(q^4-1)}.$$

If $d = 3$ then the first and third summations disappear and, on the face of it, the second might contribute a term $(q+1)/q^2(q^2-1)$. It comes, however, from relevant sequences (a, r, f, V_0, X_0, X) in which $r = 1$, $f(t) = t - \lambda$, $\dim V_0 = 2$, and X_0 is scalar multiplication by λ. Here $c_X(t) = (t-\lambda)^3$ and $\lambda^3 = a$. Thus the number of choices for λ (when a is given) is at most 3, and it follows that the contribution to $\nu(G)$ is at most $3/|C|$, that is, at most $3/q^2(q^2-1)$ (and it is at most $1/q^2(q^2-1)$ if 3 does not divide $(q+1)/|D|$ because then the eigenvalue λ must lie in D). In summary, ignoring the last (parenthetic) point, we have found that

$$\nu(G) < \begin{cases} 1/q(q^2-1)+3/q^2(q^2-1) & \text{if } d=3, \\ 1/q(q^2-1)+1/q^2(q^2-1)+1/q^2(q-1)(q^2+1) & \text{if } d=4, \\ 1/q(q^2-1)+1/q^2(q^2-1)+1/q^2(q^4-1)+1/q^8 & \text{if } d\geqslant 5, \end{cases}$$

and Theorem 6.1 is a slightly simplified version of this.

7. NON-CYCLIC MATRICES IN SYMPLECTIC GROUPS

In this section we take d to be even, φ to be a symplectic form on V, and G to be a group such that $\mathrm{Sp}(V) \leqslant G \leqslant \mathrm{GSp}(V)$. The image of the scaling factor homomorphism $g \mapsto \mu(g)$ is a subgroup M of the multiplicative group $F^\times$, and $|M| = |G : \mathrm{Sp}(d, q)|$. Define

$$t(G) := \begin{cases} 1 & \text{if } |F^\times : M| \text{ is odd,} \\ 2 & \text{if } |F^\times : M| \text{ is even.} \end{cases}$$

Note in particular that if q is even then $t(G) = 1$ and the bound for $\nu(G)$ given in the theorem below is independent of G—as should be expected since then $\mathrm{GSp}(V) = \mathrm{Sp}(V) \times Z$ and $\nu(G) = \nu(\mathrm{Sp}(V))$.

THEOREM 7.1. *Suppose that $d \geqslant 4$, that d is even, and that* $\mathrm{Sp}(d, q) \leqslant G \leqslant \mathrm{GSp}(d, q)$. *Define $\nu(G)$ to be the probability that a random matrix in G is not cyclic. Then*

$$\nu(G) < \frac{1+t(G)}{q(q^2-1)} + \frac{1}{2q^2(q^2-1)} + \frac{t(G)}{q^2(q-1)(q^2-1)}.$$

In particular, $\nu(G) < (1+t(G))q^{-3} + O(q^{-4})$.

Remark 7.2. Since $\mathrm{Sp}(2, q) = \mathrm{SL}(2, q)$ and $\mathrm{GSp}(2, q) = \mathrm{GL}(2, q)$ we find that if $d = 2$ then $\nu(G) = t(G)/q(q^2-1)$, just as in the general linear case.

Cosets ρ of $\mathrm{Sp}(d, q)$ in $\mathrm{GSp}(d, q)$ correspond to values of the multiplier. Therefore in the symplectic case we modify the notation of Section 5 slightly and write our relevant sequences as (μ, r, f, V_0, X_0, X) where $\mu \in M$ and $\mu(X_0) = \mu(X) = \mu$. The leading term in our upper bound for $\nu(G)$ comes from three different types of relevant sequence: those with $r = 1$ and U non-degenerate, those with $r = 1$ and U totally singular, and those with $r = 2$ and U non-degenerate. We treat these first as separate cases.

Case $r = 1$ *and* $\mathrm{rank}(U) = 2$. In this case our sequences are of the form $(\mu, 1, t - \lambda, V_0, X_0, X)$ for some $\lambda \in F^\times$, and X_0 is multiplication by λ. Then $\lambda^2 = \mu$, so λ determines μ and the number of choices for λ, or for the first three entries of the sequence, is $t(G)|M|$. By Lemma 5.5, once those first three entries are chosen, the number of relevant sequences for this data is $|\mathrm{Sp}(d, q)|/|C|$ where $C \cong \mathrm{Sp}(2, q)$. Thus the total number of relevant sequences in which $r = 1$ and V_0 is non-degenerate of dimension 2 is $t(G)|M|\,|\mathrm{Sp}(d, q)|/|\mathrm{Sp}(2, q)|$, which is $t(G)|G|/q(q^2 - 1)$. These contribute $t(G)/q(q^2 - 1)$ to $\nu(G)$.

Case $r = 1$ *and* $\mathrm{rank}(U) = 0$. In this case the relevant sequences again take the form $(\mu, 1, t - \lambda, V_0, X_0, X)$, where now, however, V_0 is totally singular. The number of possibilities for μ is $|M|$, and since now there is no restriction on λ other than that it be non-zero, the number of choices for λ is $q - 1$. By Lemma 4.4.1, however, some of these choices may be discarded. For, if X is non-cyclic in virtue of the fact that $\dim V_\lambda \geqslant 2$ (where, recall, V_λ denotes the λ-eigenspace of X) then it will also have been counted among those matrices which are non-cyclic in virtue of the fact that $\dim V_{\mu/\lambda} \geqslant 2$. Thus from each pair $\{a, \mu/a\}$ with $a \in F^\times$ we need only choose one value of λ and the number of choices for λ comes down to $\frac{1}{2}(q + 1)$ if q is odd and μ is square in $F^\times$, to $\frac{1}{2}(q - 1)$ if q is odd and μ is non-square in $F^\times$, and to $\frac{1}{2}q$ if q is even. If q is odd and $t(G) = 1$ then half the members of M are squares and half are not, whereas if q is odd and $t(G) = 2$, or if q is even, then all the members of M are squares. It follows easily that the number of choices for the pair (μ, λ) is $\frac{1}{2}(q + t(G) - 1)|M|$. By Lemma 5.5, for given λ, μ, the number of relevant sequences in which V_0 is two-dimensional and totally singular is $|\mathrm{Sp}(d, q)|/|C|$ where now $C \cong \mathrm{GL}(2, q)$. Thus we get $\frac{1}{2}(q + t(G) - 1)\,|M|\,|\mathrm{Sp}(d, q)|/|\mathrm{GL}(2, q)$ relevant sequences and a contribution $\frac{1}{2}(q + t(G) - 1)/q(q - 1)(q^2 - 1)$ to $\nu(G)$.

Putting these two results together we have the following fact.

LEMMA 7.3. *Suppose that* $\mathrm{Sp}(d, q) \leqslant G \leqslant \mathrm{GSp}(d, q)$ *with* $d \geqslant 4$, *and define* $\nu_1(G)$ *to be the probability that a random element of* G *has an eigenspace of dimension* $\geqslant 2$. *Then*

$$\nu_1(G) \leqslant \frac{t(G) + (1/2)}{q(q^2 - 1)} + \frac{t(G)}{2q(q - 1)(q^2 - 1)}.$$

Case $r = 2$ *and* $\mathrm{rank}(U) = 4$. Here interest focuses on relevant sequences $(\mu, 2, f, V_0, X_0, X)$ where f is quadratic irreducible, and V_0 is a four-dimensional non-degenerate space. Since X_0 preserves a non-degenerate bilinear form on V_0 up to multiplication by μ, f must satisfy condition $\mathrm{C}(\mu)$. Given μ, by Lemma 4.4.3, the number of choices for f is $\frac{1}{2}(q + 1)$ if q is odd and μ is non-square, $\frac{1}{2}(q - 1)$ if q is odd and μ is square, and $\frac{1}{2}q$ if q is even. Much as in the previous case, the number of choices for the pair (μ, f) turns out to be $\frac{1}{2}(q+1-t(G))$. By Lemma 5.5, for each such choice the number of relevant sequences is $|\mathrm{Sp}(d,q)/|C|$, where by Lemma 5.4, $|C| = q(q^2-1)(q+1)$. Thus the total number of sequences is at most $|M| \times (q+1-t(G))/2 \times |\mathrm{Sp}(d,q)|/q(q^2-1)(q+1)$, and if the contribution to $\nu(G)$ is $\nu_2(G)$ then

$$\nu_2(G) \leqslant \frac{1}{2q(q^2-1)} - \frac{t(G)}{2q(q+1)(q^2-1)}.$$

Adding the two principal contributions to $\nu(G)$ we find that

$$\nu_1(G) + \nu_2(G) \leqslant \frac{1+t(G)}{q(q^2-1)} + \frac{t(G)}{q(q^2-1)^2}.$$

Other Cases in which $r \geqslant 2$. For relevant sequences (μ, r, f, V_0, X_0, X) in which $r \geqslant 2$, f is irreducible of degree r, and V_0 is a $2r$-dimensional non-degenerate space, the number of choices for μ is $|M|$; given r, an even integer $\geqslant 4$ for the moment (since the case where $r = 2$ and V_0 is non-degenerate has already been accounted for), the number of choices for f is then at most $(q^{r/2}+1)/r$; and when μ, r, and f are fixed the number of relevant sequences is $|\mathrm{Sp}(d,q)|/q^{r/2}(q^r-1)(q^{r/2}+1)$. Thus the contribution to $\nu(G)$ is at most $\sum_{r \geqslant 4} 1/rq^{r/2}(q^r-1)$, where the sum is over even r.

Next, for fixed $r \geqslant 2$, we estimate the number of relevant sequences in which $\mathrm{rank}(V_0) = r$. The number of choices for μ is $|M|$ and, given μ, since f must satisfy condition $\mathrm{C}(\mu)$, the number of possibilities for f is 0 if r is odd and it is $\leqslant (q^{r/2}+1)/r$ if r is even. If r, μ, and f are given then by Lemmas 5.5 and 5.4 the number of relevant sequences is at most $|\mathrm{Sp}(d,q)|/q^r(q^r-1)(q^{r/2}+1)$. Thus for given r the number of relevant sequences is

$$\leqslant |M| \times \frac{q^{r/2}+1}{r} \times \frac{|\mathrm{Sp}(d,q)|}{q^r(q^r-1)(q^{r/2}+1)},$$

which is $|G|/rq^r(q^r-1)$, and the contribution to $\nu(G)$ is at most $\sum_{r \geqslant 2} 1/rq^r(q^r-1)$, where the sum is over even r.

Last we estimate the number of relevant sequences in which V_0 is totally singular. The number of choices for μ is $|M|$, and by Lemma 2.2 the number of choices for f is at most $(q^r-q)/r$. By Lemmas 5.5 and 5.4, for given μ, r, f the number of these relevant sequences is at most $|\mathrm{Sp}(d,q)|/q^r(q^r-1)(q^{2r}-1)$. Thus for given $r \geqslant 2$ the total number of relevant sequences in which V_0 is totally singular is

$$\leqslant |M| \times \frac{(q^r-q)}{r} \times \frac{|\mathrm{Sp}(d,q)|}{q^r(q^r-1)(q^{2r}-1)} = |G| \frac{(q^r-q)}{rq^r(q^r-1)(q^{2r}-1)}.$$

It is easy to check that $(q^r - q)/q^r(q^r - 1)(q^{2r} - 1) < 1/q^{3r}$, and so we get a contribution $< \sum_{r \geqslant 2} 1/rq^{3r}$ to $\nu(G)$.

Putting all these estimates together we find that

$$\nu(G) < \nu_1(G) + \nu_2(G) + \sum_{\substack{r \geqslant 4,\\ r\,\text{even}}} \frac{1}{rq^{r/2}(q^r - 1)} + \sum_{\substack{r \geqslant 2,\\ r\,\text{even}}} \frac{1}{rq^r(q^r - 1)} + \sum_{r \geqslant 2} \frac{1}{rq^{3r}}.$$

The three summations add to an error term which is $O(q^{-4})$. In fact, the only summand which is of this order of magnitude is the term with $r = 2$ in the second summation, namely $1/2q^2(q^2 - 1)$. It is not hard to see that

$$\sum_{\substack{r \geqslant 4,\\ r\,\text{even}}} \frac{1}{rq^{r/2}(q^r - 1)} + \sum_{\substack{r \geqslant 4,\\ r\,\text{even}}} \frac{1}{rq^r(q^r - 1)} + \sum_{r \geqslant 2} \frac{1}{rq^{3r}} < \frac{7}{24q^6} + \frac{1}{24q^6} + \frac{2}{3q^6}.$$

Then

$$\nu(G) < \frac{1 + t(G)}{q(q^2 - 1)} + \frac{t(G)}{q(q^2 - 1)^2} + \frac{1}{2q^2(q^2 - 1)} + \frac{1}{q^6},$$

and the theorem follows easily.

8. NON-CYCLIC MATRICES IN EVEN-DIMENSIONAL ORTHOGONAL GROUPS

In this section we take d to be even, Q to be a non-degenerate quadratic form on V with polar form φ and type ε, and G to be a group such that $\Omega(V) \leqslant G \leqslant \mathrm{GO}(V)$. Small dimensional orthogonal groups are treated in Section 10 below; here we assume that $d \geqslant 6$. If q is odd then $\mathrm{GO}(V)/(\Omega(V).Z)$ is a dihedral group of order 8 and $(\mathrm{SO}(V).Z)/(\Omega(V).Z)$ is its centre; $\mathrm{GO}(V)/(\mathrm{SO}(V).Z) \cong Z_2 \times Z_2$. Also $\mathrm{O}(V).Z = \{X \in \mathrm{GO}(V) \mid \mu(X) \text{ is square in } F^{\times}\}$. If q is even then $\mathrm{GO}(V) = \mathrm{O}(V) \times Z$. As usual, define

$$\nu(G) := |G \cap \mathrm{Noncyc}(d, q)| \div |G|,$$

the probability that a random matrix in G is not cyclic. Recall that $\nu(G) = \nu(GZ)$ where Z is the group of non-zero scalar matrices. For $d \geqslant 6$ (indeed, for $d \geqslant 4$) the probability $\nu(G)$ depends primarily on q and the parameter $s(G)$ defined as follows:

$$s(G) := \begin{cases} |\mathrm{GO}(V) : G.\mathrm{SO}(V).Z| & \text{if } q \text{ is odd,} \\ |\mathrm{GO}(V) : G.Z| & \text{if } q \text{ is even.} \end{cases}$$

When q is odd $s(G)$ is 1, 2, or 4; when q is even $s(G)$ is 1 or 2.

THEOREM 8.1. *Suppose that* d *is even,* $d \geqslant 6$, *and* $\Omega^{\varepsilon}(d,q) \leqslant G \leqslant \mathrm{GO}^{\varepsilon}(d,q)$. *Then*

$$\nu(G) < \begin{cases} \dfrac{s(G)}{2q} + \dfrac{q+4}{2q(q^2-1)} & \text{if } q \text{ is odd,} \\ \dfrac{s(G)}{2q} + \dfrac{2}{q(q^2-1)} & \text{if } q \text{ is even,} \end{cases}$$

and so $\nu(G) < \frac{1}{2}s(G)q^{-1} + O(q^{-2})$.

We begin by establishing some further notation and conventions. Let M be the image of the scaling factor homomorphism $g \mapsto \mu(g)$ and, as in the symplectic case, define

$$t(G) := \begin{cases} 2 & \text{if } |F^{\times} : M| \text{ is even,} \\ 1 & \text{if } F^{\times} : M| \text{ is odd.} \end{cases}$$

It is not hard to see that $t(G) = |\mathrm{GO}(V) : G.\mathrm{O}(V).Z|$. Define also

$$t'(G) := \begin{cases} |G.\mathrm{O}(V).Z : G.\mathrm{SO}(V).Z| & \text{if } q \text{ is odd,} \\ |\mathrm{GO}(V) : G.Z| & \text{if } q \text{ is even.} \end{cases}$$

Clearly, $s(G) = s(G.Z)$, $t(G) = t(G.Z)$, $t'(G) = t'(G.Z)$, and $s(G) = t(G)t'(G)$.

The natural homomorphism $\mathrm{GO}(V) \to \mathrm{GO}(V)/\Omega(V)$ will be denoted $X \mapsto \overline{X}$. Define $R := \overline{G}$, the image of G under this map. The scaling factor homomorphism $\mathrm{GO}(V) \to F^{\times}$ induces a homomorphism $\mathrm{GO}(V)/\Omega(V) \to F^{\times}$, which we write $\rho \mapsto \mu(\rho)$. Its kernel is $\mathrm{O}(V)/\Omega(V)$ and so this homomorphism is four-to-one if q is odd and it is two-to-one if q is even.

For $\lambda \in F^{\times}$ and a $d \times d$ matrix X let $V_{\lambda}(X)$ be the λ-eigenspace $\{v \in V \mid vX = \lambda v\}$. If $\mu(X) \neq \lambda^2$ and $\dim V_{\lambda}(X) \geqslant 2$ then $V_{\lambda}(X)$ must be totally singular—matrices of this kind will be treated later. The leading term in $\nu(G)$ comes from those matrices X for which there exists λ such that $\dim V_{\lambda}(X) \geqslant 2$ and $\lambda^2 = \mu(X)$, and we focus on these first. Define

$$\begin{aligned} N_{\lambda}(G) &:= \{X \in G \mid \dim V_{\lambda}(X) \geqslant 2 \text{ and } \lambda^2 = \mu(X)\}, \\ N(G) &:= \bigcup \{N_{\lambda}(G) \mid \lambda \in F^{\times}\}, \\ \nu_1(G) &:= |N(G)| \div |G|. \end{aligned}$$

We first bound $\nu_1(G)$.

LEMMA 8.2.

$$\nu_1(G) < \frac{s(G)}{2q} + \frac{t(G)}{q(q^2-1)}.$$

Proof. Suppose first that q is odd. Define $G_2 := \{X \in G \mid \mu(X)$ is square in $F^{\times}\}$. From the definition of $t(G)$ it follows that $|G : G_2| = 2/t(G)$. Also of course $N(G) \subseteq G_2$ and therefore $\nu_1(G) = \nu_1(G_2)/|G : G_2|$; that is, $\nu_1(G) = \nu_1(G_2).t(G)/2$. Since $s(G) = t(G)t'(G)$ what we need to prove is that $\nu_1(G_2) < t'(G)/q + 2/q(q^2 - 1)$.

Now define $H_1 := (G.Z) \cap \mathrm{O}(V)$ and $H_0 := (G.Z) \cap \mathrm{SO}(V)$. If $H_0 = H_1$ then $H_1 \leqslant \mathrm{SO}(V)$ and one sees easily that $t'(G) = 2$, whereas if $|H_1 : H_0| = 2$ then $H_1.\mathrm{SO}(V) = \mathrm{O}(V)$ and $t'(G) = 1$. Thus $|H_1 : H_0| = 2/t'(G)$. Now $H_1.Z = G_2.Z$ and it follows that $\nu_1(H_1) = \nu_1(G_2)$. Therefore we may work with H_1 and need to prove that $\nu_1(H_1) < t'(G)/q + 2/q(q^2 - 1)$.

Define $n_\lambda(H_1) := |N_\lambda(H_1)|/|H_1|$. If $X \in H_1$ then $\mu(X) = 1$ and, since the eigenvalues λ we are concerned with satisfy $\lambda^2 = \mu(X)$, they are ± 1. Consider first the contributions to $n_{\pm 1}(H_1)$ coming from H_0. We have $\{\pm I\} \leqslant H_0$ and so if $X \in H_0$ then also $-X \in H_0$; also, $V_{-1}(X) = V_1(-X)$ and it follows immediately that $n_{-1}(H_0) = n_1(H_0)$. Now $\Omega(V) \leqslant H_0$ and, since $d > 2$, $\Omega(V)$ is transitive on non-zero vectors v with a given value of $Q(v)$. It follows that H_0 is transitive on such vectors and so it has q orbits in $V \backslash \{0\}$. By Not Burnside's Lemma, $\sum_{X \in H_0} |\mathrm{Fix}(X)| = q|H_0|$, so $n_1(H_0)(q^2 - 1) < q|H_0|$ and

$$n_1(H_0) + n_{-1}(H_0) = 2\,n_1(H_0) < 2\,|H_0|\,\frac{q}{q^2 - 1}\,.$$

If $H_0 = H_1$ then $t'(G) = 2$ and

$$\nu_1(H_1) = \frac{n_1(H_1) + n_{-1}(H_1)}{|H_1|} < \frac{2q}{q^2 - 1} = \frac{2}{q} + \frac{2}{q(q^2 - 1)}\,,$$

so that $\nu_1(H_1) < t'(G)/q + 2/q(q^2 - 1)$ as required. Thus we may assume that H_0 is a proper subgroup of H_1, in which case $|H_1 : H_0| = 2$. Applying Not Burnside's Lemma in the same way as above to H_0 and to H_1, and subtracting, we get that $\sum_{X \in H_1 \backslash H_0} |\mathrm{Fix}(X)| = q|H_0|$, and so

$$\sum_{X \in H_1 \backslash H_0} (|\mathrm{Fix}(X)| - (q - 1)) = |H_0|.$$

The point is that if $X \in H_1 \backslash H_0$ then $\dim \mathrm{Ker}(I - X)$ is odd (see, for example, [10, Theorem 11.43]). Therefore every term in the sum is non-negative, and if $X \in N_1(H_1) \cap (H_1 \backslash H_0)$ then $\dim \mathrm{Ker}(I - X) \geqslant 3$ and $|\mathrm{Fix}(X)| - (q - 1) \geqslant q^3 - q$. Consequently,

$$|N_1(H_1) \cap (H_1 \backslash H_0)| \leqslant |H_0|/q(q^2 - 1),$$
$$n_1(H_1) \leqslant |H_0|(q/(q^2 - 1) + 1/q(q^2 - 1)),$$

and

$$n_1(H_1) + n_{-1}(H_1) = 2\,n_1(H_1) < 2\,|H_0|\left(\frac{q}{q^2 - 1} + \frac{1}{q(q^2 - 1)}\right).$$

Since we are assuming that $|H_1| = 2|H_0|$, we get that

$$\nu_1(H_1) = \frac{n_1(H_1) + n_{-1}(H_1)}{|H_1|} < \frac{q}{q^2-1} + \frac{1}{q(q^2-1)} = \frac{1}{q} + \frac{2}{q(q^2-1)},$$

and, since $t'(G) = 1$, this is what we wanted to prove.

Now suppose that q is even. Define $H_1 := G \cap \mathrm{O}(V)$, $H_0 := G \cap \Omega(V)$. The above argument still works, but has to be modified in minor ways. First, $\nu_1(G) = \nu_1(H_1)$. Second, for H_1 there is only one relevant eigenvalue, namely 1, and therefore $\nu_1(H_1) = n_1(H_1)/|H_1|$. These two adjustments, which involve multiplying and dividing by 2, respectively, cancel each other out and the result is the same.

To deal with other non-cyclic matrices we count relevant sequences $(\rho, r, f, V_0, X_0, X)$ of type (U, T) as defined in Section 5. There are five cases to be considered.

Case $r = 1$, $f(t) = t - \lambda$, and $\lambda^2 \neq \mu(\rho)$. Define $\mu := \mu(\rho)$. By Lemma 4.4.1, $\dim V_\lambda(X) = \dim V_{\mu/\lambda}(X)$. Therefore it is sufficient to treat just one of λ, μ/λ and, for fixed ρ, the number of choices for λ is $\frac{1}{2}(q-3)$ when q is odd and $\frac{1}{2}(q-2)$ when q is even. The space U must be totally singular since $\lambda^2 \neq \mu$ and so by Lemmas 5.5 and 5.4, for fixed ρ and λ, the number of relevant sequences is $|\Omega(V)|/q(q-1)(q^2-1)$. Then, since the number of choices for ρ is $|R|$ and $|R| \times |\Omega(V)| = |G|$, we find that $\nu(G)$ acquires

$$\text{contribution} \leqslant \begin{cases} \dfrac{q-3}{2q(q-1)(q^2-1)} & \text{if } q \text{ is odd,} \\ \dfrac{q-2}{2q(q-1)(q^2-1)} & \text{if } q \text{ is even} \end{cases} \tag{1}$$

from this case.

Case $r \geqslant 2$ and U is totally singular. In a relevant sequence $(\rho, r, f, V_0, X_0, X)$ with $\mathrm{rank}(V_0) = 0$ the number of choices for ρ is $|R|$, the number of choices for f is at most $(q^r - q)/r$, and then, by Lemmas 5.5 and 5.4, the number of possibilities for (V_0, X_0, X) is $c\,|\Omega(V)| \div (q^{2r}-1)(q^{2r}-q^r)$, where $c = 1$ if $4r \leqslant d-2$ and c divides $|O(V) : \Omega(V)|$ if $4r = d$. Thus we get a contribution to $\nu(G)$ which is

$$\leqslant \sum_{2 \leqslant r \leqslant (d-2)/4} \frac{q^r - q}{r} \, \frac{1}{(q^{2r}-1)(q^{2r}-q^r)} + E,$$

where E accounts for cases where $d = 4r$. Thus $E = 0$ if $d \equiv 2 \pmod 4$ and if $d = 4m$ then

$$E \leqslant c' \, \frac{q^m - q}{m} \, \frac{1}{(q^{2m}-1)(q^{2m}-q^m)},$$

where $c' = 4$ if q is odd and $c' = 2$ if q is even. It is easy to check that

$$\sum_{2 \leqslant r \leqslant (d-2)/4} \frac{q^r - q}{r(q^{2r}-1)(q^{2r}-q^r)} + E \leqslant \frac{c'}{2q(q+1)(q^4-1)},$$

and so $\nu(G)$ acquires

$$\text{contribution} < \begin{cases} \dfrac{2}{q(q+1)(q^4-1)} & \text{if } q \text{ is odd,} \\ \dfrac{1}{q(q+1)(q^4-1)} & \text{if } q \text{ is even} \end{cases} \tag{2}$$

from this case.

Case $r = 2$, $f(t) = t^2 - \mu$, *and* $\mathrm{rank}(U) = r_0 > 0$. Let $N(\rho, r_0, \varepsilon')$ be the number of relevant sequences $(\rho, 2, t^2 - \mu, V_0, X_0, X)$ of type (U, T) in which $\mathrm{rank}(U) = r_0$ and $\mathrm{type}(U) = \varepsilon'$, and of course $\mu = \mu(\rho)$. If $\mu(\rho)$ is square in $F^\times$ then $N(\rho, r_0, \varepsilon')$ is the empty set. Otherwise, by Lemmas 5.5 and 5.4 we have that

$$\sum_{\substack{r_0 \in \{4,2\},\\ \varepsilon' \in \{+,-\}}} \frac{|N(\rho, r_0, \varepsilon')|}{|\Omega(V)|} \leqslant \frac{c_{4,+}}{2(q^2-1)} + \frac{c_{4,-}}{2(q^2+1)} + \frac{c_{2,+}}{2q^2(q^2-1)} + \frac{c_{2,-}}{2q^2(q^2-1)},$$

where the coefficients $c_{r_0,\varepsilon}$ are those appearing in Lemma 5.5. If $d \geqslant 8$ then $c_{r_0,\varepsilon'} = 1$ in all four cases. If $d = 6$ then $c_{4,+} = c_{4,-} = 1$, but $c_{2,+}$ and $c_{2,-}$ might be 4. One of $c_{2,+}$ and $c_{2,-}$ must, however, be 0. For, let $U_1 := U \cap U^\perp$ and let U_2 be a T-invariant complement for U_1 in U. Then U_2 is non-degenerate and $V = U_2 \oplus U_2^\perp$. Now $U_2^\perp$, which is of dimension 4, is non-degenerate and contains the two-dimensional totally singular subspace U_1. Therefore $\mathrm{type}(U_2^\perp) = +$ and so $\mathrm{type}(U) = \mathrm{type}(U_2) = \varepsilon$, where, as usual, $\varepsilon = \mathrm{type}(V)$. Thus

$$\sum_{\substack{r_0 \in \{4,2\},\\ \varepsilon' \in \{+,-\}}} \frac{|N(\rho, r_0, \varepsilon')|}{|\Omega(V)|} \leqslant \frac{q^2}{q^4-1} + \frac{2}{q^2(q^2-1)} = \frac{q^2+1}{q^2(q^2-1)} + \frac{1}{q^2(q^4-1)}.$$

Adding over all $\rho \in R$ we find that the contribution to $\nu(G)$ is 0 if $\mu(\rho)$ is a square in $F^\times$ for all $\rho \in R$ and it is $\frac{1}{2}|R| \times |R|^{-1}\big((q^2+1)/q^2(q^2-1) + 1/q^2(q^4-1)\big)$ otherwise. Therefore $\nu(G)$ acquires

$$\text{contribution} \leqslant \begin{cases} \dfrac{2 - t(G)}{2}\left(\dfrac{q^2+1}{q^2(q^2-1)} + \dfrac{1}{q^2(q^4-1)}\right) & \text{if } q \text{ is odd} \\ 0 & \text{if } q \text{ is even} \end{cases} \tag{3}$$

from this situation.

Case $r \geqslant 2$, $f(t) \neq t^2 - \mu$, *and* $\operatorname{rank}(U) = 2r$. Since the polynomial components f of our relevant sequences $(\rho, r, f, V_0, X_0, X)$ must satisfy condition $C(\mu)$, where $\mu = \mu(\rho)$, they have even degree and we may suppose that $r = 2s$. By what should now be a familiar argument, the contribution to $\nu(G)$ is at most $\sum_s (q^s + 1)/2s \times 1/q^s(q^{2s} - 1)(q^s + 1) + E$, where E accounts for terms in which $2r > d - 2$. Let $m := \lfloor d/4 \rfloor$ and let c be as in Lemma 5.5. By that lemma

$$\begin{aligned} 0 \leqslant E &\leqslant \frac{c\,(q^m + 1)}{2m} \, \frac{1}{q^m(q^{2m} - 1)(q^m + 1)} \\ &= \frac{c}{2m\, q^m\, (q^{2m} - 1)} \leqslant \begin{cases} 2/mq^m(q^{2m} - 1) & \text{if } q \text{ is odd,} \\ 1/mq^m(q^{2m} - 1) & \text{if } q \text{ is even.} \end{cases} \end{aligned}$$

It follows easily that the sum of E and the terms with $s \geqslant 2$ is at most $1/q^2(q^4 - 1)$ if q is odd and at most $1/2q^2(q^4 - 1)$ if q is even. Then, since $d \geqslant 6$, we find that $\nu(G)$ acquires

$$\text{contribution} \leqslant \begin{cases} \dfrac{1}{2q(q^2 - 1)} + \dfrac{1}{q^2(q^4 - 1)} & \text{if } q \text{ is odd,} \\ \dfrac{1}{2q(q^2 - 1)} + \dfrac{1}{2q^2(q^4 - 1)} & \text{if } q \text{ is even.} \end{cases} \tag{4}$$

from this case.

Case $r \geqslant 2$, $f(t) \neq t^2 - \mu$, *and* $\operatorname{rank}(U) = r$. The polynomial components f of our sequences $(\rho, r, f, V_0, X_0, X)$ again satisfy condition $C(\mu)$, where $\mu = \mu(\rho)$, and therefore have even degree, so we may take it that $r = 2s$. Moreover, $d \geqslant 3r$. The contribution to $\nu(G)$ is at most $\sum_s (q^s + 1)/2s \times 1/q^{2s}(q^{2s} - 1)(q^s + 1) + E'$, where E' accounts for terms in which $3r > d - 2$. If $m := \lfloor d/6 \rfloor$ then $0 \leqslant E' \leqslant 2/mq^m(q^{2m} - 1)$ by Lemma 5.5, and it follows easily that if $d \geqslant 8$ then $\nu(G)$ acquires

$$\text{contribution} < \frac{1}{2q^2(q^2 - 1)} + \frac{1}{q^4(q^4 - 1)} \tag{5}$$

from this case. As it happens this also holds for $d = 6$: it is not hard to prove that if $d = 6$ and q is odd then this case does not arise so that the relevant contribution is 0, and that if $d = 6$ and q is even then Lemma 5.5 holds with $c = 1$ so that the relevant contribution is at most $1/2q^2(q^2 - 1)$.

Now we put all this together to estimate $\nu(G)$. Suppose first that q is odd. The terms of order q^{-1}, q^{-2}, q^{-3} that involve $s(G)$ and $t(G)$ come from Lemma 8.2 and inequality (3). They are

$$\frac{s(G)}{2q} + \frac{t(G)}{q(q^2 - 1)} - \frac{t(G)\,(q^2 + 1)}{2q^2(q^2 - 1)},$$

which is

$$\frac{s(G)}{2q} - \frac{t(G)\,(q-1)}{2q^2(q+1)}.$$

Let E_2 be the sum of the terms of order q^{-2}, q^{-3}, q^{-4} that do not involve $s(G)$ or $t(G)$. There are contributions to E_2 from inequalities (3), (1), (4), and (5):

$$\begin{aligned} E_2 &\leqslant \frac{q^2+1}{q^2(q^2-1)} + \frac{q-3}{2q(q-1)(q^2-1)} + \frac{1}{2q(q^2-1)} + \frac{1}{2q^2(q^2-1)} \\ &= \frac{1}{q(q-1)} + \frac{q-3}{2q^2(q-1)(q^2-1)}. \end{aligned}$$

Collecting terms of order q^{-6} and q^{-8} from inequalities (1), (3), (4), and (5) (and remembering in relation to (3) that $(2-t(G))/2 \leqslant \frac{1}{2}$) we find a contribution E_6, where

$$\begin{aligned} E_6 &< \frac{2}{q(q+1)(q^4-1)} + \frac{1}{2q^2(q^4-1)} + \frac{1}{q^2(q^4-1)} + \frac{1}{q^4(q^4-1)} \\ &< \frac{7}{2q^2(q^4-1)}. \end{aligned}$$

Therefore if q is odd then

$$\begin{aligned} \nu(G) &< \frac{s(G)}{2q} - \frac{t(G)\,(q-1)}{2q^2(q+1)} + \frac{1}{q(q-1)} \\ &\quad + \frac{q-3}{2q^2(q-1)(q^2-1)} + \frac{7}{2q^2(q^4-1)} \\ &\leqslant \frac{s(G)}{2q} + \frac{q+4}{2q(q^2-1)} - \frac{1}{2q^2(q^2-1)} \\ &\quad + \frac{q-3}{2q^2(q-1)(q^2-1)} + \frac{7}{2q^2(q^4-1)}, \end{aligned}$$

and since, as is easy to check, $(q-3)/2q^2(q-1)(q^2-1) + 7/2q^2(q^4-1) < 1/2q^2(q^2-1)$ for all q, this case of Theorem 8.1 follows.

Suppose now that q is even. In this case $t(G) = 1$ and there are no contributions to $\nu(G)$ from inequality (3). Therefore the terms of order q^{-1} to q^{-4} come from Lemma 8.2 and from inequalities (1), (4), and (5). If their contribution is $s(G)/2q + E_2$ then

$$\begin{aligned} E_2 &< \frac{1}{q(q^2-1)} + \frac{q-2}{2q(q-1)(q^2-1)} + \frac{1}{2q(q^2-1)} + \frac{1}{2q^2(q^2-1)} \\ &= \frac{2}{q(q^2-1)} - \frac{1}{2q^2(q-1)(q^2-1)}. \end{aligned}$$

There are contributions of order q^{-6} and q^{-8} coming from inequalities (2), (4), and (5). If E_6 is their sum then

$$E_6 < \frac{1}{q(q+1)(q^4-1)} + \frac{1}{2q^2(q^4-1)} + \frac{1}{q^4(q^4-1)} < \frac{3}{2q^2(q^4-1)}.$$

Therefore

$$\nu(G) < \frac{s(G)}{2q} + \frac{2}{q(q^2-1)} - \frac{1}{2q^2(q-1)(q^2-1)} + \frac{3}{2q^2(q^4-1)}.$$

Now $1/2q^2(q-1)(q^2-1) > 3/2q^2(q^4-1)$ for all q and so the inequality of Theorem 8.1 holds when q is even.

9. ORTHOGONAL GROUPS OF ODD DIMENSION

In this section notation is the same as in Section 8. We take d to be odd and then, since Q is a non-degenerate quadratic form on V, also q must be odd. Recall from Lemma 4.2.1 that if $X \in \mathrm{GO}(V)$ then $\mu(X)$ is a square in $F^\times$, and it follows that $\mathrm{GO}(d,q) = \mathrm{SO}(d,q) \times Z$. Furthermore, 1 occurs as an eigenvalue of every matrix X in $\mathrm{SO}(d,q)$ with odd algebraic multiplicity, in the sense that $c_X(t) = (t-1)^m f(t)$ where m is odd and $f(1) \neq 0$, and also with odd geometric multiplicity, in the sense that $\dim \mathrm{Ker}(I-X)$ is odd.

THEOREM 9.1. *If d and q are odd, $d \geqslant 5$, $\Omega(d,q) \leqslant G \leqslant \mathrm{GO}(d,q)$, and, as usual, $\nu(G)$ is the proportion of non-cyclic matrices in G, then*

$$\nu(G) < \frac{1}{q-1} + \frac{3}{(q-1)(q^2+1)} = q^{-1} + O(q^{-2}).$$

Although the proof is based on the ideas of Section 8 there are some significant differences. First, there is a simplification—since $\mathrm{GO}(V) = \mathrm{SO}(V) \times Z$, there is no loss of generality in assuming that $\Omega(V) \leqslant G \leqslant \mathrm{SO}(V)$, that is, that $G = \Omega(V)$ or $G = \mathrm{SO}(V)$. Second, however, Lemma 8.2 does not work quite so well. For even-dimensional groups that lemma not only allowed us to avoid detailed treatment of relevant sequences $(\rho, r, f, V_0, X_0, X)$ in which $r = 1$, $f(t) = t - \lambda$, and the two-dimensional space V_0 was not totally singular, it also gave a better bound than the general method. For $\lambda = \pm 1$ define

$$N_\lambda(G) := \{X \in G \mid \dim V_\lambda(X) \geqslant 2\}, \qquad \nu_\lambda(G) := |N_\lambda(G)|/|G|.$$

We find that we have to use the general method to deal with eigenvalue -1, and it is this that gives the leading term in the upper bound of the theorem. By way of contrast, the contribution from the eigenvalue 1, which was significant in the even-dimensional case, is very small here:

LEMMA 9.2. $\nu_1(G) < 1/q(q^2 - 1)$.

Proof. As in Lemma 8.2 we consider the permutation action of G on $V \backslash \{0\}$ and use Not Burnside's Lemma. Since G is transitive on the set of vectors v with given value $Q(v)$, it has q orbits. Therefore $\sum_{X \in G} |\mathrm{Fix}(X)| = q|G|$. The equation may be re-written in the form $\sum_{X \in G} (|\mathrm{Fix}(X)| - q + 1) = |G|$. The point of the rewriting is that, since every element of G has 1 as an eigenvalue, every term in the sum is non-negative. The positive terms come from elements of $N_1(G)$ and, since $\dim V_1(X)$ is odd, each of these contributes at least $q^3 - q$ to the sum. Thus $q(q^2 - 1)|N_1(G)| < |G|$ (strict inequality because some X have fixed-point spaces of dimension greater than 3) and the result follows immediately.

From here on we count relevant sequences. Estimates are exactly as in Section 8 except that the case $r = 1$, $f(t) = t + 1$ has to be treated separately.

LEMMA 9.3. $\nu_{-1}(G) < q^2/(q-1)(q^2 - 1)$.

Proof. Consider relevant sequences $(\rho, 1, t+1, V_0, X_0, X)$. If (U, T) is their type then U is two-dimensional and $T = -I_2$. They lead to a contribution $1/|C|$ to $\nu_{-1}(G)$ where, as in Section 5, C is the centraliser of T in $\mathrm{Aut}(U)$; that is, $C = \mathrm{Aut}(U)$. If U is non-singular and $\varepsilon := \mathrm{type}(U)$ then $|C| = 2(q - \varepsilon)$, and so such sequences contribute $1/2(q-1) + 1/2(q+1)$ that is, $q/(q^2 - 1)$. If U is of rank 1 then $|C| = 2q(q-1)$ and such sequences contribute $1/q(q-1)$ since there are two possible types. If U is totally singular then $C = \mathrm{GL}(U)$, so the contribution is $1/q(q-1)(q^2-1)$. Adding, we find that

$$\nu_{-1} < \frac{q}{q^2 - 1} + \frac{1}{q(q-1)} + \frac{1}{q(q-1)(q^2-1)} = \frac{q^2}{(q-1)(q^2-1)},$$

as the lemma states.

Proof of Theorem 9.1. Relevant sequences $(\rho, 1, t+1, V_0, X_0, X)$, in which $r = 1$ and $f(t) = t - \lambda$ where $\lambda \neq \pm 1$, and sequences in which $r \geqslant 2$ are treated in exactly the same way as in Section 8. Thus, the contribution from those in which $r = 1$ and V_0 is totally singular is smaller than $(q-3)/2q(q-1)(q^2-1)$. The contribution from those in which $r \geqslant 2$ and V_0 is totally singular is smaller than $\sum_{r \geqslant 2} (q^r - q)/r \times 1/(q^{2r} - 1)(q^{2r} - q^r) + E$, where E accounts for cases where $4r = d - 1$. Now $E = 0$ if $d \equiv 2 \pmod 4$ and if $d = 4m + 1$ then $E \leqslant 2(q^m - q)/m \times 1/(q^{2m} - 1)(q^{2m} - q^m)$, since $|\mathrm{O}(V) : \Omega(V)| = 2$. Therefore this contribution turns out to be less than $1/q(q+1)(q^4 - 1)$.

Since $G \leqslant \mathrm{SO}(V)$, μ is 1, which is square, and so there is no contribution from relevant sequences in which $f(t) = t^2 - \mu$. The contribution from those in which $r \geqslant 2$ and V_0 is non-degenerate is less than $1/2q(q^2-1) + 1/q^2(q^4-1)$ and that from sequences in which $r \geqslant 2$ and $\mathrm{rank}(V_0) = r$ is less than $1/2q^2(q^2-1) + 1/q^4(q^4-1)$. Treating terms of order q^{-6} or less in the same way as in Section 8 we find that

$$\nu(G) < \frac{q^2}{(q-1)(q^2-1)} + \frac{3}{2q(q^2-1)} + \frac{q-3}{2q(q-1)(q^2-1)} + \frac{1}{2q^2(q^2-1)} + \frac{2}{q^2(q^4-1)},$$

and routine algebra yields Theorem 9.1.

10. ORTHOGONAL GROUPS OF SMALL DIMENSION

This section is devoted to orthogonal groups of dimension $\leqslant 4$. They are treated exactly for two reasons: first, in order to add some insight into why the estimates of Sections 8, 9 work and; second, in order to confirm that those estimates are not unrealistic. Notation is the same as in the previous two sections. For $d = 2$ the situation is different from the general case and is this:

THEOREM 10.1. *Let G be a group such that $\Omega^{\varepsilon}(2,q) \leqslant G \leqslant \mathrm{GO}^{\varepsilon}(2,q)$ and let $s'(G) := |\mathrm{GO}^{\varepsilon}(2,q) : GZ|$. Then $\nu(G) = s'(G)/2(q-\varepsilon)$.*

Proof. The only non-cyclic matrices that can occur are scalar matrices and so we find that

$$\nu(G) = \frac{|G \cap Z|}{|G|} = \frac{|Z|}{|GZ|} = \frac{|Z|}{|\mathrm{GO}^{\varepsilon}(2,q)|}|\mathrm{GO}^{\varepsilon}(2,q) : GZ| = \frac{s'(G)}{2(q-\varepsilon)}$$

in all cases.

Note (1). If q is even then $s'(G) = s(G)$ as defined in Section 8. But if q is odd then the possibilities for $s'(G)$ depend to some extent upon the congruence class of q modulo 4. The orthogonal groups $\mathrm{O}^+(2,q)$, $\mathrm{O}^-(2,q)$ are dihedral groups $D_{2(q-1)}$ and $D_{2(q+1)}$, respectively, the general orthogonal group $\mathrm{GO}^+(2,q)$ is the monomial group $Z_{q-1} \,\mathrm{wr}\, Z_2$ (wreath product of $F^{\times}$ by Z_2), and $\mathrm{GO}^-(2,q)$ is the normaliser of a Singer cycle in $\mathrm{GL}(2,q)$, so that $\mathrm{GO}^-(2,q) \cong \langle t, u \mid t^{q^2-1} = u^2 = 1,\ t^u = t^q \rangle$. The groups $\Omega^+(2,q)$, $\Omega^-(2,q)$ are cyclic groups $Z_{(q-1)/2}$, $Z_{(q+1)/2}$, respectively, if q is odd, and they are cyclic groups Z_{q-1}, Z_{q+1} if q is even. Since $\Omega(V)Z \leqslant GZ \leqslant \mathrm{GO}(V)$ the parameter $s'(G)$ is a divisor of $|\mathrm{GO}(V) : \Omega(V)Z|$. Now

$$\mathrm{GO}(V)/\Omega(V)Z \cong \begin{cases} Z_2 & \text{if } q \text{ is even,} \\ Z_2 \times Z_2 & \text{if } q \equiv \varepsilon \pmod 4, \\ D_8 & \text{if } q \equiv -\varepsilon \pmod 4, \end{cases}$$

where ε is the type of V, and so $s'(G)$ is 1, 2, 4, or 8. Asymptotically we have $\nu(G) \leqslant 4/(q-1)$ for all G.

Note (2). For small values of q it can happen that all elements of G are non-cyclic (*i.e.,* scalar). In fact $\Omega^+(2,2)$, $\Omega^{\pm}(2,3)$, and $\Omega^+(2,5)$ consist of scalar matrices.

Next we treat the three-dimensional case. Since the dimension is odd and V is non-degenerate, q must be odd.

THEOREM 10.2. *If q is odd and $\Omega(3,q) \leqslant G \leqslant \mathrm{GO}(3,q)$ then*

$$\nu(G) = \begin{cases} \dfrac{q^2+1}{q(q^2-1)} & \textit{if } \mathrm{SO}(3,q) \leqslant G, \\ \dfrac{q^2+\eta q+2}{q(q^2-1)} & \textit{otherwise,} \end{cases}$$

where $\eta := (-1)^{(q-1)/2}$.

Proof. We may assume (compare Section 9) that $G \leqslant \mathrm{SO}(3,q)$, that is, that $G = \mathrm{SO}(3,q)$ or $G = \Omega(3,q)$. A non-cyclic matrix X in $\mathrm{SO}(3,q)$ has an eigenvalue λ whose eigenspace V_λ is of dimension $\geqslant 2$. Since X is orthogonal, $\lambda = \pm 1$, and since $\det X = 1$, either $c_X(t) = (t-1)^3$ or $c_X(t) = (t-1)(t+1)^2$. By a theorem of R. H. Dye (see [10, p. 160]), $\dim \mathrm{Ker}(X-I)$ is odd. Therefore the only non-cyclic matrix in $\mathrm{SO}(3,q)$ with characteristic polynomial $(t-1)^3$, that is, the only non-cyclic unipotent matrix in $\mathrm{SO}(3,q)$, is the identity matrix I. Consider now non-cyclic matrices X with characteristic polynomial $(t-1)(t+1)^2$. A non-degenerate one-dimensional subspace of V can be assigned to each such matrix, namely, its 1-eigenspace. Conversely, for each non-degenerate one-dimensional subspace V_1 of V there is a unique isometry X that fixes V_1 pointwise and acts on $V_1^\perp$ as multiplication by -1. Thus the number of non-cyclic matrices with characteristic polynomial $(t-1)(t+1)^2$ in $\mathrm{SO}(3,q)$ is the same as the number of one-dimensional non-degenerate subspaces, which is q^2. Therefore $\nu(\mathrm{SO}(3,q)) = (q^2+1)/|\mathrm{SO}(3,q)| = (q^2+1)/q(q^2-1)$.

Taking $Q(x_1,x_2,x_3)$ to be the standard form $x_1^2+x_2^2+x_3^2$ and using Taylor's description [10, p. 163] of the spinor norm, we find that a non-cyclic matrix $X \in \mathrm{SO}(3,q)$ with characteristic polynomial $(t-1)(t+1)^2$ and two-dimensional (-1)-eigenspace W lies in $\Omega(3,q)$ if and only if the discriminant of $Q\restriction W$ is a square in $F^\times$. Now $\operatorname{disc}(Q\restriction W) \times \operatorname{disc}(Q\restriction W^\perp) = \operatorname{disc}(Q) = 1$ modulo squares, and so $X \in \Omega(3, q)$ if and only if $Q(v_1)$ is a square in $F^\times$, where $\langle v_1 \rangle = W^\perp$; that is, v_1 is a 1-eigenvector for X. The number of one-dimensional spaces $\langle v \rangle$ for which $Q(v)$ is square is $\frac{1}{2}q(q+\eta)$. Since $|\Omega(3, q)| = \frac{1}{2}q(q^2-1)$, the formula for $\nu(\Omega(3, q))$ given in the statement of the theorem follows easily.

For the remainder of this section we take d to be 4. Let X be a non-cyclic matrix in $\mathrm{GO}(V)$ with multiplier μ. Then one of the following holds:

(I) for some λ such that $\lambda^2 = \mu$ the eigenspace $V_\lambda(X)$ is of dimension $\geqslant 2$;

(II) there is a decomposition $V = U_1 \oplus U_2$, in which U_1, U_2 are totally singular subspaces of dimension 2, and with respect to which $X = \lambda I_2 \oplus (\mu/\lambda) I_2$ for some $\lambda \in F^\times$ such that $\lambda^2 \neq \mu$;

(III) μ is not square in $F^\times$ and $X^2 = \mu I_4$;

(IV) there is a monic quadratic irreducible polynomial $f(t)$ satisfying condition $\mathrm{C}(\mu)$ such that $f(t) \neq t^2 - \mu$ and $f(X) = 0$.

Matrices of the first kind may be divided into subcategories as follows:

I(i) $X \sim \lambda I_2 \oplus X_2$, where X_2 is a 2×2 matrix that has neither λ nor $-\lambda$ as eigenvalues;

I(ii) $X \sim \lambda I_2 \oplus (-\lambda) I_2$;

I(iii) $X \sim \lambda I_3 \oplus (-\lambda) I_1$;

I(iv) X is λ-potent (that is, $\lambda I - X$ is nilpotent).

Of course if q is even then subcategories I(ii) and I(iii) are subsumed by I(iv) and category III is empty.

Our first goal is to reduce the calculation of $\nu(G)$ to groups G contained in $\mathrm{O}(V)$. If q is even then that is immediate because $\mathrm{GO}(V) = \mathrm{O}(V) \times Z$, $\nu(G) = \nu(G.Z) = \nu(G.Z \cap O(V))$. Suppose therefore that q is odd. The matrix equation $X^{\mathrm{tr}} A X = \mu X$ implies that $\det(X)^2 = \mu^4$ and so $\det(X) = \pm\mu^2$. There are two natural homomorphisms $\mathrm{GO}(V) \to Z_2$: one maps X to $\mu(X)$ modulo squares in $F^\times$; the other maps X to $\mu^{-2}\det(X)$. It is not hard to see that the intersection of their kernels is $\mathrm{SO}(V).Z$. Thus $\mathrm{GO}(V)/\mathrm{SO}(V).Z \cong Z_2 \times Z_2$ and there are five subgroups $G_0, \ldots, G_4$ of $\mathrm{GO}(V)$ that contain $\mathrm{SO}(V).Z$. They may be numbered so that $G_0 = \mathrm{SO}(V).Z$, $G_4 = \mathrm{GO}(V)$, and G_1, G_2, G_3 are the three subgroups of index 2 in $\mathrm{GO}(V)$. Of these, one is $\mathrm{O}(V).Z$, which can be described as $\{Y \in \mathrm{GO}(V) \mid \mu(Y) \text{ is square in } F^\times\}$ and which we take to be G_1; another is $\{Y \in \mathrm{GO}(V) \mid \det(Y) = \mu(Y)^2\}$, and we take this to be G_2. The third group is less easy to describe and we shall refer to it simply as G_3. All X of type I lie in G_1; those of types II, III, and IV lie in G_2.

From here on we find it prudent to deal separately with orthogonal spaces of positive and negative type. We treat the case $\varepsilon = -$ first. If $\varepsilon = -$ then $-I_4 \notin \Omega(V)$ (see, for example, [10, p. 165]) and so $\mathrm{SO}(V) = \Omega(V) \times \{\pm I_4\}$ and $\Omega(V).Z = G_0$. Thus $G.Z$ must be one of the five groups $G_1, \dots, G_4$. In order to reduce our problem to the study of groups contained in $\mathrm{O}(V)$ we consider the disposition of non-cyclic matrices lying outside G_1.

LEMMA 10.3. *Suppose that* $d = 4$, $\mathrm{type}(V) = -$, *and* q *is odd. Define* G_i *for* $0 \leqslant i \leqslant 4$ *as above and define* $\nu_0 := \nu(\Omega(V))$, $\nu_1 := \nu(\mathrm{O}(V))$. *Then* $\nu(G_0) = \nu_0$, $\nu(G_1) = \nu_1$,

$$\nu(G_2) = \frac{\nu_0}{2} + \frac{1}{2(q^2+1)}, \quad \nu(G_3) = \frac{\nu_0}{2}, \quad \textit{and} \quad \nu(G_4) = \frac{\nu_1}{2} + \frac{1}{4(q^2+1)}.$$

Proof. That $\nu(G_0) = \nu_0$ and $\nu(G_1) = \nu_1$ comes directly from the definitions of G_0 as $\Omega(V).Z$ and G_1 as $\mathrm{O}(V).Z$. We have already observed that there are no non-cyclic matrices in $G_3 \backslash G_0$ and so $\nu(G_3) = \frac{1}{2}\nu(G_0) = \frac{1}{2}\nu_0$. Thus to prove the substance of the lemma we need to find $\nu(G_2)$ and $\nu(G_4)$.

Consider non-cyclic matrices X in $\mathrm{GO}(V) \backslash G_1$, in other words, non-cyclic matrices for which μ is non-square, where $\mu := \mu(X)$. Since $\mathrm{type}(V) = -$ there are no totally singular subspaces of dimension 2 and so there are no X of type II. There are also none of type IV because all their two-dimensional X-invariant subspaces of V would have to have type $-$ (see Lemma 4.5.2) and so V would have type $+$, contrary to assumption. Thus X has type III. It follows easily from Lemma 4.5.3 that for a given non-square μ the non-cyclic matrices annihilated by $t^2 - \mu$ form a single conjugacy class under the action of $\mathrm{O}(V)$ and then, by Lemma 5.4(5), the number of them is $|\mathrm{O}(V)|/2(q^2+1)$. Since there are $\frac{1}{2}(q-1)$ choices for μ and $|\mathrm{O}(V)| = 2q^2(q^4-1)$, the number of non-cyclic matrices in $\mathrm{GO}(V) \backslash G_1$ is $\frac{1}{2}q^2(q-1)(q^2-1)$. Consequently,

$$\nu(G_4) = \frac{1}{|G_4|}\left(|G_1|.\nu(G_1) + \frac{1}{2}q^2(q-1)(q^2-1)\right) = \frac{\nu(G_1)}{2} + \frac{1}{4(q^2+1)},$$

since $|G_4| = 2q^2(q-1)(q^4-1)$. Similarly,

$$\nu(G_2) = \frac{1}{|G_2|}\left(|G_0|.\nu(G_0) + \frac{1}{2}q^2(q-1)(q^2-1)\right) = \frac{\nu(G_0)}{2} + \frac{1}{2(q^2+1)},$$

since $|G_2| = q^2(q-1)(q^4-1)$.

THEOREM 10.4. *Suppose that* $\Omega^-(4,q) \leqslant G \leqslant \mathrm{GO}(4,q)$. *If* q *is odd and* $G_0, \dots, G_4$ *are the groups between* $\Omega(V)$ *and* $\mathrm{GO}(V)$ *as described above* *then*

$$\nu(G) = \begin{cases} \dfrac{2q^3 - q^2 + 2q - 3}{q^4 - 1} & \textit{if } G.Z = G_0, \\ \dfrac{2q^4 - q^3 + 4q^2 - 3q + 2}{2q(q^4 - 1)} & \textit{if } G.Z = G_1, \\ \dfrac{2q^3 + 2q - 2}{2(q^4 - 1)} & \textit{if } G.Z = G_2, \\ \dfrac{2q^3 - q^2 + 2q - 3}{2(q^4 - 1)} & \textit{if } G.Z = G_3, \\ \dfrac{2q^4 + 4q^2 - 4q + 2}{4q(q^4 - 1)} & \textit{if } G.Z = G_4. \end{cases}$$

If q is even then

$$\nu(G) = \begin{cases} \dfrac{q^3 + q - 1}{q^4 - 1} & \textit{if } \mathrm{O}(V) \not\leqslant G, \\ \dfrac{q^4 + 2q^2 - q + 1}{2q(q^4 - 1)} & \textit{if } \mathrm{O}(V) \leqslant G. \end{cases}$$

Thus $\nu(G) = s(G)/2q + O(q^{-2})$ in all cases.

Proof. The lemma tells us that for odd q we need only compute ν_0 and ν_1, where $\nu_0 = \nu(\Omega(V))$ and $\nu_1 = \nu(\mathrm{O}(V))$. The same is of course true if q is even, for then $\mathrm{GO}(V) = \mathrm{O}(V) \times Z$ and $|\mathrm{O}(V) : \Omega(V)| = 2$. Adapting the argument in the first paragraph of the proof of the preceding lemma to matrices with multiplier 1, we see that if a matrix in $\mathrm{O}(V)$ is non-cyclic then it is of type I with $\lambda = \pm 1$.

For the matrices of type I(i) there is a decomposition $V = U \oplus W$ with respect to which $X = \lambda I_2 \oplus X_2$, where $\lambda = \pm 1$. Then $U \perp W$ and U, W must be non-degenerate. The elements of $\mathrm{O}(W)$ that cannot serve as X_2 are those that have an eigenvalue ± 1, namely $\pm I_2$ together with all elements of $\mathrm{O}(W) \backslash \mathrm{SO}(W)$. Thus we may count matrices of type I(i) by enumerating pairs (W, X_2), where W is a non-degenerate two-dimensional subspace of V and $X_2 \in \mathrm{SO}(W) \backslash \{\pm I_2\}$. For a given type ε' the number of possibilities for W of type ε' is $\frac{1}{2}q^2(q^2 + 1)$. Then the number of possibilities for $\lambda I_2 \oplus X_2$ is $2(q - 2 - \varepsilon')$ if q is odd and $q - 1 - \varepsilon'$ if q is even, and so the number of pairs (W, X_2) is $q^2(q^2 + 1)(q - 2 - \varepsilon')$ if q is odd and $\frac{1}{2}q^2(q^2 + 1)(q - 1 - \varepsilon')$ if q is even. Hence the number of non-cyclic matrices X of type I(i) is

$$\begin{array}{ll} 2q^2(q^2 + 1)(q - 2) & \text{if } q \text{ is odd,} \\ q^2(q^2 + 1)(q - 1) & \text{if } q \text{ is even.} \end{array}$$

If q is odd then $X \in \Omega(V)$ if and only if $-X \notin \Omega(V)$, and it follows that exactly half of these matrices lie in $\Omega(V)$. If q is even then, since $\dim \operatorname{Ker}(I_4 - X) = 2$, which is even, they all do. Therefore, since $|\mathrm{O}(V)| = 2q^2(q^4-1)$, while $|\Omega(V)| = \frac{1}{2}q^2(q^4-1)$ if q is odd and $|\Omega(V)| = q^2(q^4-1)$ if q is even, there are contributions

$$\text{to } \nu_1 \text{ of } \begin{cases} (q-2)/(q^2-1) & \text{if } q \text{ is odd,} \\ 1/2(q+1) & \text{if } q \text{ is even,} \end{cases}$$

$$\text{to } \nu_0 \text{ of } \begin{cases} 2(q-2)/(q^2-1) & \text{if } q \text{ is odd,} \\ 1/(q+1) & \text{if } q \text{ is even,} \end{cases}$$

from non-cyclic matrices of type I(i).

For the matrices of type I(ii) (when q is odd) there is a unique decomposition $V = U \oplus W$ with respect to which $X = I_2 \oplus -I_2$. If $u \in U$, $w \in W$, then $\varphi(u, w) = \varphi(uX, wX) = -\varphi(u, w)$. Therefore $U \perp W$ (that is, U, W are orthogonal to each other), and both U, W must be non-degenerate, one of positive type, the other of negative type. There are two conjugacy classes of elements X in $\mathrm{O}(V)$, depending on ε' where $\varepsilon' := \mathrm{type}(W)$ and, since $C_{\mathrm{O}(V)}(X) \cong \mathrm{O}^{-\varepsilon'}(2, q) \times \mathrm{O}^{\varepsilon'}(2, q)$, the number of matrices X in each class is $|\mathrm{O}(V)|/4(q^2-1)$. A class lies in $\Omega(V)$ if and only if $-I_2 \in \Omega(W)$, that is, if and only if $\varepsilon' = (-1)^{(q-1)/2}$ (see, for example, [10, p. 165]). Thus one class lies in Ω, the other does not, and the contributions to ν_1, ν_0 are $1/2(q^2-1)$ and $1/(q^2-1)$, respectively.

If $V = U \oplus W$ and $X = \lambda I_3 \oplus (-\lambda)I_1$ with respect to this decomposition, where $\lambda = \pm 1$, then $U \perp W$ and U, W must be non-degenerate. There are four conjugacy classes of such matrices in $\mathrm{O}(V)$, one for each choice of the pair $(\lambda, \mathrm{type}(W))$. Since they have determinant -1, these matrices do not lie in $\Omega(V)$. Clearly, $C_{\mathrm{O}(V)}(X) \cong \mathrm{O}(U) \times \mathrm{O}(W)$, and so the number of matrices in each class is $|\mathrm{O}(V)|/(2q(q^2-1) \times 2)$. Thus the contribution to ν_1 is $1/q(q^2-1)$ and the contribution to ν_0 is 0 from matrices of type I(iii).

If X is λ-potent then $X = \lambda X_1$ where X_1 is unipotent. When q is odd, all unipotent matrices lie in $\Omega(V)$ and they are all non-cyclic. By Steinberg's theorem the number of them is q^4. Since V has negative type, $-I_4 \notin \Omega(V)$ and if X_1 is unipotent then $-X_1 \notin \Omega(V)$. Thus the contributions to ν_1, ν_0 are $2q^4/|\mathrm{O}(V)|$ and $q^4/|\Omega(V)|$, that is, $q^2/(q^4-1)$ and $2q^2/(q^4-1)$, respectively. If q is even then $X \in \Omega(V)$ if and only if $\dim \operatorname{Ker}(I - X)$ is even. It follows that all unipotent matrices in $\Omega(V)$ are non-cyclic. By Steinberg's theorem the number of these is q^4 and they contribute $q^2/2(q^4-1)$ and $q^2/(q^4-1)$ respectively to ν_1, ν_0. There are, however, non-cyclic unipotent matrices also in $\mathrm{O}(V) \backslash \Omega(V)$. For such a matrix $\operatorname{Ker}(I - X)$ has dimension 3 and rank 2. Let U be a two-dimensional non-degenerate subspace of $\operatorname{Ker}(I - X)$ and let $W := U^{\perp}$. Then X is in Jordan canonical form $I_2 \oplus J_2$ with respect to the decomposition $V = U \oplus^{\perp} W$.

There are two conjugacy classes of these matrices in $\mathrm{O}(V)$ determined by the type ε' of U. Since there are q^2 choices for U in $\mathrm{Ker}(I-X)$, while $|C_U(I_2)| = 2(q-\varepsilon')$ and $|C_W(J_2)| = 2$, the corresponding centralisers have order $4q^2(q-\varepsilon')$. The contribution to ν_1 therefore is $1/4q^2(q-1)$ $+1/4q^2(q+1)$, which is $1/2q(q^2-1)$ (and the contribution to ν_0 is of course 0). Thus ν_1 acquires a contribution

$$\begin{array}{ll} q^2/(q^4-1) & \text{if } q \text{ is odd,} \\ q^2/2(q^4-1)+1/2q(q^2-1) & \text{if } q \text{ is even,} \end{array}$$

and ν_0 acquires a contribution

$$\begin{array}{ll} 2q^2/(q^4-1) & \text{if } q \text{ is odd,} \\ q^2/(q^4-1) & \text{if } q \text{ is even.} \end{array}$$

from matrices of type I(iv).

Adding the four contributions we find that if q is odd then

$$\begin{aligned} \nu_1 &= \frac{q-2}{q^2-1} + \frac{1}{2(q^2-1)} + \frac{1}{q(q^2-1)} + \frac{q^2}{q^4-1} \\ &= \frac{2q^4-q^3+4q^2-3q+2}{2q(q^4-1)}, \\ \nu_0 &= \frac{2(q-2)}{q^2-1} + \frac{1}{q^2-1} + \frac{2q^2}{q^4-1} = \frac{2q^3-q^2+2q-3}{q^4-1}, \end{aligned}$$

while if q is even then

$$\begin{aligned} \nu_1 &= \frac{1}{2(q+1)} + \frac{q^2}{2(q^4-1)} + \frac{1}{2q(q^2-1)} = \frac{q^4+2q^2-q+1}{2q(q^4-1)}, \\ \nu_0 &= \frac{1}{q+1} + \frac{q^2}{q^4-1} = \frac{q^3+q-1}{q^4-1}, \end{aligned}$$

and, substituting into the formulae of Lemma 10.3, we get the theorem.

Suppose from now on that $\varepsilon = +$; that is, (V, Q) is of positive type. Then $-I_4 \in \Omega(V)$ and $\Omega(V).Z$ is a subgroup G_{-1} of index 2 in G_0. In this case G_4/G_{-1} is dihedral of order 8, G_1/G_{-1} and G_2/G_{-1} are its two elementary abelian maximal subgroups of order 4, and G_3/G_{-1} is cyclic of order 4. Its centre is G_0/G_{-1} and conjugation by elements of $\mathrm{O}(V)$ interchanges the two cosets of G_{-1} in $G_2 \backslash G_0$.

Lemma 10.5. *Suppose that* $d = 4$, $\mathrm{type}(V) = +$, *and* q *is odd. Define* G_i *for* $-1 \leqslant i \leqslant 4$ *as above and define* $\nu_{-1} := \nu(\Omega(V))$, $\nu_0 := \nu(\mathrm{SO}(V)$,

$\nu_1 := \nu(\mathrm{O}(V))$. *If* $\Omega(V) \leqslant G \leqslant \mathrm{GO}(V)$ *and* $G.Z \nleqslant G_1$ *then*

$$\nu(G) = \begin{cases} \dfrac{\nu_1}{2} + \dfrac{q^2-q+4}{4q(q-1)(q^2-1)} & \text{if } G.Z = G_4, \\ \dfrac{\nu_0}{2} & \text{if } G.Z = G_3, \\ \dfrac{\nu_0}{2} + \dfrac{q^2-q+4}{2q(q-1)(q^2-1)} & \text{if } G.Z = G_2, \\ \dfrac{\nu_{-1}}{2} + \dfrac{q^2-q+4}{2q(q-1)(q^2-1)} & \text{otherwise.} \end{cases}$$

Proof. We count the non-cyclic matrices in $\mathrm{GO}(V)\backslash \mathrm{O}(V).Z$. These are of types II, III, and IV. Consider first matrices X of type II; that is, $X = \lambda I_2 \oplus (\mu/\lambda)I_2$ with totally singular eigenspaces U_1, U_2. For a given pair $\{\lambda, \mu/\lambda\}$ (with $\lambda^2 \neq \mu$) these matrices form a single class under conjugacy by elements of $\mathrm{O}(V)$. It is not hard to see that they lie in G_{-1} if μ is a square in $F^\times$ and otherwise they lie in $G_2\backslash G_0$ and are equally divided between the two cosets of G_{-1} in $G_2\backslash G_0$. The centraliser of one of them in $\mathrm{O}(V)$ is isomorphic to $\mathrm{GL}(2,q)$ and therefore the number of them is $2q^2(q^2-1)^2/q(q^2-1)(q-1)$, which is $2q(q+1)$. Since the number of pairs $\{\lambda, \mu/\lambda\}$ is $\frac{1}{2}(q-1)$ if μ is not square, it follows that the number of such matrices is $q(q^2-1)$ and the number in each of the two cosets of G_{-1} in $G_2\backslash G_0$ is $\frac{1}{2}q(q^2-1)$.

All matrices of type III lie in $G_2\backslash G_0$. For each non-square $\mu \in F^\times$ they form a single conjugacy class under $\mathrm{O}(V)$, and therefore the number of them is $\frac{1}{2}(q-1)|\mathrm{O}(V) : C|$, where, by Lemma 5.4, $|C| = 2(q^2-1)$. They are equally divided between the two cosets of G_{-1} in $G_2\backslash G_0$, and so each of those cosets contains $q^2(q-1)(q^2-1)/4$ of these matrices.

For a given quadratic minimal polynomial $f(t)$ satisfying $\mathrm{C}(\mu)$ the matrices of type IV form a single class under conjugation by elements of $\mathrm{O}(V)$. Since $\det(X) = \mu^2$ they lie in G_0 if and only if μ is a square. Those for which μ is non-square are equally divided between the two cosets of G_{-1} in $G_2\backslash G_0$. The size of the class is $|\mathrm{O}(V) : C|$, where, by Lemma 5.4, $|C| = q(q^2-1)(q+1)$. It is not difficult to see that the number of monic irreducible quadratic polynomials satisfying $\mathrm{C}(\mu)$ is $\frac{1}{2}(q+1)$ if μ is non-square. Therefore each coset of G_{-1} in $G_2\backslash G_0$ contains $\frac{1}{2}q(q^2-1)$ such matrices.

Now let G be a group such that $G_{-1} \leqslant G \leqslant G_4$, and $G \nleqslant G_1$. Define $H := G \cap G_1$. The possibilities are that $H = G_0$ and G is G_2 or G_3, or $H = G_1$ and $G = G_4$, or $H = G_{-1}$ and G is one of the two conjugate groups contained in G_2 such that $G/G_{-1} \cong Z_2$. If $H = G_0$ and $G = G_2$ then all the matrices treated above lie in G and so the number of non-cyclic matrices in G is $|G_0|\nu_0 + q(q^2-1) + \frac{1}{2}q^2(q-1)(q^2-1) + q(q^2-1)$, which is $\frac{1}{2}|G|\nu_0 + \frac{1}{2}q(q^2-1)(q^2-q+4)$ and, since $|G| = \frac{1}{2}|\mathrm{GO}(V)| = (q-1)q^2(q^2-1)^2$,

$$\nu(G) = \frac{\nu_0}{2} + \frac{q^2-q+4}{2q(q-1)(q^2-1)}.$$

If $H = G_0$ and $G = G_3$ then, since $G_3 \backslash G_0$ contains no non-cyclic matrices, $\nu(G) = \frac{1}{2}\nu_0$. The calculations for the cases where $G = G_4$ and where $H = G_{-1}$ and $G/H \cong Z_2$ are very similar to that for G_2 and are omitted.

In the light of this lemma, what remains is to analyse groups G such that $G.Z \leqslant G_1$. Since $G.Z = (G.Z \cap \mathrm{O}(V)).Z$ it is sufficient to treat groups H such that $\Omega(V) \leqslant H \leqslant \mathrm{O}(V)$. When q is even $H = \Omega(V)$ or $H = \mathrm{O}(V)$. But when q is odd $\mathrm{O}(V)/\Omega(V) \cong Z_2 \times Z_2$ and so there are five such groups. We label them $H_0, \ldots, H_4$, where $H_0 = \Omega(V)$, $H_1 = \mathrm{SO}(V)$, H_2 and H_3 are the other two subgroups of index 2 in $\mathrm{O}(V)$, and $H_4 = \mathrm{O}(V)$. The groups H_2, H_3 are conjugate in $\mathrm{GO}(V)$ and therefore $\nu(H_2) = \nu(H_3)$. It will be useful to distinguish the cosets of $\Omega(V)$ in $\mathrm{O}(V)$ and they will be listed as $\Omega_0, \ldots, \Omega_3$, where $\Omega_0 = \Omega(V)$ and $\Omega_1 = \mathrm{SO}(V) \backslash \Omega(V)$. The cosets Ω_2 and Ω_3, which may be taken to be $H_2 \backslash H_0$ and $H_3 \backslash H_0$, respectively, and whose union is $\mathrm{O}(V) \backslash \mathrm{SO}(V)$, are conjugate in $\mathrm{GO}(V)$ and therefore contain the same number of non-cyclic matrices.

LEMMA 10.6. *Let H be a group such that $\Omega^+(4,q) \leqslant H \leqslant \mathrm{O}^+(4,q)$. When q is odd,*

$$\nu(H) = \begin{cases} \dfrac{2q^4 - q^3 - 2(\eta-1)q^2 - 13q - 4}{q(q^2-1)^2} & \text{if } H = \Omega(V), \\ \dfrac{2q^4 - q^3 - 7q - 2}{q(q^2-1)^2} & \text{if } H = \mathrm{SO}(V), \\ \dfrac{2q^4 - q^3 - 2(\eta-2)q^2 - 13q - 6}{2q(q^2-1)^2} & \text{if } H = H_2 \text{ or } H = H_3, \\ \dfrac{2q^4 - q^3 + 2q^2 - 7q - 4}{2q(q^2-1)^2} & \text{if } H = \mathrm{O}(V), \end{cases}$$

where H_2, H_3 are the subgroups of index 2 in $\mathrm{O}(V)$ other than $\mathrm{SO}(V)$. And if q is even then

$$\nu(\Omega(V)) = \frac{q^4 + q^2 - 3q - 2}{q(q^2-1)^2},$$

$$\nu(\mathrm{O}(V)) = \frac{q^4 + 2q^2 - 3q - 3}{2q(q^2-1)^2}.$$

Proof. Our group H contains no matrices of type III; the only matrices of types I, II, and IV that are relevant are those with $\mu = 1$. For the matrices of type I(i) there is a decomposition $V = U \oplus W$ with respect to which $X = \lambda I_2 \oplus X_2$. As in the proof of Theorem 10.4, we may count matrices of type I(i) by enumerating pairs (W, X_2), where W is a non-degenerate two-dimensional subspace of V and $X_2 \in \mathrm{SO}(W)\backslash\{\pm I_2\}$. But now for a given type ε' the number of possibilities for W of type ε' is $\frac{1}{2}q^2(q+\varepsilon')^2$; then the number of possibilities for $\lambda I_2 \oplus X_2$ is $2(q-2-\varepsilon')$ if q is odd and $q-1-\varepsilon'$ if q is even, and so the number of pairs (W, X_2) is $q^2(q+\varepsilon')^2(q-2-\varepsilon')$ if q is odd, $\frac{1}{2}q^2(q+\varepsilon')^2(q-1-\varepsilon')$ if q is even. Hence the number of non-cyclic matrices X of type I(i) is

$$2q^2(q^3-2q^2-q-2) \qquad \text{if } q \text{ is odd,}$$

$$q^2(q^3-q^2-q-1) \qquad \text{if } q \text{ is even.}$$

When q is even all these matrices lie in $\Omega(V)$, but when q is odd the situation is more complicated. They all lie in $\mathrm{SO}(V)$, but $\lambda I_2 \oplus X_2$ lies in $\Omega(V)$ if and only if $\lambda I_2 \in \Omega(U)$, $X_2 \in \Omega(W)$ or $\lambda I_2 \notin \Omega(U)$, $X_2 \notin \Omega(W)$. Now $-I_2 \in \Omega^{\varepsilon'}(2,q)$ if and only if $\varepsilon' = \eta$, where $\eta = (-1)^{(q-1)/2}$ (see [10, p. 165]). If $\varepsilon' = \eta$ then $\lambda I_2 \in \Omega(U)$, $\pm I_2 \in \Omega(W)$ and so, multiplying together the number of possibilities for W, λ, and X_2 we find that the number of our matrices that lie in $\Omega(V)$ is $\frac{1}{2}q^2(q+\eta)^2 \times 2\times (\frac{1}{2}(q-\eta)-2)$. If $\varepsilon' = -\eta$ then $-I_2 \notin \Omega(U)$, $-I_2 \notin \Omega(W)$ and the number of our matrices in $\Omega(V)$ is $\frac{1}{2}q^2(q-\eta)^2 \times 2 \times (\frac{1}{2}(q+\eta)-1)$. Adding these two contributions we find that when q is odd the number of X of type I(i) lying in Ω_0 is $q^2(q^3-3q^2-(2\eta+1)q-3)$ and the remainder lie in Ω_1.

The matrices of type I(ii) are of interest only when q is odd. As in the case when $\varepsilon = -$, the eigenspaces U, W are orthogonal and non-degenerate, but now $\mathrm{type}(U) = \mathrm{type}(W) = \varepsilon'$, say. There are two conjugacy classes of elements X in $\mathrm{O}(V)$, one for each value of ε'. Since $C_{\mathrm{O}(V)}(X) \cong \mathrm{O}^{\varepsilon'}(2,q) \times \mathrm{O}^{\varepsilon'}(2,q)$ the number of matrices X in the class is $|\mathrm{O}(V)|/4(q-\varepsilon')^2$, which is $\frac{1}{2}q^2(q+\varepsilon')^2$. Both classes lie in $\mathrm{SO}(V)$; a class lies in $\Omega(V)$ if and only if $-I_2 \in \Omega(W)$, that is, if and only if $\varepsilon' = \eta$, where $\eta := (-1)^{(q-1)/2}$. Thus there are $\frac{1}{2}q^2(q+\eta)^2$ of these matrices in Ω_0, and $\frac{1}{2}q^2(q-\eta)^2$ of them in Ω_1.

For the matrices of type I(iii) when q is odd, $V = U \oplus^{\perp} W$, where U, W are non-degenerate, and $X = \lambda I_3 \oplus (-\lambda)I_1$ with respect to this decomposition. Since they have determinant -1, these matrices lie in $\Omega_2 \cup \Omega_3$. There are four conjugacy classes of them in $\mathrm{O}(V)$, one for each choice of the pair $(\lambda, \mathrm{type}(W))$. The conjugacy classes corresponding to pairs $(\lambda, +)$ and $(\lambda, -)$ are, however, interchanged by conjugation by an element of $\mathrm{GO}(V)$ with non-square multiplier and therefore one of these classes lies in Ω_2; the other lies in Ω_3. Clearly, $C_{\mathrm{O}(V)}(X) \cong \mathrm{O}(U) \times \mathrm{O}(W)$, and so the number of matrices in each class is $|\mathrm{O}(V)|/(2q(q^2-1)\times 2)$, that is, $\frac{1}{2}q(q^2-1)$. Therefore the number in each coset Ω_2, Ω_3 is $q(q^2-1)$.

The matrices of type I(iv) have the form λX_1 where X_1 is unipotent. When q is odd, all unipotent matrices lie in $\Omega(V)$, they are all non-cyclic, and by Steinberg's theorem the number of them is q^4. Since V has positive type, $-I_4 \in \Omega(V)$ and so all $2q^4$ of the matrices of type I(iv) lie in Ω_0. When q is even the analysis is very similar to that when type$(V) = -$ (see above). All the unipotent matrices in $\Omega(V)$ are non-cyclic and there are q^4 of them. The non-cyclic unipotent matrices in $\mathrm{O}(V)\backslash\Omega(V)$ have Jordan canonical form $I_2 \oplus J_2$ with respect to a decomposition $V = U \oplus^{\perp} W$ and there are two conjugacy classes of these matrices in $\mathrm{O}(V)$ determined by the type ε' of U. The corresponding centralisers have order $4q^2(q-\varepsilon')$ and so the classes have sizes $\frac{1}{2}(q+\varepsilon')(q^2-1)$. Thus there are $q(q^2-1)$ non-cyclic unipotent matrices in $\mathrm{O}(V)\backslash\Omega(V)$ when q is even.

Matrices X of type II have the form $\lambda I_2 \oplus \lambda^{-1}I_2$ with totally singular eigenspaces U_1, U_2. They all lie in $\Omega(V)$: if q is even this is because $\dim \mathrm{Ker}(I-X)$ is even, while if q is odd it can be calculated using the method given by Taylor in [10, p. 163]. For a given pair $\{\lambda, \lambda^{-1}\}$ (with $\lambda^2 \neq 1$) they form a single conjugacy class in $\mathrm{O}(V)$. The centraliser of one of them in $\mathrm{O}(V)$ is isomorphic to $\mathrm{GL}(2,q)$ and therefore the number in each class is $2q^2(q^2-1)^2/q(q^2-1)(q-1)$, which is $2q(q+1)$. Since the number of pairs $\{\lambda, \lambda^{-1}\}$ is $\frac{1}{2}(q-3)$ if q is odd and $\frac{1}{2}(q-2)$ if q is even, it follows that the number of such matrices is $q(q+1)(q-3)$ if q is odd, and $q(q+1)(q-2)$ if q is even.

For a given quadratic minimal polynomial $f(t)$ the matrices of type IV in $\mathrm{O}(V)$ form a single conjugacy class which lies in $\Omega(V)$. The size of the class is $|\mathrm{O}(V) : C|$, where, by Lemma 5.4, $|C| = q(q^2-1)(q+1)$. The number of monic irreducible quadratic polynomials satisfying C(1) is $\frac{1}{2}(q-1)$ if q is odd and it is $\frac{1}{2}q$ if q is even. Therefore there are $q(q-1)^2$ such matrices in $\Omega(V)$ if q is odd and $q^2(q-1)$ of them if q is even.

By this census we have found that when q is odd the number of non-cyclic matrices in Ω_0 is $q^2(q^3-3q^2-(2\eta-1)q-3)+\frac{1}{2}q^2(q+\eta)^2+2q^4+q(q+1)(q-3)+q(q-1)^2$, which is $\frac{1}{2}q(2q^4-q^3-2(\eta-1)q^2-13q-4)$. Similarly, the number of them in Ω_1 is $\frac{1}{2}q^2(2q^3-q^2+2(\eta-1)q-1)$ and there are $q(q^2-1)$ in each of Ω_2, Ω_3. When q is even there are $q^2(q^3-q^2-q-1)+q^4+q(q+1)(q-2)+q^2(q-1)$ non-cyclic matrices in $\Omega(V)$ and a further $q(q^2-1)$ in $\mathrm{O}(V)\backslash\Omega(V)$. That is, there are $q(q^4+q^2-3q-2)$ in $\Omega(V)$ and $q(q^4+2q^2-3q-3)$ in $\mathrm{O}(V)$. Elementary algebra yields the lemma.

Putting Lemmas 10.5 and 10.6 together we get exact values for $\nu(G)$ when $\Omega^+(4,q) \leqslant G \leqslant \mathrm{GO}^+(4,q)$. Theorem 10.4 gives exact values when $\Omega^-(4,q) \leqslant G \leqslant \mathrm{GO}^-(4,q)$. We are very grateful to Alice Niemeyer for enumerating the cyclic matrices in $\mathrm{O}^{\varepsilon}(4,q)$, $\mathrm{SO}^{\varepsilon}(4,q)$, and $\Omega^{\varepsilon}(4,q)$ for $q := 3, 4, 5$ to confirm that our formulae give the correct probabilities in these cases. Finally, recall the parameter $s(G)$ introduced in the first paragraph of Section 8. When q is odd it has the following values:

$$s(G) = \begin{cases} 4 & \text{if } G.Z \leqslant G_0, \\ 1 & \text{if } G.Z = G_4, \\ 2 & \text{otherwise.} \end{cases}$$

And combining this with Theorem 10.4, Lemma 10.5, and Lemma 10.6 we have the following as a crude summary.

THEOREM 10.7. *If* $\Omega^{\varepsilon}(4,q) \leqslant G \leqslant \mathrm{GO}^{\varepsilon}(4,q)$ *then* $\nu(G) = \frac{1}{2}s(G)q^{-1} + O(q^{-2})$.

REFERENCES

1. Michael Aschbacher, “Finite Group Theory,” Cambridge Univ. press, Cambridge, UK, 1986.
2. Jason Fulman, “Probability in the Classical Groups over Finite Fields: Symmetric Functions, Stochastic Algorithms and Cycle Indices,” Ph.D. thesis, Harvard University, 1997.
3. Jason Fulman, Cycle indices for the finite classical groups, *J. Group Theory* **2** (1999), 251–289.
4. Jason E. Fulman, Peter M. Neumann, and Cheryl E. Praeger, A generating function approach to the enumeration of cyclic and separable matrices in classical groups over finite fields, in preparation.
5. Robert M. Guralnick and Frank Lübeck, On p-singular elements in Chevalley groups in characteristic p, Preprint, January 24, 1999.
6. Peter Kleidman and Martin Liebeck, “The Subgroup Structure of the Finite Classical Groups,” London Math. Soc. Lect. Note Series 129, Cambridge Univ. press, Cambridge, UK, 1990.
7. Peter M. Neumann and Cheryl E. Praeger, Cyclic matrices over finite fields, *J. London Math. Soc. (2)* **52** (1995), 263–284.
8. Peter M. Neumann and Cheryl E. Praeger, Derangements and eigenvalue-free elements in finite classical groups, *J. London Math. Soc. (2)* **58** (1998), 564–586.
9. Peter M. Neumann and Cheryl E. Praeger, Exploiting cyclic matrices in computer algebra: Sharpening the Meataxe, in preparation.
10. Donald E. Taylor, “The Geometry of the Classical Groups,” Heldermann Verlag, Berlin, 1992.
11. G. E. Wall, On the conjugacy classes in the unitary, symplectic and orthogonal groups, *J. Austral. Math. Soc.* **3** (1963), 1–63.
12. G. E. Wall, Counting cyclic and separable matrices over a finite field, *Bull. Austral. Math. Soc.* **60** (1999), 253–284.