Available online at www.sciencedirect.com
SCIENCE DIRECT®
ELSEVIER
Linear Algebra and its Applications 408 (2005) 120–150
LINEAR ALGEBRA AND ITS APPLICATIONS
www.elsevier.com/locate/laa

Unitriangular actions on quadratic forms and character degrees ☆

Andrea Previtali

Dipartimento di Fisica e Matematica, Università dell'Insubria, Via Valleggio, 11 Como-22100, Italy

Received 11 February 2005; accepted 18 May 2005
Available online 8 August 2005
Submitted by R.A. Brualdi

Abstract

We determine canonical representatives and generating functions of orbit sizes for sesquilinear and quadratic forms under unitriangular action. These results are used to control how far character degrees and class sizes of unipotent subgroups of classical groups are from being powers of the order of the underlying field.

AMS classification: 20C15; 20C33; 20G40; 20E45; 15A33

Keywords: Representation theory; Finite groups of Lie type; Conjugacy classes; Quadratic and sesquilinear forms; Recurrence relations

1. Introduction

Let $G = G(F)$ be a classical group defined over a finite field F. As usual we call $p = \mathrm{char}(F)$ the *natural characteristic* of G. Let U be a maximal unipotent subgroup (or equivalently a Sylow p-subgroup) of G. If the natural module for G is the orthogonal sum of hyperbolic planes (maximal Witt index) and p is odd, we

☆ This research was supported by a fellowship from the Italian National Council for Research and from grants from the Cofin project "Teoria dei Gruppi e Applicazioni" while the author was visiting the mathematical department of the University College of Dublin.

E-mail address: andrea.previtali@uninsubria.it

0024-3795/$ - see front matter
doi:10.1016/j.laa.2005.05.003

have shown (see [18,19]) that all irreducible complex character degrees and conjugacy class sizes of U are q-powers, where $|F| = q^m$, $m = 2$ when $G = \mathrm{SU}(2n, F)$ and $m = 1$ when $G = \mathrm{Sp}(2n, F)$ or $G = \mathrm{SO}^+(2n, F)$. These results relied upon the existence of a maximal abelian normal subgroup A of U whose complement is isomorphic to the lower unitriangular group K of $\mathrm{SL}(n, F)$ and the fact that the same orbit sizes occurred under the action of K on A and on $\mathrm{Irr}(A)$ (*weak equivalence*). Examples given in [12,19] show that this is not true if $p = 2$, e.g. if $G = \mathrm{Sp}(4, q)$ then $q/2$ is both a character degree and a class size of U. In [17,9] we prove that any element of A or $\mathrm{Irr}(A)$ may be identified with a sesquilinear or a quadratic form. Moreover $C_U(a) = AC_K(a)$, where K acts on A via $a^k = kak^\tau$, where $(k_{ij})^\tau = (k^q_{ji})$. Therefore the orbit sizes under this action occur as conjugacy class sizes of U. On the other hand, let tr be the field trace from F to $\mathbb{F}_p$ and $\psi(a, b) = \mathrm{tr}\big(\sum_i (ab)_{ii}\big)$. Fix $\lambda \in \mathbb{C}^*$ such that $\lambda^p = 1$. Then ψ defines a non-degenerate pairing on $R = (F)_n$ and any $\chi \in \mathrm{Irr}(A)$ has shape $\chi(a) = \lambda^{\psi(a,b)}$, for some $b \in R$. Since $A = \ker(1 - \varepsilon\tau)$, i.e. $a^\tau = \varepsilon a$, where $\varepsilon = \pm 1$, we would like to determine $A^\perp$ and $R/A^\perp$. We can prove that these sets may be identified with sesquilinear and quadratic forms, respectively. They admit a K-module structure via the dual action of K on A. By Clifford theory the sizes of the orbits in this action occur as character degrees of U.

We first refine some results obtained in [14,9] providing canonical representatives for such forms under the action of K. It turns out that to any sesquilinear form f is uniquely associated an involution $\sigma = \sigma(f)$ of type $1^t 2^s$, and a list of $t + s$ scalars. This data is sufficient to recover the K-conjugacy class of f unless $\mathrm{char}(F) = 2$, where we need a further list of scalars of length s. For a quadratic form Q, not surprisingly, we also need its Arf invariant. To prove that this data completely characterize Q^K, we need to apply Witt's Lemma in an inductive argument, where, strangely enough, we increase the dimension of the underlying vector space. Moreover we define a recursive procedure to obtain the centralizer of a given form in K. In particular, we are able to obtain recursive relations for the generating function associated to the sequence counting the orbits of given size. It turns out that when p is odd the set of orbit sizes of K on B, $s(B, K)$, $B = A$ or $\mathrm{Irr}(A)$, has shape $\{q^j : 0 \leqslant j \leqslant b_G(n)\}$, where b_G is an explicit function depending only on the type of G. As we mentioned already $s(A, K) = s(\mathrm{Irr}(A), K)$ when p is odd (see [17]).

In the characteristic 2 case, we show that the same results hold when $B = A$. When $B = \mathrm{Irr}(A)$ the picture changes drastically. If G is of symplectic type, then A is the set of symmetric matrices and $\mathrm{Irr}(A)$ is equivalent as a K-set to the collection of quadratic forms. We pin down exactly $s(\mathrm{Irr}(A), K)$ in this case proving it coincides with $\left\{q^k/2^j : \binom{2j}{2} \leqslant k \leqslant \binom{n}{2}, 0 \leqslant j \leqslant \lfloor n/2 \rfloor\right\}$, generalizing results in [9].

The striking novelty here is that we have a complete control even on multiplicities and not only on the size of the orbits. Most of the results have been checked and conjectured using code written for `Magma` (see [5]) freely available on the author's web page `http:\\scienze-como.uninsubria.it\previtali\Research.html`. We also have the feeling that much more may be unearthed from the recurrence

relations describing the orbit size polynomials. We could not unfortunately find closed-forms for them, since these relations do not have hypergeometric coefficients in $n = \dim(V)$ (see [16,13]).

Finally we prove a non-degeneracy result on restricting sesquilinear forms to suitable subspaces and use some results from [18,19] to establish that any irreducible character of $U \in \mathrm{Syl}_2(\mathrm{SU}(2n, q^2))$, q even, has q-power degree.

We are confident that the techniques used in this paper will turn useful in the problem of determining the number of conjugacy classes of the unitriangular groups over $\mathbb{F}_q$ according to size, in particular whether this can be expressed by a polynomial in q (see [1–3,22]).

2. Notation

Given a finite group U we call $\mathrm{Irr}(U)$ the set of its irreducible complex characters, $\mathrm{cd}(U)$ the set of their degrees, $\mathrm{cc}(U)$ its conjugacy classes and $\mathrm{cs}(U)$ the class sizes of U. If $\mathrm{cs}(U) \subseteq \{q^j\}$ or $\mathrm{cd}(U) \subseteq \{q^j\}$, for some integer q, we say that U is a *q-power size* or *q-power degree* group. Given a vector space V, we denote with $\mathcal{F}$ a maximal flag in V and with b an ordered basis of V. If L, M are lists, $\mathrm{cut}(L, M)$ will be the sublist of L obtained striking out the elements in M, and $\mathrm{add}(L, M)$ will be the list obtained concatenating L with M. Let $[n]$ be the set $\{1, \ldots, n\}$. If σ is an involution, we define the set of its ancestors, $\Delta(\sigma)$ as $\{i : i < i^\sigma\}$. We denote with F the field of order q^m, $m = 2$ in the unitary case, $m = 1$ otherwise, with α the automorphism $x^\alpha = x^q$, for any $x \in F$, and with F_0 the fixed points $C_F(\alpha)$ of α. Given a sesquilinear form f on F^n, $N = N_f$ will the be the norm of f, namely $N(v) = f(v, v)$. We recall that f is *alternating* if $N \equiv 0$, *symmetric* if $f(u, v) = f(v, u)$ and *hermitian* if $f(u, v) = f(v, u)^q$, where $|F| = q^2$. We denote with $\tau = \tau(f)$ the endomorphism of $R = (F)_n$ defined via $(a_{ij})^\tau = (\varepsilon a_{ji}^q)$, where $\varepsilon = -1$ for alternating forms, 1 otherwise (see [6,23]).

3. Unitriangular equivalence

Let G be $\mathrm{Sp}(2n, F)$, $\mathrm{SO}^+(2n, F)$, or $\mathrm{SU}(2n, F)$, F a finite field. Denote with U a maximal unipotent subgroup of G. Then $U = A_0 \rtimes K_0$, where A_0 is a maximal abelian normal subgroup and K_0 is isomorphic to the lower unitriangular subgroup K of $\mathrm{GL}(n, F)$ (see [19]). Let $R = (F)_n$ be the full matrix algebra over F. Given $\beta \in \mathrm{Aut}(F)$ we define $\tau \in \mathrm{End}(R)$ via $(r_{ij})^\tau = (r_{ji}^\beta)$. Then A_0 is isomorphic to $\ker(1 - \varepsilon\tau)$, i.e. $a^\tau = \varepsilon a$, where $(\varepsilon, \beta) = (1, id_F)$, $(-1, id_F)$, or $(1, \alpha)$, $|\alpha| = 2$. The determination of $\mathrm{cs}(U)$ and $\mathrm{cd}(U)$ led us to consider the K-orbits of A under the action $a^k = kak^\tau$ (see [19]).

We now prove an existence and uniqueness result on canonical representatives for such orbits which may be of independent interest. The inspiration for the subsequent

assertions is the Bruhat decomposition for $\mathrm{GL}(n, F)$. In fact, $\mathrm{GL}(n, F) = \bigsqcup_i BwB$, where B is the Borel subgroup of lower triangular invertible matrices over F and w_i is associated to some element of the Weyl group $\mathcal{W}$ of $\mathrm{GL}(n, F)$. More precisely, $\mathcal{W} \cong \mathrm{Sym}_n$ and the w_i's may be chosen as permutation matrices. Let $V = F^n$ be endowed with a sesquilinear reflexive form f. We remind that reflexive means that f-orthogonality is a symmetric relation. Let $\alpha = \alpha(f) \in \mathrm{Aut}(F)$ be defined as $f(u, \lambda v) = \lambda^\alpha f(u, v)$.

We recall that, up to a change of basis, $V = \perp_i H_i$, where $\dim(H_i) = 1$ or H_i is a hyperbolic plane. Therefore one would expect such a result under the action of K up to scalars and permutations.

Since we will work by induction on $\dim(V)$, we feel we must provide a more intrinsic definition for the group K. We digress on the concept of height function and maximal flag.

Definition 1. Given an n-dimensional space V, we call $\mathcal{F}$ a *maximal flag* of V, if $\mathcal{F} = (V_0, V_1, \ldots, V_n)$, where $V_0 = 0$, $V_n = V$, $V_i \leqslant V_{i+1}$, and $\dim(V_{i+1}/V_i) = 1$.

Given $\mathcal{F}$, we may define a function $h = h_\mathcal{F}$ as $h_\mathcal{F}(v) = \min\{i \mid v \in V_i\}$. Then h satisfies some properties:

(H1) $h(v) = 0$ iff $v = 0$;
(H2) $h(\lambda v) \leqslant h(v)$, $\lambda \in F$;
(H3) $h(v_1 + v_2) \leqslant \max(h(v_1), h(v_2))$;
(H4) $h(V) = \{0, \ldots, \dim(V)\}$.

We remark that (H2) implies $h(v) = h(\lambda v)$, for $\lambda \neq 0$ and (H3), the ultrametric inequality, implies the apparently stronger statement that $h(v_1 + v_2) = h(v_2)$, if $h(v_1) < h(v_2)$.

Definition 2. If h from V to $\mathbb{N}$ satisfies (H1)–(H4), we call it a *height* function.

Conversely, given a height function h, we may define a maximal flag $\mathcal{F}_h$ of V as follows: $V_i = \{v \in V \mid h(v) \leqslant i\}$. In fact, by (H1)–(H3) V_i is a subspace of V, moreover, by (H4) $\exists v_{i+1}$ of height $i + 1$, so $V_i < V_{i+1}$. Finally $\dim(V_i) = i$. Using induction $\dim(V_i) \geqslant i$, but it can not be greater otherwise $\dim(V_n) > \dim(V)$.

It is easy to prove that the maps $\mathcal{F} \mapsto h_\mathcal{F}$ and $h \mapsto \mathcal{F}_h$ are inverse to each other. Given an ordered basis $b = (b_1, \ldots, b_n)$, define a maximal flag $\mathcal{F}$ of V whose elements are $V_i = \langle b_1, \ldots, b_i \rangle$. Let $C_{\mathrm{GL}}(V_i/V_{i-1}) = \{g \in \mathrm{GL}(V) : g_{V_i/V_{i-1}} = 1_{V_i/V_{i-1}}\}$ and $C(b) = \bigcap_{i=1}^n C_{\mathrm{GL}}(V_i/V_{i-1})$.

For example if b is the standard basis $(e_1, \ldots, e_n)$, then $K = C(b)$ coincides with the group of lower unitriangular matrices. In particular, we make the convention that V is a right K-module.

Example 3. Suppose that $N(e_1) = 0$, $f(e_1, e_2) = \beta$. For $k \in K$, $e_2^k = e_2 + ae_1$, $e_1^k = e_1$, then $f(e_1, e_2 + ae_1) = \beta$, so this value can not be reduced to 1. Moreover, $N(e_2 + ae_1) = N(e_2) + a\beta + \varepsilon(a\beta)^\alpha$, where $\alpha = \alpha(f)$, $\varepsilon = \pm 1$, may always be reduced to 0 unless $\alpha = id_F$, $\mathrm{char}(F) = 2$, and f is symmetric.

Definition 4. We say that (u, v) is a *generalized hyperbolic pair* for f, if $f(u, u) = f(v, v) = 0 \neq f(u, v)$ and call its span a *generalized hyperbolic plane* (ghp).

If f is symmetric and $\mathrm{char}(F) = 2$ we need another fundamental building block.

Example 5. Let $V = F^2$, $\mathrm{char}(F) = 2$, and f symmetric. If $N(e_1) = 0$, then $f^k = f$ for any $k \in K$; so V is not K-equivalent to a ghp.

Definition 6. We say that (u, v) is a *generalized elliptic pair* for f, if u is f-isotropic and $f(u, v) f(v, v) \neq 0$ and call its span a *generalized elliptic plane* (gep).

In the following examples we assume that $\mathrm{char}(F) = 2$ and f symmetric. We will only list those pairs (e_i, e_j) for which $f(e_i, e_j) = f(e_j, e_i) \neq 0$.

Example 7. Let $\mathrm{char}(F) = 2$, $V = \langle e_1, e_3\rangle \perp \langle e_2\rangle$, $f(e_1, e_3) = \beta$, $f(e_3, e_3) = \delta$ and $f(e_2, e_2) = \gamma$. Then $V = \langle e_1, e_3 + be_2\rangle \perp \langle e_2 + ae_1\rangle$, the orthogonal sum of a hyperbolic plane and an anisotropic vector, where $b = \sqrt{\delta/\gamma}$ and $a = \sqrt{\delta\gamma}/\beta$.

Example 8. Let $\mathrm{char}(F) = 2$, $V = F^4$, $f = \beta(e_{14} + e_{41}) + \gamma(e_{23} + e_{32}) + \delta e_{33} + \epsilon e_{44}$, $\beta\gamma\delta\epsilon \neq 0$. Again $V = \langle e_1, e_4 + \sqrt{\epsilon/\delta}e_3\rangle \perp \langle e_2 + \gamma\sqrt{\epsilon\delta}e_1, e_3 + \sqrt{\epsilon\delta}/\beta e_2\rangle$ is an orthogonal sum of a hyperbolic plane and an elliptic one.

We now provide an example of a four-dimensional space whose only at most two-dimensional orthogonal summands are gep.

Example 9. Let $\mathrm{char}(F) = 2$, $V = F^4$, and $f = \beta(e_{13} + e_{31}) + \gamma(e_{24} + e_{42}) + \delta e_{33} + \epsilon e_{44}$, $\beta\gamma\delta\epsilon \neq 0$. Thus $V = \langle e_1, e_3\rangle \perp \langle e_2, e_4\rangle$, a sum of two generalized elliptic planes. Let $V = B \perp B'$, with $B = \langle e_i^x, e_j^x\rangle$ and $B' = \langle e_k^x, e_l^x\rangle$, where $x \in K$ and $\{i, j, k, l\} = [4]$. Then $f = f^x$. In particular B, B' are generalized elliptic planes.

Proof. Let $e_1 \in B \Rightarrow B' \leqslant \langle e_1\rangle^\perp = \langle e_1, e_2, e_4\rangle \not\ni e_3^x \Rightarrow B' = \langle e_2^x, e_4^x\rangle$ and $B = \langle e_1, e_3^x\rangle$. Thus $e_4^x \in \langle e_1, e_2, e_4\rangle$. Since $N \equiv 0$ on $\langle e_1, e_2\rangle$ and $N(\sum \alpha_i e_i) = \sum \alpha_i^2 N(e_i)$, it follows that $N(e_i^x) = N(e_i)$, for $i = 3, 4$. Moreover $f(e_3^x, e_2^x) = 0$ forces $e_2^x = e_2$. Finally $e_i^x - e_i \in \langle e_1, e_2\rangle^\perp$, for $i = 3, 4$, so $f = f^x$. In particular B, B' are generalized elliptic planes. □

In general if $\langle e_1, e_i\rangle$ is an elliptic plane, then $e_i^k = e_i + \lambda e_1 + w$, $w \in \langle e_s \mid 1 < s < i\rangle = W$. Then e_i^k is isotropic iff $N(e_i) = N(w)$. This forces $N_W \not\equiv 0$. Example 9 shows that this condition is not sufficient to reduce an elliptic plane to a hyperbolic one.

Given a triple (V, f, b) where V is a vector space, b an ordered basis for V and f a sesquilinear form on V our aim is to determine a suitable element of $k \in C(b)$ such that with respect to b^k V becomes the orthogonal sum of one-dimensional subspaces, generalized hyperbolic or generalized elliptic planes, the latter occurring only when $\mathrm{char}(F) = 2$ and f is symmetric. (In fact, it is otherwise easy to transform a gep to a ghp.) Examples 8 and 7 show that a gep occurring as an orthogonal summand may be reduced to a hyperbolic one.

Definition 10. Given a triple (V, f, b), we say that V admits an *f-nice decomposition* with respect to b if $V = \perp_i H_i$, where H_i is generated by elements in b and has dimension 1 or is a ghp or a gep; the latter case occurring only if $\mathrm{char}(F) = 2$ and f symmetric. If $H = \langle u, v\rangle$ is a gep in the decomposition, we further require that there is no other orthogonal summand $H' = \langle w, z\rangle$ a gep with $u < w < z < v$ or $H' = \langle z\rangle$, z anisotropic and $u < z < v$, where $u < v$ means u occurs before v in b. We also say that f has *standard shape* with respect to b.

Theorem 11. *Given a triple (V, f, b), there exists $k \in K = C(b)$ so that V admits an f-nice decomposition with respect to b^k.*

Proof. We work by induction on $\dim(V)$. Let $b = (e_i)_{i=1}^n$.

(A) $e_1 \in \mathrm{Rad} f$: by induction $W = \langle e_i \mid i > 1\rangle$ admits a nice decomposition, that is, $\exists k' \in C(b')$, $b' = \mathrm{cut}(b, e_1)$ such that $\{e_i^{k'} \mid i > 1\}$, induces a nice decomposition on W. Now k' lifts to $k = 1 \perp k' \in C(b)$ and (e_i^k) induces a nice decomposition.

(B) $N(e_1) \neq 0$: $k : e_i \mapsto e_i - \frac{f(e_i, e_1)}{\mathrm{N}(e_1)} e_1$ lies in K and $V = \langle e_1\rangle \perp W$, where $W = \langle e_i^k : i > 1\rangle$. By induction $\exists k' \in C(b')$, $b' = \mathrm{cut}(b, e_1)$, such that $\{e_i^{kk'} \mid i > 1\}$ induces a nice decomposition. Now k' lifts to $u \in K$, say $e_i^u = e_i^{k'}$, $i > 1$, e_1 fixed. Thus $\{e_i^{ku}\}$ induces a nice decomposition.

(C) $N(e_1) = 0$, $e_1 \notin \mathrm{Rad} f$: set $i = \min\{j \mid f(e_1, e_j) \neq 0\}$ and substitute e_j with $e_j - \frac{f(e_j, e_i)}{f(e_i, e_1)} e_i$ for $j > i$, then e_j becomes orthogonal to e_1. Thus we may assume that $f(e_1, e_j) = 0$ for $j \neq i$. For $j \neq 1, i$, send e_j to $e_j - \frac{f(e_j, e_i)}{f(e_1, e_i)} e_1$, then these vectors are orthogonal to $\langle e_1, e_i\rangle$. Assume from the beginning that $W = \langle e_j \mid j \neq 1, i\rangle = \langle e_1, e_i\rangle^\perp$, then $\exists k' \in K'$ such that $\{e_j^{k'} \mid j \neq 1, i\}$ induces a nice decomposition on W, k' lifts to $k \in K$ so that $\{e_1, e_i, e_j^k\}$ induces a nice decomposition on V. If $N(e_i) = 0$ we are done. On the contrary suppose that $N(e_i) \neq 0$. Now $N(e_i + \lambda e_1) = N(e_i) + \lambda^\alpha f(e_i, e_1) + \lambda f(e_1, e_i)$, where $\alpha = \alpha(f) \in \mathrm{Aut}(F)$. If $|\alpha| = 2$, since F is finite, F/F_0 is separable and tr_{F/F_0} is onto, hence $\exists \lambda \in F$ such that $N(e_i + \lambda e_1) = 0$. If $\alpha = 1$ then $N(e_i + \lambda e_1) = N(e_i) + 2\lambda f(e_1, e_i)$ may be mapped

to zero unless $\mathrm{char}(F) = 2$ and $N(e_i) \neq 0$. In this circumstance examples 7, 8 show that the gep $\langle e_1, e_i\rangle$ may be modified until we obtain an f-nice decomposition for V. □

We now prove that such a decomposition is unique.

Theorem 12. *Given a triple (V, f, b), set $K = C(b)$. If $b = \{e_i\}$ and $b^k = \{e_i^k\}$ are f-nice bases, $k \in K$, then k is an f-isometry.*

Proof. (A) $e_1 \in \underline{\mathrm{Rad}}\, f$: remark that in general given $v \in \mathrm{Rad}\, f$, $\varphi \in \underline{\mathrm{End}}(V)$, $\overline{V} = V/\langle v\rangle$, $\overline{\varphi}(\overline{w}) := \overline{\varphi(w)}$, then φ is an isometry iff $\overline{\varphi}$ is such. Now set $\overline{V} = V/\langle e_1\rangle$, $\overline{b} = \overline{\mathrm{cut}(b, e_1)}$, then $\exists \overline{k} \in C(\overline{b})$ such that $\overline{e_i^k} = \overline{e_i}^{\overline{k}}$. By induction $\overline{k}$ is an isometry and the same holds for k.

(B) $N(e_1) \neq 0$: here $V = \langle e_1\rangle \perp \langle e_1\rangle^\perp$. Since $e_1^k = e_1$ and $\{e_i^k\}$ induces a nice decomposition, $W := \langle e_1\rangle^\perp$ equals $\langle e_i^k \mid i \geqslant 2\rangle$. By induction k_W is an isometry so that $k = 1_{\langle e_1\rangle} \perp k_W$ is an isometry, too.

(C) $N(e_1) = 0$, $e_1 \notin \mathrm{Rad}\, f$: let e_i be the unique vector in $b \setminus \langle e_1\rangle^\perp$. Set $H = \langle e_1, e_i\rangle$, then $W = H^\perp$ equals $\langle e_j \mid j \neq 1, i\rangle$. Let $V = L \perp Z$ be a nice decomposition with respect to b^k with $e_1 \in L$, L of minimal dimension. We claim that $L = \langle e_1, e_i^k\rangle$. In fact $f(e_1, e_i^k) = f(e_1, e_i + w) = f(e_1, e_i) \neq 0$, since $h(w) < i$. Recall that $Z = \langle e_j^k : j \in \Sigma\rangle$, for some subset $\Sigma \subseteq [n]$, thus $e_i^k \notin Z \Rightarrow e_i^k \in L$. Secondly, if $H \xrightarrow{\varphi} L$ and $W \xrightarrow{\psi} Z$ are isometries, then $\varphi \perp \psi$ is an isometry of V. Now $W = \langle e_j \mid j \neq 1, i\rangle = H^\perp$ and $Z = \langle e_j^k \mid j \neq 1, i\rangle = L^\perp$. Define on $\overline{V} = \langle e_1\rangle^\perp/\langle e_1\rangle$ the following metric $\overline{f}(\overline{v}, \overline{w}) := f(v, w)$ and consider

$$(W, \mathrm{Res}_W(f)) \xrightarrow{\beta} (\overline{V}, \overline{f}) \xrightarrow{\gamma} (\overline{V}, \overline{f}) \xrightarrow{\delta} (Z, \mathrm{Res}_Z(f))$$

acting elementwise

$$e_j \mapsto \overline{e_j} \mapsto \overline{e_j^k} \mapsto e_j^k, \quad j \neq 1, i.$$

We claim that β, γ, δ are isometries. Since W, $Z \subseteq \langle e_1\rangle^\perp$, we may consider the restriction of the canonical map $\langle e_1\rangle^\perp \xrightarrow{\pi} \overline{V}$ to these spaces. Since $\ker \pi = \langle e_1\rangle$, $W \cap \langle e_1\rangle = Z \cap \langle e_1\rangle = 0$, $\mathrm{Res}_W(\pi)$ and $\mathrm{Res}_Z(\pi)$ are monomorphisms. Since $\dim(W) = \dim(Z) = \dim(\overline{V})$, they are bijections and $\beta = \mathrm{Res}_W(\pi)$, $\delta = \mathrm{Res}_Z(\pi)^{-1}$. As is easily seen, they are also isometries. Let $\overline{b} = \mathrm{cut}(b, \{e_1, e_i\})^\pi$ then $\exists \overline{k} \in C(\overline{b})$ such that $\overline{e_j^k} = \overline{e_j}^{\overline{k}}$. Since $\{\overline{e_j}\}_{j\neq 1,i}$ and $\{\overline{e_j}^{\overline{k}}\}_{j\neq 1,i}$ induce nice decompositions on $\overline{V}$, by induction, we have that γ is an isometry. Thus $\mathrm{Res}_W(k) = \beta\gamma\delta$ is an isometry. We only need to prove that $H \xrightarrow{\mathrm{Res}_H(k)} L$ is an isometry. Assume the contrary. Since $e_1^k = e_1$ and $e_i^k - e_i \in \langle e_1\rangle^\perp$, we must have $N(e_i) \neq N(e_i^k)$. By symmetry assume $N(e_i) \neq 0$. Recall that under our assumption this forces $\mathrm{char}(F) = 2$. Thus

$$N(e_i) = N(e_i + \lambda e_1 + w) = N(e_i) + N(w),$$

where $w = \sum_{j=2}^{i-1} \omega_j e_j$. Thus $0 \neq N(w) = \sum_{j=2}^{i-1} \omega_j^2 N(e_j)$. But, by nice decomposability, $N(e_j) = 0$ in the summation range and we reach a contradiction. □

We describe the matrix associated to f with respect to a nice basis b. If $|b| = n$, then f is encoded by

1. an involution $\sigma = \sigma(f) \in S_n$ whose fixed points correspond to one-dimensional orthogonal summands and whose 2-cycles (i, j) prescribe the pairs $b_i, b_j \in b$ such that $f(b_i, b_j) \neq 0$;
2. the vector $N(b) = (N(b_i))$, where
   (a) if $p = 2$ and f symmetric then $N(b_i) = 0$ if $i < i^\sigma$ or $i^\sigma < j^\sigma \leqslant j < i$ with $N(b_j) \neq 0$;
   (b) otherwise $N(b_i) = 0$ if $i \neq i^\sigma$.

We would like to spend some words on the determination of $|C_K(f)|$. Let $B = N_{\mathrm{GL}}(K) = DK$, D a torus of GL, then $|f^{dK}| = |f^{Kd}| = |f^K|$. Hence, without loss of generality, we may substitute f with f^d, $d = \mathrm{diag}(d_1, \ldots, d_n)$. Assume that f has standard shape with respect to b. Since $f \mapsto f^d$ corresponds to $f_{ij} \mapsto d_i^\alpha f_{ij} d_j$ and at most two entries are different from zero on any row and column, we deduce that any nonzero entry of f may be reduced to 1, unless f is alternating; here non-diagonal entries equal to -1 must occur. When this happens we say that f has *reduced standard shape*. Such an f is therefore encoded by an involution σ and a $(0, 1)$-vector. We would like to analyze how $|f^K|$ is related to $\sigma(f)$. We need to recall that the number of inversions of σ, $I(\sigma)$, is the cardinality of $\{(i, j) : i < j, i^\sigma > j^\sigma\}$. This set is the disjoint union of $\Delta(\sigma) = \{(i, i^\sigma) : i < i^\sigma\}$, the trivial inversions, $\Delta^+ = \{(i, j) : i < j, i^\sigma > j^\sigma > i\}$, and $\Delta^- = \{(i, j) : i < j, \min(i^\sigma, i) > j^\sigma\}$. Moreover $(i, j) \leftrightarrow (j^\sigma, i^\sigma)$ induces a bijection between Δ^+ and Δ^-, so that $I(\sigma) = |\Delta(\sigma)| + 2|\Delta^+|$. We determine $|C_K(f)|$ restricting f on a suitable $C_K(f)$-module $\overline{V}$ in such a way that the restriction $\overline{f}$ still has reduced standard shape. We describe the setup we need to handle the various situations. Given a G-module V, we call the action of G on V the homomorphism $\rho : G \to \mathrm{End}(V)$. We need a somewhat technical lemma.

Lemma 13. *Assume f has reduced standard shape with respect to a basis b; set $K = C(b)$. Let v be the first vector in b. Then $\overline{V} = \langle v\rangle^\perp/\langle v\rangle$ is a $C_K(f)$-module endowed with a form $\overline{f} = f_{\overline{V}}$. Let ρ denote the induced action, $\overline{b} = \overline{(b \cap \langle v\rangle^\perp) \setminus \{v\}}$, $\overline{K} = C(\overline{b})$ then*

$$\ker \rho \rightarrowtail C_K(f) \overset{\rho}{\twoheadrightarrow} C_{\overline{K}}(\overline{f}).$$

Proof. Observe that $\rho : K \to \mathrm{GL}(\overline{V})$ is defined as $\overline{u}^{k^\rho} := \overline{u^k}$. Moreover let h denote the height function induced by the ordering on b, then $h(w^k - w) < h(w)$ implies $\overline{h}(\overline{w}^{k^\rho} - \overline{w}) < \overline{h}(\overline{w})$ for any $w \in b \cap \langle v\rangle^\perp$. Thus $\rho(K) \leqslant \overline{K}$. If $k \in C_K(f)$, then

$$\overline{f}(\overline{w}^{k^\rho}, \overline{u}^{k^\rho}) = \overline{f}(\overline{w^k}, \overline{u^k}) = f(w^k, u^k) = f(w, u) = \overline{f}(\overline{w}, \overline{u}),$$

hence $\rho(C_K(f)) \leqslant C_{\overline{K}}(\overline{f})$. The hard part is to prove that ρ is surjective. Choose $\overline{k} \in C_{\overline{K}}(\overline{f})$ and for any $\overline{u} \in \overline{b}$ let $\overline{u}^{\overline{k}} = \overline{w_u}$ for a fixed $w_u \in \langle v\rangle^\perp$. A candidate extension k for $\overline{k}$ should act on any element u of $b \cap \langle v\rangle^\perp$ as follows: $u^k = w_u + \mu_u v$. If $u, t \in b \cap \langle v\rangle^\perp$, then

$$f(u^k, t^k) = f(w_u, w_t) = \overline{f}(\overline{w_u}, \overline{w_t}) = \overline{f}(\overline{u}^{\overline{k}}, \overline{t}^{\overline{k}}) = \overline{f}(\overline{u}, \overline{t}) = f(u, t).$$

Therefore if $V = \langle v\rangle^\perp$ we are done. Otherwise, let z be the unique element in $b \setminus \langle v\rangle^\perp$, then $0 \neq f(v, z) = f(v, z^k)$, so

$$f(u^k, z^k) = f(w_u, z^k) + \mu_u f(v, z^k) = f(u, z)$$

is a non-trivial linear equation in μ_u, for any $u \in b \cap \langle v\rangle^\perp$. If $z = v$, then $z^k = z$ otherwise $z^k = z + \sum_{b \ni u < z} \lambda_u u = z + \lambda v + w$. Since $z \notin \langle v\rangle^\perp$, we have that

$$N(z^k) - N(z) = \lambda + \varepsilon\lambda^\alpha + N(w) = 0,$$

$\varepsilon = \pm 1$, admits a solution in λ unless $\mathrm{char}(F) = 2$, $\alpha = \alpha(f) = 1$. In this case we are led to the condition

$$0 = N(w) = N\left(\sum_{v<u<z} \lambda_u u\right) = \sum_{v<u<z} \lambda_u^2 N(u) = \left(\sum_{v<u<z} \lambda_u f_u\right)^2,$$

that is, $\sum_{v<u<z} \lambda_u f_u = 0$, where $N(u) = f_u^2 \in F$, which is linear in λ_u. In this way we proved that ρ is surjective. □

Lemma 14. *Given (V, f, b), where f has reduced standard shape with respect to b, let v be the first vector in $b \cap \mathrm{Rad}(f)$, $\overline{V} = V/\langle v\rangle$, $\overline{f} = f_{\overline{V}}$, $\overline{b} = \overline{\mathrm{cut}(b, v)}$, $\overline{K} = C(\overline{b})$. Then $\overline{f}$ has reduced standard shape with respect to $\overline{b}$ and $|C_K(f)| = |F|^{\dim(V)-h(v)}|C_{\overline{K}}(\overline{f})|$.*

Proof. Let ρ be the action of $C_K(f)$ on $\overline{V}$. Arguing as in Lemma 13 we see that $\rho(C_K(f)) = C_{\overline{K}}(\overline{f})$. Since $\ker\rho = \{k \in K : u^k - u = \mu_u v\}$, for any $u \in b, h(u) > h(v)$, it has order $|F|^{\dim(V)-h(v)}$. □

Applying Lemma 14 enough times we may assume that $\mathrm{Rad}(f) = 0$.

Theorem 15. *Let (V, f, b) be a triple with f in reduced standard shape with respect to b, $\mathrm{Rad}(f) = 0$. Let $\sigma = \sigma(f)$ be the involution associated to f. Set $K = C(b)$. Then there exists a triple $(\overline{V}, \overline{f}, \overline{b})$, where $\overline{V}$ is a $C_K(f)$-module, $\overline{f}$ in reduced standard shape with respect to $\overline{b}$, such that the sequence*

$$\ker\rho \rightarrowtail C_K(f) \overset{\rho}{\twoheadrightarrow} C_{\overline{K}}(\overline{f})$$

is exact, where $\overline{K} = C(\overline{b})$. *Let* $v = b_1$ *be the first element of* b, z *the unique basis vector not orthogonal to* v *and* $W = \langle u : v < u < z, u \in b \rangle$:

1. *if* $N(v) = 1$, *then* $|\ker \rho| = 1$ *and* $\overline{V} = \langle v \rangle^{\perp}$;
2. *if* $N(v) = 0$, f *alternating or* f *symmetric with* $\mathrm{char}(F) = 2$, *and* $N_W \equiv 0$, *then* $|\ker \rho| = |F|^{1^{\sigma}-1}$ *and* $\overline{V} = \langle v \rangle^{\perp}/\langle v \rangle$;
3. *if* $N(v) = 0$, f *hermitian, then* $|\ker \rho| = |F|^{1^{\sigma}-\frac{3}{2}}$ *and* $\overline{V} = \langle v \rangle^{\perp}/\langle v \rangle$;
4. *if* $N(v) = 0$, f *symmetric and either* $\mathrm{char}(F) \neq 2$ *or* $\mathrm{char}(F) = 2$ *and* $N_W \not\equiv 0$, *then* $|\ker \rho| = |F|^{1^{\sigma}-2}$ *and* $\overline{V} = \langle v \rangle^{\perp}/\langle v \rangle$.

Proof. We build the above exact sequence distinguishing several cases:

(A) $N(v) = 1$: $L = \langle v \rangle^{\perp}$ is K-invariant and restriction realizes an isomorphism between $C_K(f)$ and $C_{N_K(L)}(f_L)$.

(B) $N(v) = 0$: let $\overline{V}$ be $\langle v \rangle^{\perp}/\langle v \rangle$ endowed with $\overline{f}$, $\overline{f}(\overline{v}, \overline{w}) = f(v, w)$. Define $\overline{b} = \overline{\mathrm{cut}(b, \{v, z\})}$, $\overline{K} = C(\overline{b})$, and let ρ be the induced action on $\overline{V}$. Then Lemma 13 proves that $\rho(C_K(f)) = C_{\overline{K}}(\overline{f})$. Clearly $\overline{f}$ has reduced standard shape with respect to $\overline{b}$. To determine the order of $\ker \rho$ we apply again Lemma 13. Referring to the notation used there, we know that μ_u's are determined by $z^k = z + \lambda v + w$, and $N(z)$ is preserved iff $\varepsilon\lambda + \lambda^{\alpha} + N(w) = 0$. We must consider different situations. If f is alternating, there is no condition, hence $|\ker \rho| = |F|^{1^{\sigma}-1}$. If f is hermitian, then $k \in C_K(f)$ iff $\mathrm{tr}(\lambda) + N(w) = 0$, which admits $|F|^{1^{\sigma}-\frac{3}{2}}$ solutions (λ, w). If f is symmetric, then $k \in C_K(f)$ iff $2\lambda + N(w) = 0$. If $\mathrm{char}(F) \neq 2$ the former condition admits $|F|^{1^{\sigma}-2}$ solutions, otherwise $N(w) = L(w)^2$ for some linear form L. Clearly $L \equiv 0$ iff $N_W \equiv 0$. □

As we proved in [17] when $\mathrm{char}(F)$ is odd any orbit has q-power size, $|F| = q^m$, $m = 2$ in the unitary case, 1 otherwise. Here we extend this result to any prime, an improvement justified by the section on quadratic forms.

Corollary 16. *Given a sesquilinear form* f *on* $V = F^n$, $|F| = q^{|\alpha(f)|}$ *and* $K = C(\mathcal{F})$, $\mathcal{F}$ *a maximal flag in* V, *then* $|f^K|$ *is a* q*-power.*

We apply Theorem 15 to obtain more detailed information on orbit sizes and their multiplicities. We organize it using generating functions. It turns out that we have to distinguish four cases:

(A) alternating;
(H) hermitian;
(S) symmetric in odd characteristic;
(B) symmetric in even characteristic.

The last case requires a more difficult analysis.

Definition 17. Given a sequence $\{a_i\}_{i\geqslant 0}$, we call $a(t)=\sum_{i\geqslant 0} a_i t^i$ its generating function.

Notice that formally a generating function is a power series in the indeterminate t. Given $n\in\mathbb{N}$ and a field F of order q^m, m equals 2 in case **H**, 1 otherwise, we define for each of the four cases a generating function which turns out to be a polynomial in t.

Definition 18. We denote $\ell_n(t)$ the polynomial $\sum_{i\geqslant 0}\ell_{ni}t^i$, where ℓ_{ni} counts the number of orbits of order q^i in case L, L $\in\{\mathbf{B},\mathbf{A},\mathbf{S},\mathbf{H}\}$. We call $\ell_n(t)$ the *orbit size polynomial* in case L.

We obtain initial conditions and recurrence equations of degree 2 for the orbit polynomials in the first three cases and derive some useful consequences from this description. Unfortunately these equations do not meet the requirements in [16] or [13], since their coefficients are sum of hypergeometric terms in n not reducible to a single hypergeometric term.

Theorem 19. *Let ℓ_n be the orbit size polynomial in case* L *over $\mathbb{F}_{q^m}$. Set $w=q-1$, then $\ell_n\in\mathbb{N}[w,t]$ and, for $n\in\mathbb{N}$,*

$$\ell_{n+2}=c_n\ell_{n+1}+d_n\ell_n, \tag{1}$$

where $c_n,d_n\in\mathbb{N}[w,t]$ and ℓ_0,ℓ_1 are as follows:

- **(A)** $c_n=1$, $d_n=wt^n\frac{t^{n+1}-1}{t-1}$, $\ell_0=\ell_1=1$, $\deg_w\ell_n=\lfloor\frac{n}{2}\rfloor$, $\deg_t\ell_n=\binom{n}{2}-\lfloor\frac{n}{2}\rfloor$;
- **(S)** $c_n=1+wt^{n+1}$, $d_n=wt^{n+1}\frac{t^{n+1}-1}{t-1}$, $\ell_0=1$ *and* $\ell_1=w+1$, $\deg_w\ell_n=n$, $\deg_t\ell_n=\binom{n}{2}$;
- **(H)** $c_n=1+wt^{2n+2}$, $d_n=w(w+2)t^{2n+1}\frac{t^{2n+2}-1}{t^2-1}$, $\ell_0=1$ *and* $\ell_1=w+1$, $\deg_w\ell_n=n$, $\deg_t\ell_n=n(n-1)$.

Write $\ell_n(w,t)=\sum_i\ell_{n,i}(w)t^i=\sum_j\hat{\ell}_{n,j}(t)w^j$, then $\ell_{n,i}$ has coefficients independent from w. Moreover, $\ell_{n,i}(w)\neq 0$ as polynomials in w for $0\leqslant i\leqslant\deg_t\ell_n$. In particular $\ell_{n,i}(u)>0$ in the same range for any $u\in\mathbb{N}_{>0}$, that is, any orbit size occurs. A similar conclusion holds for $\hat{\ell}_{n,j}$. Finally $\ell_{n,i}(0)=\delta_{0,i}$.

Proof. We denote with a_n, s_n, and h_n the polynomial ℓ_n in case **A**, **S**, and **H**. The initial conditions were obtained with explicit calculations for $n=1,2$ and using the recurrence equation (1) backwards to get ℓ_0. We work out the details only in case **H**, the other cases being similar. So let (V,f,b) be a triple with f hermitian in standard shape, $|b|=n+2$. If $e_1\in\mathrm{Rad}(f)$, then $f=0\perp\overline{f}$ and $|f^K|=|\overline{f}^{\overline{K}}|$ leading to a contribution of h_{n+1} to h_{n+2}. If $N(e_1)=\nu\neq 0$, then $f=\nu\perp$

$\overline{f}$ and $|f^K| = q^{2(n+1)}|\overline{f}^{\overline{K}}|$. Now $N(e_1)$ may assume $q-1 = |F_0^*|$ values. Thus we obtain a further contribution of $(q-1)t^{2(n+1)}h_{n+1}$. Otherwise assume i is the unique index such that $f(e_1, e_i) \neq 0$, then $f = f_1 \perp \overline{f}$, where $f_1 = f_L$, $\overline{f} = f_{L^\perp}$ and $L = \langle e_1, e_i\rangle$. By Theorem 19 $|f^K| = q^{4n+5-2i}|\overline{f}^{\overline{K}}|$. In fact, $|K| = q^{4n+2}|\overline{K}|$ and $|C_K(f)| = q^{2i-3}|C_{\overline{K}}(\overline{f})|$. Since $f(e_1, e_i)$ may assume $q^2-1 = |F^*|$ values, we get a final contribution of

$$(q^2-1)\left(\sum_{i=2}^{n+2} t^{4n+5-2i}\right)h_n = (q^2-1)t^{2n+1}\frac{t^{2(n+1)}-1}{t^2-1}h_n.$$

We show by induction on n that $\deg_t h_n = n(n-1)$ and $0 \neq h_{n,i}(w) \in \mathbb{N}[w]$ for $0 \leqslant i \leqslant n(n-1)$, where $w = q-1$. This holds for $n = 0, 1$. Using induction and the first summand on the right hand side of the recurrence relation (1) we see that $0 \neq h_{n+2,i} \in \mathbb{N}[w]$ unless $(n+1)n < 2n+1$, namely $n = 0, 1$. In these cases the second summand involves non-zero polynomial coefficients in w for t^{2n+1}. Thus

$$\deg_t h_{n+2} = \max(2(n+1) + \deg_t h_{n+1}, 4n+1+\deg_t h_n) = (n+2)(n+1)$$

by an easy induction argument. Again induction and the shape of the first summand in the recurrence equation (1) show that $0 \neq \hat{h}_{n,i}(t) \in \mathbb{N}[t]$ for $0 \leqslant i \leqslant n$. The final claim also follows by induction on n since $h_{n+2}(0,t) = h_{n+1}(0,t) = h_1(0,t) = 1$. □

We now turn to the more difficult case **B**. To deal with this case we need to remark that when F is a perfect field of characteristic 2, then N, the norm function corresponding to a given symmetric form f, is the square of a linear form. In fact, $N\left(\sum_i \lambda_i e_i\right) = \sum_i \lambda_i^2 N(e_i) = \left(\sum_i \sqrt{N(e_i)}\lambda_i\right)^2$. Moreover, given an ordered basis $b = (e_1, \ldots, e_n)$ and the associated maximal flag $0 = V_0 < V_1 < \cdots < V_n = F^n$, $V_i = \langle e_1, \ldots, e_i\rangle$, we may define the *depth* of f, $m(f)$, to be 0 if f is alternating or $\min\{j : N_{V_j} \not\equiv 0\}$, where $N(v) = f(v, v)$. Then $m(f) = \min\{j : N(e_j) \neq 0\}$ and $m(f) = m(f^k)$, for any $k \in K = C(b)$. Namely $m(f)$ is an invariant of the orbit f^K.

Definition 20. Let $F = \mathbb{F}_q$, q even. We denote with $b_{nj}(t)$ the polynomial $\sum_{i\geqslant 0} b_{nji}t^i$, where b_{nji} counts the number of orbits of order q^i of symmetric forms f of dimension n over F with $m(f) = j$. Notice that $b_{n0} = a_n$. We set $b_{nj} = 0$ if $j < 0$ or $j > n$.

We now provide recursive equations satisfied by b_{nj}. Notice that in case **B** the orbit size polynomial b_n equals $\sum_{j=0}^n b_{nj}$. We apply the convention $\sum_a^b t = 0$ if $a > b$.

Theorem 21. *Let b_{nj} denote the orbit size polynomials relative to symmetric forms f with $m(f) = j$ of dimension n over $\mathbb{F}_q$, q even. Set $w = q - 1$. Then b_{nj} is completely determined by the following initial conditions and recurrence equations*:

(a) $b_{n0} = a_n$;
(b) $b_{n1} = wt^{n-1} \sum_{k=0}^{n-1} b_{n-1,k}$;
(c) *for* $2 \leqslant j \leqslant n$,

$$b_{nj} = b_{n-1,j-1} + wt^{2n-j-1}\frac{t^{j-2}-1}{t-1}b_{n-2,j-2} + wt^{n-1}\frac{t^{n-j}-1}{t-1}b_{n-2,j-1} + w^2t^{2n-2-j}\left(a_{n-2} + \sum_{k=j-1}^{n-2} b_{n-2,k}\right).$$

Moreover, $b_{nj} \in \mathbb{N}[w,t]$, $\deg_t(b_{n0}) = \lfloor \frac{n}{2} \rfloor$, $\deg_t(b_{nj}) = n$, *for* $1 \leqslant j \leqslant 1 + \lfloor \frac{n}{2} \rfloor$, $\deg_t(b_{n,1+\lfloor \frac{n}{2} \rfloor + j}) = n - j$, *for* $1 \leqslant j \leqslant \lfloor \frac{n-1}{2} \rfloor$ *and* $\deg_w(b_{n0}) = \binom{n}{2} - \lfloor \frac{n}{2} \rfloor$, $\deg_w(b_{nj}) = \binom{n}{2} - \lfloor \frac{j}{2} \rfloor$, *for* $1 \leqslant j \leqslant n$. *In particular*, *since* $b_n = \sum_{j=0}^{n} b_{nj}$, $\deg_w b_n = n$, $\deg_t b_n = \binom{n}{2}$ *and any orbit size* q^i, i *in the range* $0, \ldots, \binom{n}{2}$, *occurs*.

Proof. Claim (a) is immediate since b_{n0} counts alternating form orbits by convention. If $m(f) = 1$, then $f = N(e_1) \perp \overline{f}$, where $\overline{f}$ is arbitrary. Since $|f^K| = q^{n-1}|\overline{F}^{\overline{K}}|$, we get claim (b). Assume $j = m(f) \geqslant 2$, with f in standard shape. If $e_1 \in \mathrm{Rad}(f)$, then $f = 0 \perp \overline{f}$, $|f^K| = |\overline{f}^{\overline{K}}|$, and $m(\overline{f}) = j - 1$. So we get a contribution to b_{nj} of $b_{n-1,j-1}$. Otherwise let i be the unique index such that $f(e_1, e_i) \neq 0$. Then $f = f_1 \perp \overline{f}$, where f_1 has dimension 2 and $\overline{f}$ dimension $n - 2$. We distinguish 3 cases:

1. $1 < i < j$: here $m(\overline{f}) = j - 2$. By Theorem 15.2 the contribution amounts to $wt^{2n-2-i}b_{n-2,j-2}$. Since $\sum_{i=2}^{j-1} t^{2n-2-i} = t^{2n-j-1}\frac{t^{j-2}-1}{t-1}$ we get the term $wt^{2n-j-1}\frac{t^{j-2}-1}{t-1}b_{n-2,j-2}$;
2. $i = j$: here $m(\overline{f}) \geq j - 1$ or $m(\overline{f}) = 0$. By Theorem 15.2 the contribution amounts to $w^2t^{2n-2-i}b_{n-2,j-2}(a_{n-2} + \sum_{k=j-1}^{n-2} b_{n-2,k})$. Notice that the factor w^2 counts the number of choices for $f(e_1, e_i)$ and $N(e_i)$ in F^*;
3. $n \geq i > j$: here $m(\overline{f}) = j - 1$. By Theorem 15.4 the contribution amounts to $wt^{2n-1-i}b_{n-2,j-1}$. Since $\sum_{i=j+1}^{n} t^{2n-1-i} = t^{n-1}\frac{t^{n-j}-1}{t-1}$ we get the term $wt^{n-1}\frac{t^{n-j}-1}{t-1}b_{n-2,j-1}$.

The remaining part of the assertion follows by induction on n using the recurrence equation. □

We have implemented these recurrences in Magma (see [5]) using the two variable generating polynomial $B_n(w,t,u) = \sum_j b_{nj}(w,t)u^j$. Thus $b_n(w,t) = B_n(w,t,1)$.

Example 22. $B_3(w,t,u) = (w^2t^2 + w^2t + w^2 + w)u^3 + ((w^3 + 2w^2)t^2 + (w^2 + w)t)u^2 + ((w^3 + w^2)t^3 + w(w^2 + 2w + 1)t^2)u + wt^2 + wt + w + 1$ and $b_3(w,t) = (w^2 + 2w + 1) + 2w(w + 1)t + w(2w^2 + 5w + 2)t^2 + w^2(w + 1)t^3$.

We point out that instead of looking for global information, one might use Theorem 15 to get $|f^K|$, f in reduced standard shape. If we consider the case when σ is a fixed-point-free involution,

$$\Delta^+(\sigma(f)) = \left\{(i,j) : i < j,\ i^\sigma > j^\sigma > i\right\},$$

$\overline{V} = \frac{\langle e_1\rangle^\perp}{\langle e_1\rangle}$, then $\Delta^+(\sigma(\overline{f})) = \{(i,j) \in \Delta^+(\sigma(f)) : i,j \notin \{1, 1^\sigma\}\}$. Now $(i,j) \in \Delta^+(\sigma(f))$ iff $1^\sigma > j^\sigma > 1$, while $(i,1^\sigma), (1^\sigma, j) \notin \Delta^+(\sigma(f))$. So $|\Delta^+(\sigma(f))| = 1^\sigma - 2 + |\Delta^+(\sigma(\overline{f}))|$ and we may relate the number of inversions of $\sigma = \sigma(f)$ to $|f^K|$ (see [14]).

4. Quadratic forms

As we saw in [17,18], $\mathrm{cd}(U)$ was related to $s(A,K) = \{|f^K| : f \in A\}$, the set of sizes of K-orbits on A. There we proved that $s(A,K) = s(\mathrm{Irr}(A),K)$ associating to any element of $\mathrm{Irr}(A)$ a unique element of A provided $\mathrm{char}(F) \neq 2$. Isaacs [12] proved the latter equality does not hold when $\mathrm{char}(F) = 2$ and G is a symplectic group. Recall that in this situation A may be identified with the set of symmetric matrices on F. We will show that its dual $\mathrm{Irr}(A)$ coincides as a K-set with $\mathcal{Q}(V)$, the collection of quadratic forms on $V = F^n$.

Lemma 23. *Denote with $R = (F)_n$, $\tau \in \mathrm{End}(R)$ the transposition, $S = \ker(1-\tau)$, $T = R^{1-\tau}$, and ψ the bilinear pairing on R defined as $\psi(a,b) = \mathrm{tr}(ab) \in F$. Then ψ is non-degenerate and $S^\perp = T$.*

Proof. Choose $0 \neq a \in R$, $\exists a_{ij} \neq 0$, then $\psi(ae_{ji}) = a_{ij}$ and ψ is non-degenerate. Now $\psi(s, a^{1-\tau}) = \psi(s,a) - \psi(s,a^\tau) = \psi(s,a) - \psi(a,s) = 0$, for $s \in S$, $a \in R$. Thus $T \leqslant S^\perp$. Since $n^2 = \dim(S) + \dim(S^\perp) = \dim(S) + \dim(T)$, we have equality. □

For any $a \in R$ we may define a quadratic form $Q_a : V \to F$ as $Q_a(x) = xax^\tau$, $x \in V$. Define $\rho : R \to \mathcal{Q}(V)$ as $a^\rho = Q_a$.

Lemma 24. *Let ρ be defined as $a^\rho = Q_a$, then $T \rightarrowtail R \overset{\rho}{\twoheadrightarrow} \mathcal{Q}(V)$ is exact.*

Proof. Clearly ρ is surjective. Now $Q_a(x) = \sum_i a_{ii}x_i^2 + \sum_{i\neq j}(a_{ij} + a_{ji})x_i x_j \equiv 0$ iff $a_{ii} = a_{ij} + a_{ji} = 0$ iff $a \in T$. □

Therefore as vector spaces $\widehat{S} \simeq R/T \simeq \mathcal{Q}(V)$. Now S is a K-set via $s \mapsto ksk^\tau$. Since $\mathrm{tr}(bksk^\tau) = \mathrm{tr}(k^\tau bks)$, we see that the dual action of K on $\widehat{S} \simeq R/T$ is given by $(b+T)^k = k^\tau bk + T$. So if we define a K-action on $\mathcal{Q}(V)$ via $Q_b^k = Q_{k^\tau bk}$ we see that $\widehat{S}$ and $\mathcal{Q}(V)$ are K-equivalent sets. Our goal will be to classify the K-orbits on $\mathcal{Q}(V)$, their sizes and to determine canonical representatives as we did for sesquilinear forms. Trying to figure out the shape of a canonical representative we worked on some examples which turned out to be the paradigm for all situations.

From now on we assume that $\mathrm{char}(F) = 2$, Q will always denote a quadratic form on V and $f = \mathrm{Pol}(Q)$ its polarization, that is, the bilinear alternating form defined via

$$f(v, w) = Q(v + w) + Q(v) + Q(w).$$

In what follows we essentially assume that we are given an ordered basis for V with stabilizing group K and an alternating form in standard shape with respect to this basis. We would like to analyze which moves are allowed to reduce most of the values of Q on this basis to zero acting via f-isometries. We start with the case when there exists a non singular vector in $\mathrm{Rad}(f)$.

Example 25. Assume $u \in \mathrm{Rad}(f)$ and $Q(u) \neq 0$. Choose v such that $h(v) > h(u)$, then $k : v \mapsto v + au$ is an f-isometry in K and $Q(v + au)$ may be reduced to zero for a suitable a.

We next examine reduction on non-degenerate planes.

Example 26. Let $f = \alpha(e_{12} + e_{21}) \neq 0$, $Q(e_1) = 0$. Then $C_K(f)$ coincides with the maps fixing e_1 and applying e_2 to $e_2 + ae_1$. Now $Q(e_2 + ae_1) = Q(e_2) + a\alpha$ may be reduced to zero for a suitable $a \in F$.

Definition 27. We say that (u, v) is a *Q-singular pair* if (u, v) is an f-generalized hyperbolic pair and u, v are Q-singular.

We need to digress on the maps defined as $\wp_{\beta,\alpha}(a) = \beta a^2 + \alpha a$. Those maps are elements of $\mathrm{End}_{\mathbb{F}_2}(F)$. If $\alpha\beta = 0$, $(\alpha, \beta) \neq 0$, then $\wp_{\beta,\alpha}(F) = F$. Thus assume $\alpha\beta \neq 0$, then $\wp_{\beta,\alpha}(a) = \wp_{1,\frac{\alpha}{\sqrt{\beta}}}(\sqrt{\beta}a)$. Set $\wp_\alpha = \wp_{1,\alpha}$, $\wp = \wp_1$, then $\wp_\alpha(a) = \alpha^2\wp(a/\alpha)$. Now $\ker\wp = \mathbb{F}_2$ has order 2 and $\wp(F)$ is an $\mathbb{F}_2$-hyperplane of F. Call $T = \{0, \tau\}$ a transversal for $\wp(F)$ in F, then $T_\alpha = \{0, \alpha^2\tau\}$ is a transversal for $\wp_\alpha(F)$ in F.

Proposition 28. *If $\alpha \neq \beta$ then $\wp_\alpha(F) \neq \wp_\beta(F)$, hence any $\mathbb{F}_2$-hyperplane of F coincides with $\wp_\alpha(F)$ for some $0 \neq \alpha \in F$.*

Proof. We may assume that $\alpha\beta \neq 0$. By way of contradiction let $\wp_\alpha(F) = \wp_\beta(F)$, then $\frac{\alpha^2}{\beta^2}\wp(F) = \wp(F)$, that is, setting $\lambda = \frac{\alpha}{\beta}$,

$$x^2 + x = \lambda^2(a^2 + a) \tag{2}$$

always admits a solution for any a. Setting $y = x + \lambda a$, this reduces to $y^2 + y + (\lambda^2 + \lambda)a = 0$ being always soluble in y. Since $\lambda \notin \mathbb{F}_2$, then $\lambda^2 + \lambda \neq 0$ and $(\lambda^2 + \lambda)F = F \nsupseteq \wp(F)$, there exists $a \in F$ such that $\wp(\lambda)a \notin \wp(F)$ and (2) is not soluble. □

Example 29. The same f of Example 26, but $Q(e_1) = \beta \neq 0$, then $Q(e_2 + ae_1) = Q(e_2) + \alpha a + \beta a^2$. Therefore we may assume that $Q(e_2)$ lies in $\frac{\alpha^2}{\beta}T$.

Definition 30. We say that (u, v) is a *reduced non-singular* pair, if (u, v) is an f-generalized hyperbolic pair, $u < v$, and $Q(v) \in \frac{\alpha^2}{\beta}T$, where $Q(u) = \beta \neq 0 \neq \alpha = f(u, v)$, T a fixed transversal for $\wp(F)$ in F.

We switch to four-dimensional non-degenerate spaces.

Example 31. Assume $f = \alpha_1(e_{14} + e_{41}) + \alpha_2(e_{23} + e_{32})$, then k fixing e_1, e_3 and sending e_2 to $e_2 + ae_1$and e_4 to $e_4 + \rho a e_3$, $\rho = \frac{\alpha_1}{\alpha_2}$ is an f-isometry. If $Q(e_1) \neq 0$, there exists $k \in C_K(f)$ satisfying $Q(e_2^k) = 0$.

Example 32. Assume $f = \alpha_1(e_{13} + e_{31}) + \alpha_2(e_{24} + e_{42})$, then $C_K(f) = \begin{pmatrix} 1 & 0 \\ A & 1 \end{pmatrix}$, $A = \begin{pmatrix} a & b \\ \rho b & \rho c \end{pmatrix}$, where $\rho = \frac{\alpha_2}{\alpha_1}$. If both $Q(e_1)Q(e_2) \neq 0$, then we may reduce one out of $\{Q(e_3), Q(e_4)\}$ to zero. Using the Arf's invariant $\mathrm{Arf}(Q) \in F/\wp(F)$ (see [8]) we see that the other term is determined since $\frac{Q(e_1)Q(e_3)}{f(e_1,e_3)^2} + \frac{Q(e_2)Q(e_4)}{f(e_2,e_4)^2} \bmod \wp(F)$ is $C_K(f)$-invariant.

Remark that if $\{v_i\}$ is a standard symplectic basis, that is, $f(v_i, v_j) = \delta_{i,i^\sigma}$ for a fixed-point-free involution σ (usually $\sigma : i \mapsto i + n$ in $\mathbb{Z}_{2n}$), then $\sum Q(v_i)Q(v_{i^\sigma}) \bmod \wp(F)$ is $C(f)$-invariant. If f has standard shape with respect to $\{e_i : i \in [2n]\}$, then $v_i = \frac{e_i}{f(e_i, e_{i^\sigma})}$, for $i \in \Delta(\sigma)$, $v_j = e_j$ otherwise, defines a standard symplectic basis, thus $\sum_{i\in\Delta(\sigma)} Q(v_i)Q(v_{i^\sigma}) = \sum_{i\in\Delta(\sigma)} \frac{Q(e_i)Q(e_{i^\sigma})}{f(e_i,e_{i^\sigma})^2} \bmod \wp(F)$ is $C_K(f)$-invariant. We would like to build a graph associated to Q. Assume that with respect to $(e_i)_{i=1}^{2n}$, $f = \mathrm{Pol}(Q)$ has standard shape and let $\sigma = \sigma(f)$. We say that (ii^σ) *braids* (jj^σ) if $i < j < i^\sigma < j^\sigma$ and $Q(e_i)Q(e_j) \neq 0$. Let B be the symmetric and transitive closure of the braid relation.

Definition 33. We define the *braid graph* associated to Q, $B(Q)$, the graph whose vertices $V(B)$ are the cycles (ii^σ) and whose edges $E(B)$ are (v, w), where vBw, $v \neq w$.

Definition 34. Given a subgraph Γ of $B(Q)$, let $f = \mathrm{Pol}(Q)$, $\sigma = \sigma(f)$; we define $\Delta(\Gamma)$ as $\{i \in \Delta(\sigma) : (ii^\sigma) \in V(\Gamma)\}$.

Proposition 35. *Let $Q \in \mathcal{Q}(V)$ and assume that $f = \mathrm{Pol}(Q)$ has standard shape with respect to $\{e_i\}$ and is non-degenerate. Denote with σ the fixed-point-free involution associated to f and with $\Delta(\sigma)$ its set of ancestors. Let B^0 be a connected component of the braid graph $B(Q)$. Fix $l \in \Delta(B^0)$. Then there exists $k \in C_K(f)$ such that $Q(e_{i^\sigma}) = 0$ for all $i \in \Delta(B^0)\setminus\{l\}$ and $e_i^k = e_i$, for $i \in \Delta(B^0)$. Moreover $Q(e_{l^\sigma})$ is determined as the unique element in $\frac{f(e_l, e_{l^\sigma})^2}{Q(e_l)}T$ such that $\sum_{i\in\Delta(B^0)} \frac{Q(e_i)Q(e_{i^\sigma})}{f(e_i, e_{i^\sigma})^2} \equiv \frac{Q(e_l)Q(e_{l^\sigma}^k)}{f(e_l, e_{l^\sigma})^2} \bmod \wp(F)$.*

Proof. We proceed by induction on $|B^0|$. Call $\widetilde{B}$ the subgraph of B^0 obtained striking out (ll^σ) and all edges adjacent to it, then $\widetilde{B} = \bigcup_i B_i$, B_i the connected components of $\widetilde{B}$. Choose $l_i \in \Delta(B_i)$ such that $(l_i l_i^\sigma)B(ll^\sigma)$. By induction we may assume that $\exists k_i \in C_{K_i}(f_{W_i})$, where $W_i = \langle e_j, e_{j^\sigma} : j \in \Delta(B_i)\rangle$ and $K_i = N_K(W_i)$, such that $e_j^{k_i} = e_j$, $j \in \Delta(B_i)$ and $Q(e_j^{k_i}) = 0$ for $j \in (\Delta(B_i)\setminus\{l_i\})^\sigma$. Remark that f_{W_i} is non-degenerate and u_i may be extended to all of V letting it act trivially on $W_i^\perp$. By Example 32 there exists $x_i \in C_K(f_{U_i})$, where $U_i = \langle e_{l_i}, e_{l_i^\sigma}, e_l, e_{l^\sigma}\rangle$ fixing e_{l_i} and e_l and sending $Q(e_{l_i^\sigma})$ to zero. Clearly $\prod_i k_i x_i$ is the desired transformation. Moreover since $\mathrm{Arf}(Q)$ is K-invariant we also get the last part of the assertion. □

According to the preceding examples and propositions we state some reduction principles. Assume we are given an ordered basis $\{e_i\}$ for V and $Q \in \mathcal{Q}(V)$:

(Q1) $f = \mathrm{Pol}(Q)$ has standard shape with respect to $\{e_i\}$;
(Q2) if $e_i \in \mathrm{Rad}(f)$, $Q(e_i) \neq 0$, then $Q(e_j) = 0, \forall j > i$;
(Q3) if $Q(e_i) = 0$, $i \in \Delta(\sigma)$, then $Q(e_{i^\sigma}) = 0$;
(Q4) if $Q(e_i) \neq 0$, $i \in \Delta(\sigma)$, then $Q(e_{i^\sigma}) \in T_{\frac{f(e_i, e_{i^\sigma})}{\sqrt{Q(e_i)}}}$;
(Q5) if $i < j < j^\sigma < i^\sigma$, $Q(e_i) \neq 0$, then $Q(e_j) = Q(e_{j^\sigma}) = 0$;
(Q6) if B^0 is a connected component of $B(Q)$, $l^\sigma = \max \Delta(B^0)^\sigma$, then $Q(e_j) = 0$, for $j \in (\Delta(B^0)\setminus\{l\})^\sigma$ and $Q(e_{l^\sigma}) \in T_{\frac{f(e_l, e_{l^\sigma})}{\sqrt{Q(e_l)}}}$.

Definition 36. We say that Q has standard shape with respect to $\{e_i\}$ if (Q1)–(Q6) are satisfied or, equivalently, that $\{e_i\}$ is a *Q-nice* basis.

In general if $\{e_i : i \in [n]\}$ is Q-nice, it is not true that $\{e_i : i \in J \subseteq [n]\}$ remains nice for the restriction of Q.

Example 37. Take f such that $\sigma(f) = (13)(24)$, e_1, e_2 non-singular, then $\{e_1, e_2\}$ is not Q-nice.

We show though that somehow nicety is inherited by suitable subsets of $[n]$.

Lemma 38. *Assume that* $\{e_i\}$ *is* Q*-nice,* $f = \mathrm{Pol}(Q), \sigma = \sigma(f)$, *then* $\{e_i : j \neq i, i^\sigma\}$ *is* Q_W*-nice,* $W = \langle e_j : j \neq i, i^\sigma \rangle$.

Proof. Clearly (Q1)–(Q5) hold. Any connected component of the braid graph of Q_W is a subgraph of $B(Q)$, so (Q6) holds, too. □

Theorem 39. *Given* (V, Q, b), $K = C(b)$, *there exists* $k \in K$ *such that* b^k *is* Q*-nice*.

Proof. Theorem 11 assures that (Q1) holds. Example 25, 26, 29, and 31 take care of (Q2), (Q3), (Q4), and (Q5), respectively. Example 32 and Proposition 35 prove (Q6). □

We prove that Q^K contains a unique element in standard shape.

Theorem 40. *If* $b = \{e_i\}$, $b^k = \{e_i^k\}$ *are* Q*-nice bases,* $k \in K$, *then* k *is a* Q*-isometry*.

Proof. We proceed by induction on $\dim(V)$. By (Q1), $f = \mathrm{Pol}(Q)$ has standard shape with respect to both bases and, by Theorem 12, k is an f-isometry. Define $S(Q) = \{v \in \mathrm{Rad}(f) : Q(v) = 0\}$, the *singular radical* of Q. We first prove that we may reduce to the non-degenerate case ($\mathrm{Rad}(f) = 0$).

(R1) $S(Q) = 0$: since f has standard shape with respect to b, $\mathrm{Rad}(f) = \langle u : u = u^\sigma \rangle$. Let v be the first vector in $b \cap \mathrm{Rad}(f)$, then $k \in C_K(f)$ implies that $v^k = v$. If $Q(v) = 0$, we may define $\overline{Q}$ on $\overline{V} = \frac{V}{\langle v \rangle}$ as $\overline{Q}(\overline{u}) := Q(u)$ and k induces $\overline{k} : \overline{V} \to \overline{V}$, $\overline{k} : \overline{u} \mapsto \overline{u^k}$. Now $\overline{b}$ and $\overline{b}^{\overline{k}}$ are $\overline{Q}$-nice bases, so $\overline{k}$ is a $\overline{Q}$-isometry and k is a Q-isometry. If v is not singular and $\mathrm{Rad}(f) = \langle v \rangle$ we are done, otherwise $\dim(\mathrm{Rad}(f)) \geqslant 2$. Let w be the second vector in $b \cap \mathrm{Rad}(f)$. By (Q2) w, w^k are Q-singular. Since $\mathrm{Rad}(f)$ is k-invariant $w^k = w + \lambda v$, then $0 = Q(w^k) = \lambda^2 Q(v)$. So $\lambda = 0$ and w is fixed. Therefore we may argue as before with $\overline{V} = \frac{V}{\langle w \rangle}$.

(R2) $\mathrm{Rad}(f) = 0$: since $S(Q) = 0$, $\dim(\mathrm{Rad}(f)) \leqslant 1 = |F : F^2|$; in fact if v, $w \in \mathrm{Rad}(f)$ were independent and $Q(w) \neq 0$, then $\exists \lambda$ such that $Q(v + \lambda w) = Q(v) + \lambda^2 Q(w) = 0$. Hence $\mathrm{Rad}(f) = \langle v \rangle$ and v is k-invariant. We embed V as

a hyperplane into $\widetilde{V}$ whose basis is $\widetilde{b} = \mathrm{add}(b, z)$, for a new vector z, and extending Q to $\widetilde{Q}$ as follows:

$$\widetilde{f}(u, z) = \begin{cases} 0, & u \neq v \\ 1, & u = v \end{cases}$$

and $\widetilde{Q}(z) = 0$. Call $\widetilde{K}$ the stabilizer of $\widetilde{b}$. By (Q2) $Q(u) = 0$ for any $u > v$, hence $\widetilde{Q}$ satisfies (Q1)–(Q5) with respect to $\widetilde{b}$. We are also done if $j < h(v) < j^\sigma$ and if $k < j < k^\sigma < h(v)$, the validity of (Q6) for $\widetilde{Q}$ follows since this property holds for Q. We are faced with the problem to extend k to $\widetilde{k} \in C_{\widetilde{K}}(\widetilde{f})$ such that $\widetilde{b}^{\widetilde{k}}$ is $\widetilde{Q}$-nice. By Witt's Lemma (see [4, Chapter VII, p. 81]) there exists $\widetilde{k} \in \mathrm{Sp}(\widetilde{V})$ extending k. Set $z^{\widetilde{k}} = \sum \lambda_u u$, then $1 = \widetilde{f}(v^{\widetilde{k}}, z^{\widetilde{k}}) = \lambda_z$, so that $\widetilde{k} \in \widetilde{K}$. Since $z^{\widetilde{k}} - z$ and $u^{\widetilde{k}}$ belong to $\langle v\rangle^\perp$, for $u \neq z$, we see that λ_v may be chosen arbitrarily. This means that $\widetilde{Q}(z^{\widetilde{k}})$ is determined up to an element in $\frac{1}{Q(e_i)}\wp(F)$. Thus, for a suitable $\widetilde{k}$ among all extensions of k, we have $\widetilde{Q}(z^{\widetilde{k}}) \in \frac{1}{Q(e_i)}T$ and $\widetilde{b}^{\widetilde{k}}$ is $\widetilde{Q}$-nice.

If we may prove the theorem when the symplectic form is non-degenerate, then $\widetilde{k}$ would be a $\widetilde{Q}$-isometry and k a Q-isometry. Therefore we assume from now on that $\mathrm{Rad}(f) = 0$ and use induction on $\dim(V)$. We distinguish some cases:

(A) $Q(e_1) = 0$: $\overline{Q}(\overline{v}) := Q(v)$ defines a quadratic form on $\overline{V} = \langle e_1\rangle^\perp/\langle e_1\rangle$. Since $\overline{V}$ is a K-module, $\overline{k} : \overline{e_i} \mapsto \overline{e_i^k}$ is well defined. Now by Lemma 38 $\overline{b}$ and $\overline{b}^{\overline{k}}$ are $\overline{Q}$-nice, then $\overline{k}$ is a $\overline{Q}$-isometry. Since $e_1, e_{1^\sigma}, e_{1^\sigma}^k$ are Q-singular by (Q3), k is a Q-isometry.

(B) $Q(e_1) \neq 0$: there are three subcases

(a) if $1^\sigma = 2 \Rightarrow H = \langle e_1, e_2\rangle$ and $H^\perp$ are K-invariant, thus $k = k_H \perp k_{H^\perp}$. Now $b \cap W$ and $b^k \cap W$, are Q_W-nice, $W \in \{H, H^\perp\}$, so k_W is a Q_W-isometry and k is a Q-isometry;

(b) if $2^\sigma < 1^\sigma \Rightarrow e_2, e_{2^\sigma}, e_2^k, e_{2^\sigma}^k$ are Q-singular by (Q5). Since $Q(e_2^k) = Q(e_2 + \mu e_1)$, we have that $\mu = 0$ and e_2 is k-invariant. As in case (A) with $\overline{V} = \langle e_2\rangle^\perp/\langle e_2\rangle$, $\overline{Q}(\overline{v}) := Q(v)$, $\overline{e_i}^{\overline{k}} = \overline{e_i^k}$, we obtain that $\overline{k}$ is a $\overline{Q}$-isometry and k a Q-isometry;

(c) if $1^\sigma < 2^\sigma \Rightarrow e_2^k = e_2$; in fact $e_2^k = e_2 + \mu e_1$, $e_{1^\sigma}^k = e_{1^\sigma} + v$, $v \in \langle e_1, e_2\rangle^\perp$, then $\mu = f(e_2^k, e_{1^\sigma}^k) = 0$. If $Q(e_2) = 0$ we may proceed as in (b). Otherwise $q_2 = Q(e_2) \neq 0$. Set $q_1 = Q(e_1) \neq 0$, then $Q(e_2 + \mu e_1) = 0$ for $\mu^2 = \frac{q_2}{q_1}$. Let $\alpha_1 = f(e_1, e_{1^\sigma})$ and $\alpha_2 = f(e_2, e_{2^\sigma})$ and $\rho = \frac{\alpha_2}{\mu\alpha_1}$. Define $x \in K$ as follows $e_2^x = e_2 + \mu e_1, e_{2^\sigma}^x = e_{2^\sigma} + \rho e_{1^\sigma}$ and acting as the identity on the other vectors in b. Since $Q(e_2^x) = 0$ we may endow $\overline{V} = \langle e_2^x\rangle^\perp/\langle e_2^x\rangle$ with a quadratic form $\overline{Q}$ in the usual way. Since $\overline{V}$ is k-invariant, it is generated both by $\{\overline{e_i^x} : i \neq 1, 2^\sigma\}$ and $\{\overline{e_i^{xk}} : i \neq 1, 2^\sigma\}$. We would like to prove that these bases are $\overline{Q}$-nice. By symmetry we consider only b. First of all $\overline{V} = \langle \overline{e_i^x} : i = 1, 2^\sigma\rangle \perp \langle \overline{e_i^x} : i \neq 1, 2, 1^\sigma, 2^\sigma\rangle$, so that (Q1) holds. By non-degeneracy (Q2) is voidly true. If

$i \in \Delta(\sigma)\setminus\{1,2\}$, then (Q3) and (Q4) hold for $(\overline{e_i}, \overline{e_{i^\sigma}})$ with respect to $\overline{Q}$. Let $\overline{b} = \overline{\mathrm{cut}(b^x\{e_2^x, e_{1^\sigma}^x\})}$ and $\overline{h}$ the height induced by this basis. Remark that $\overline{\sigma} = \sigma(\overline{f})$ sends $1 = \overline{h}(\overline{e_1})$ to $2^\sigma - 2 = \overline{h}(\overline{e_{2^\sigma}^x})$. Let $\overline{j} = \overline{h}(\overline{e_j^x})$, $j \neq 2, 1^\sigma$. Assume $\overline{i} < \overline{j} < \overline{j^\sigma} < \overline{i}^{\overline{\sigma}}$, $\overline{Q}(\overline{e_i})\overline{Q}(\overline{e_j}) \neq 0$. If $i \neq 1$, pulling back we would contradict (Q5) referred to Q. But the same happens if $i = 1$ since then $2 < j < j^\sigma < 2^\sigma$. Thus (Q5) holds. Finally let B^0 be a connected component of the braid graph $B(Q)$. Fix a suitable $l \in \Delta(B^0)$. Then $Q(e_{i^\sigma}) = 0$ for $i \in \Delta(B^0)\setminus\{l\}$. Therefore $\overline{Q}(\overline{e_{i^\sigma}^x}) = 0$ unless $i = l$ or 2. But $\overline{Q}(\overline{e_{2^\sigma}^x}) = Q(e_{2^\sigma}^x)$ which is zero unless $l = 2$ and (Q6) holds. Now $\overline{k} : \overline{e_i^x} \mapsto \overline{e_i^{xk}}$ is well defined, preserves $\overline{h}$ and $\{\overline{e_i^x}\}$, $\{\overline{e_i^{xk}}\}$ are $\overline{Q}$-nice, so $\overline{k}$ is a $\overline{Q}$-isometry and $Q(e_i^x) = Q(e_i^{xk})$ unless $i = 2, 1^\sigma$. But $e_2 = e_2^k$ and $Q(e_{1^\sigma}) = Q(e_{1^\sigma}^k) = 0$ by (Q6). So k is a Q-isometry. □

Our next attempt is to determine $|C_K(Q)|$, for $Q \in \mathcal{Q}(V)$. As in Section 3 we may assume that Q has standard shape. If we act by an element of the torus the orbit size remains unchanged. If H is a two-dimensional orthogonal summand of V and $f_H = \alpha(e_{12} + e_{21})$, $Q(e_1) = q_1$, $d = \mathrm{diag}(\tau, \varsigma)$, then $f^d = dfd'$ and $Q(e_1^d) = \tau^2 q_1$. For a suitable choice of τ, ς, $\alpha\tau\varsigma = 1$ and $\tau^2 q_1 \in \{0, 1\}$. Remark that $Q(\varsigma e_2) \in T$, so that the new basis is Q^d-nice. If that is the case for any element of a basis b we say that Q has *reduced standard* shape (with respect to b). We need a somewhat technical lemma. Our purpose is to provide recurrence relations counting the number of orbits of K of given size on $\mathcal{Q}(V)$. We will usually try to induce a new quadratic $\overline{Q}$ on a suitable quotient space or subspace of V. In order to do so we look for Q-singular vectors stabilized by $C_K(Q)$.

Lemma 41. *Let (V, Q, b) be a triple where Q has reduced standard shape with respect to b. Assume there exists $x \in K$ such that b^x contains a Q-singular vector stabilized by $C_K(Q)$. Let $v \in b^x$ be the first such vector. Then $\overline{Q}(\overline{u}) := Q(u)$ defines a quadratic form on $\overline{V} = \langle v\rangle^\perp/\langle v\rangle$. Let $\overline{b} = \overline{b^x \cap \langle v\rangle^\perp}$, and $\overline{K} = C(\overline{b})$. Assume further that $h(v) \leqslant 2$, $|b^x \cap \langle v\rangle^\perp| + |b^x\setminus\langle v\rangle^\perp| = n$, $|b^x\setminus\langle v\rangle^\perp| \leqslant 1$, then $\exists \ker\rho \rightarrowtail C_K(Q) \overset{\rho}{\twoheadrightarrow} C_{\overline{K}}(\overline{Q})$. Moreover $|\ker\rho|$ is a power of $|F|$.*

Proof. Since $\overline{V}$ is a $C_K(Q)$-module, there exists $\rho : K \to \mathrm{GL}(\overline{V})$ defined as $\overline{u}^{k^\rho} := \overline{u^k}$. Moreover let h denote the height function induced by the ordering on b, then $h(w^k - w) < h(w)$ implies $\overline{h}(\overline{w}^{k^\rho} - \overline{w}) < \overline{h}(\overline{w})$ for any $w \in b^x \cap \langle v\rangle^\perp$ and $\rho(K) \leqslant \overline{K}$. If $k \in C_K(Q)$, then

$$\overline{Q}(\overline{w}^{k^\rho}) = \overline{Q}(\overline{w^k}) = Q(w^k) = Q(w) = \overline{Q}(\overline{w})$$

and $\rho(C_K(Q)) \leqslant C_{\overline{K}}(\overline{Q})$. The hard part is to prove that ρ is surjective. Choose $\overline{k} \in C_{\overline{K}}(\overline{Q})$ and for any $\overline{u} \in \overline{b}$ let $\overline{u}^{\overline{k}} = \overline{w_u}$ for a fixed $w_u \in \langle v\rangle^\perp$. A candidate extension k for $\overline{k}$ should act on any element u of $b^x \cap \langle v\rangle^\perp$ as follows $u^k = w_u + \mu_u v$. Let $\overline{f} = \mathrm{Pol}(\overline{Q})$. If $u, t \in b^x \cap \langle v\rangle^\perp$, then

$$f(u^k, t^k) = f(w_u, w_t) = \overline{f}(\overline{w_u}, \overline{w_t}) = \overline{f}(\overline{u}^{\overline{k}}, \overline{t}^{\overline{k}}) = \overline{f}(\overline{u}, \overline{t}) = f(u, t)$$

and

$$Q(u^k) = Q(w_u + \mu_u v) = Q(w_u) = \overline{Q}(\overline{u}^{\overline{k}}) = \overline{Q}(\overline{u}) = Q(u).$$

Since $Q(u^k) = Q(u)$ and $f(u, w) = f(u^k, w^k)$, u, w arbitrary vectors of a fixed basis, imply that $k \in C_K(Q)$, we are done if $V = \langle v \rangle^\perp$. Otherwise let z be the unique element in $b^x \setminus \langle v \rangle^\perp$ and write z^k as

$$z + \sum_{u \in b^x}^{h(u)<h(z)} \lambda_u u = z + \lambda_v v + w.$$

Since $z \notin \langle v \rangle^\perp$, we have that $0 \neq f(v, z) = f(v, z^k)$, so

$$f(u^k, z^k) = f(w_u, z^k) + \mu_u f(v, z^k) = f(u, z)$$

is a non-trivial linear equation in μ_u, for any $u \in b^x \cap \langle v \rangle^\perp$. Finally

$$Q(z^k) = Q(z) + \lambda_v f(v, z) + Q(w) + f(z, w) = Q(z)$$

is a non-trivial linear equation in λ_v. We need to check that the putative isometry k we defined really lies in K. If $h(v) = 1$ we are done. If $h(v) = 2$, let t be the first element in b^x. Then we must have $f(t, z^k - z) = 0$. We claim that $f(t, v) = 0$. By contradiction assume $t = z$. By the minimality of v, t is not Q-singular; but then $v \mapsto v + az$, would be an isometry for a suitable $0 \neq a \in F$, against the invariance of v. Therefore $f(t, z^k - z) = 0$ is a linear equation in the λ's not involving λ_v. Finally $|\ker \rho| = |\langle u \in b^x \setminus \{v, z\} : h(u) < h(z)\rangle \cap \langle t \rangle^\perp|$ is an $|F|$-power. □

We successively reduce to the case where the singular radical of Q is zero

Lemma 42. *Assume that Q has reduced standard shape with respect to b, $S(Q)$ its singular radical and v the first vector in $b \cap S(Q)$. Let $\overline{V} = V/\langle v \rangle$ and $\overline{b}$ the ordered basis induced by b on $\overline{V}$, $\overline{K} = C(\overline{b})$. Then $|C_K(Q)|$ equals $|F|^{\dim(V)-h(v)}|C_{\overline{K}}(\overline{Q})|$.*

Proof. We need only to specialize Lemma 41 to our case. So take $x = 1$ and consider that all μ_u's are arbitrary for $u \in b$, $h(u) > h(v)$. □

Keeping the due control on the orbit size and applying Lemma 42, we may assume that $S(Q) = 0$. Thus $\dim(\mathrm{Rad}(f)) \leqslant 1$.

Lemma 43. *Let v be the first vector of $b \cap \mathrm{Rad}(f)$. Set $\overline{V} = V/\langle v \rangle$, $\overline{f}$, $\overline{b}$ as usual, then $C_K(Q) \simeq C_{\overline{K}}(\overline{f})$.*

Proof. In fact any $\overline{f}$-isometry $\overline{k}$ lifts in a unique way to a Q-isometry k defined as $u^k = w_u + \mu_u v$, where $\overline{u}^{\overline{k}} = \overline{w_u}$ and μ_u is uniquely determined by the condition $Q(w_u) + \mu_u^2 Q(v) = Q(u)$. □

Remark that this observation is the kernel in the proof of the isomorphism of orthogonal groups in odd dimension and symplectic ones in dimension one less (see [7, Chapter 1]). Now we are reduced to the non-degenerate case.

Lemma 44. *Assume that Q has reduced standard shape with respect to $b = \{e_i\}$, $S(Q) = 0$ and $e_1 \notin \mathrm{Rad}(f)$. Then there exist $\overline{V}$ a $C_K(Q)$-module, $\overline{b}$ $\overline{Q}$-nice, and an exact sequence*

$$\ker \rho \rightarrowtail C_K(Q) \twoheadrightarrow C_{\overline{K}}(\overline{Q}).$$

Moreover, $|\ker \rho| = 2$ or a power of $|F|$ depending on $\sigma(f)$, $f = \mathrm{Pol}(Q)$.

Proof. We apply and cling to the notation in Lemma 41. Let $W = \langle u \in b^x : v \neq u < z\rangle$, where v is Q-singular and $C_K(Q)$-invariant and $f(v, z) \neq 0$, $v, z \in b^x$.

(A) $Q(e_1) = 0$: take $x = 1$, $v = e_1$, $z = e_{1^\sigma}$ in Lemma 41, then all μ's are determined by $z^k = z + \lambda_v v + w$ and $\lambda_v = Q(w)$, where $w \in W$, so $\dim(\ker \rho) = h(z) - 2$.

From now on suppose that $Q(e_1) = 1$.

(B) $2 = 1^\sigma$: then $\overline{V} = \langle u \in b : u > e_2\rangle$ is a $C_K(Q)$-module. Let ρ be the restriction map on $\overline{V}$, then ρ is onto and $|\ker \rho| = 2$.

From now on $2 < 1^\sigma$. Since $Q(e_2 + ae_1) = Q(e_2) + a^2$, e_2 is $C_K(Q)$-stable.

(C) $e_2 \in \mathrm{Rad}(f)$: by assumption $Q(e_2) = 1$. Let x fix all basis vectors but e_2, where $e_2^x = e_2 + e_1$. Apply Lemma 41 with $v = e_2 + e_1$, x as above, $z = e_{1^\sigma}$. All μ_u's are determined by $z^k = z + \lambda_v v + w$, $w \in W$. Since $W \leqslant \langle e_1\rangle^\perp$, $\dim(\ker \rho) = h(z) - 2$. Remark that $\mathrm{Rad}(\overline{f})$ is generated by $\overline{e}_1$ and we are in the situation of Lemma 43.

(D) $1^\sigma > 2^\sigma > 2$: by assumption of Q-nicety of b, e_2 is Q-singular. Take $x = 1$, $v = e_2$, and $z = e_{2^\sigma}$ in Lemma 41, then all μ's are determined by $z^k = z + \lambda_v v + w$, $w \in W$ and $\lambda_v = Q(w)$. Since $W \leqslant \langle e_1\rangle^\perp$, $\dim(\ker \rho) = h(z) - 2$.

(E) $1^\sigma < 2^\sigma$ and $Q(e_2) = 0$: take $x = 1$, $v = e_2$, and $z = e_{2^\sigma}$ in Lemma 41, then all μ's are determined by $z^k = z + \lambda_v v + w$, where $\lambda_v = Q(w)$, $w \in W$. This time $W \not\leqslant \langle e_1\rangle^\perp$, so $\dim(\ker \rho) = h(z) - 3$.

(F) $1^\sigma < 2^\sigma$ and $Q(e_2) = 1$: then $v = e_2 + e_1$ is Q-singular and orthogonal to $e_{2^\sigma} + e_{1^\sigma}$. Thus define x via $e_2^x = v$, $e_{2^\sigma}^x = e_{2^\sigma} + e_{1^\sigma}$, $e_i^x = e_i$ if $i \neq 2, 2^\sigma$. We may apply Lemma 41 with $z = e_{1^\sigma}$. Then $W \leqslant \langle t\rangle^\perp$, so $\dim(\ker \rho) = h(z) - 2$.

The $\overline{Q}$-nicety of $\overline{b}$ follows applying Lemma 38 unless $x \neq 1$. In case C) it is easy to check that $\overline{Q}$ satisfies $Q1$) with respect to $\overline{b}$ and because $Q2$) holds for Q all vectors in $\overline{b}$ are $\overline{Q}$-singular, so $\overline{b}$ is $\overline{Q}$-nice. In case F) we may argue as in Theorem 40.B.c. □

We use the preceding lemmas to obtain global and detailed information on orbit sizes and their multiplicities under unitriangular action on quadratic forms.

Definition 45. Let $F = \mathbb{F}_q$, $q = 2^r$. We denote with $q_n(q,t)$ the *orbit size* polynomial, namely the generating function associated to $\{c_j\}$, where c_j is the number of orbits of K on $\mathcal{Q}(F^n)$ of size 2^j. For $2 \leqslant i \leqslant n$, $q_{n,i}(q,t)$ denotes the generating function associated to the number of orbits according to size of quadratic forms Q such that $Q(e_1) \neq 0$ and $1^\sigma = i$ (notice that i is well defined even if Q is not in standard shape).

Since we are more interested on how far orbit sizes are from being q-powers, we encode orbits of size $q^m/2^s$ via $t^m u^s$, where t, u are considered as two independent variables. The corresponding orbit size over $\mathbb{F}_{2^r}$ will then be obtained evaluating t to 2^r and u to $1/2$.

Theorem 46. *Let $p_n(w,t,u)$, $p_{ni}(w,t,u)$, $n \in \mathbb{N}$, $2 \leqslant i \leqslant n$, be the polynomials uniquely determined by the following recurrence relations and initial conditions, where $a_n(w,t)$ are the orbit size polynomials in case* **A**:

(a) $p_0 = 1$, $p_1 = w + 1$;
(b) *for* $n \geqslant 2$,

$$p_n = p_{n-1} + wt^{n-1}\left(a_{n-1} + \frac{t^{n-1}-1}{t-1}p_{n-2}\right) + \sum_{i=2}^{n} p_{ni};$$

(c) $p_{n2} = 2uw^2t^{2n-3}p_{n-2}$;
(d) *for* $3 \leqslant i \leqslant n$,

$$p_{ni} = tp_{n-1,i-1} + w^3t^{3n-4-i}a_{n-3} + wt^{2n-i}\frac{t^{i-3}-1}{t-1}p_{n-2,i-2} + wt^n\frac{t^{n-i}-1}{t-1}p_{n-2,i-1} + w^2t^{2n-1-i}\sum_{j=i+1}^{n} p_{n-2,j-2}.$$

Then p_n and p_{ni} are non-zero polynomials in $\mathbb{N}[w,t,u]$. Moreover, $q_n(q,t)$ and $q_{ni}(q,t)$ equal $p_n(q-1,t^r,t^{-1})$ and $p_{ni}(q-1,t^r,t^{-1})$.

Proof. The claim about uniqueness follows immediately. Notice that we do not need to assume $p_{ni} = 0$ if $i \leqslant 1$ or $i > n$, since in the recursive description for p_{n3} the term $p_{n-2,1}$ is multiplied by 0. Now we justify the second and third claim applying Lemmas 41–44. As we said the three variables w, t, and u must be considered as follows: $w = q - 1$, $q = |F|$; $t^m u^s$ denotes the occurrence of an orbit of size $q^m/2^s$. Clearly $p_1 = q$, and $p_0 = 1$ is obtained using backwards the recurrence relation (b) on p_2. Assume now that $n \geqslant 2$. Given a triple (V, Q, b), where $|b| = n$ and Q has (reduced) standard shape, we will analyze different cases according to some conditions on e_1 and e_2.

(A) $e_1 \in S(Q)$: set $\overline{V} = V/\langle e_1\rangle$ and $\overline{Q}(\overline{u}) = Q(u)$, then $|Q^K| = |\overline{Q}^{\overline{K}}|$; we have a contribution of p_{n-1}.

(B) $Q(e_1) = 1$, $e_1 \in \mathrm{Rad}(f)$: again $\overline{V} = V/\langle e_1\rangle$. By Lemma 43 $|Q^K| = |\overline{f}^{\overline{K}}|$. Since $\overline{f}$ is an alternating form on $\overline{V}$, and $Q(e_1)$ may assume $w = |F^*|$ values, we get a contribution of $wt^{n-1}a_{n-1}$.

From now on we assume that $e_1 \notin \mathrm{Rad}(f)$ and set $i = 1^\sigma$ the position of the only vector in $b \setminus \langle e_1\rangle^\perp$.

(C) $Q(e_1) = 0$: on $\overline{V} = \langle e_1\rangle^\perp/\langle e_1\rangle$ we define $\overline{Q}(\overline{u}) = Q(u)$. Then $|Q^K| = q^{2n-1-i}|\overline{Q}^{\overline{K}}|$, since $|K| = q^{2n-3}|\overline{K}|$ and $|\ker\rho| = q^{i-2}$ according to Lemma 44.A. Since $2 \leqslant i \leqslant n$, $\overline{Q}$ is any quadratic form on $\overline{V}$, and $f(e_1, e_i)$ may assume w values, we get a contribution of $wt^{n-1}\frac{t^{n-1}-1}{t-1}p_{n-2}$.

From now on $Q(e_1) = 1$, so wet get a final contribution to p_n of $\sum_{i=2}^{n} p_{ni}$, thus proving equation (b).

(D) $1^\sigma = 2$: $\overline{V} = \langle e_1, e_2\rangle^\perp$, $\overline{Q} = Q_{\overline{V}}$, $|Q^K| = \frac{q^{2n-3}}{2}|\overline{Q}^{\overline{K}}|$. Since $Q(e_1)$ and $f(e_1, e_2)$ may be chosen in w^2 ways and $Q(e_2)$ in two ways by Q4), we get $p_{n2} = 2w^2ut^{2n-3}p_{n-2}$, hence (c) holds.

From now on we further assume $n \geqslant i \geqslant 3$.

(E) $e_2 \in S(Q)$: set $\overline{V} = V/\langle e_2\rangle$ and $\overline{Q}(\overline{u}) = Q(u)$. By Lemma 43, $|Q^K| = q|\overline{Q}^{\overline{K}}|$. Since $1^{\overline{\sigma}} = i - 1$ we have a contribution of $tp_{n-1,i-1}$.

(F) $Q(e_2) = 1$, $e_2 \in \mathrm{Rad}(f)$: set $v = e_2 + e_1$, then $Q(v) = 0$ and v is $C_K(Q)$-stable. Let $e_2^x = v$ and $e_j^x = e_j$, $j \neq 2$, $\overline{V} = \langle v\rangle^\perp/\langle v\rangle$, $z = e_{1^\sigma}$. By Lemma 44.C, $|Q^K| = q^{2n-1-i}|\overline{Q}^{\overline{K}}|$. Since $\overline{e}_1 \in \mathrm{Rad}(\overline{f})$ we are back to step B) in dimension $n - 2$. By Lemma 43, $|\overline{Q}^{\overline{K}}| = q^{n-3}|\overline{\overline{f}}^{\overline{\overline{K}}}|$, where $\overline{\overline{f}}$ is an alternating form in dimension $n - 3$. Since $Q(e_1)$, $Q(e_2)$, and $f(e_1, e_2)$ may be chosen in w^3 ways, we get a contribution of $w^3t^{3n-4-i}a_{n-3}$.

(G) $1 < 2 < 2^\sigma < 1^\sigma$: by (Q5) $Q(e_2) = 0$ and e_2 is $C_K(Q)$-stable. So set $v = e_2$, $z = e_{2^\sigma}$, $x = 1_K$, $\overline{V} = \langle v\rangle^\perp/\langle v\rangle$. By Lemma 44.D $|Q^K| = q^{2n-1-j}|\overline{Q}^{\overline{K}}|$, where $j = 2^\sigma$. Since $f(e_2, e_{2^\sigma})$ may assume w values, $1^{\overline{\sigma}} = i - 2$, and $3 \leqslant j \leqslant i - 1$, we get the term $wt^{2n-i}\frac{t^{i-3}-1}{t-1}p_{n-2,i-2}$.

(H) $1 < 2 < 1^\sigma < 2^\sigma$, $Q(e_2) = 0$: with the same notation as in case G), we get $|Q^K| = q^{2n-j}|\overline{Q}^{\overline{K}}|$ by Lemma 44.E. Since $f(e_2, e_{2^\sigma})$ may assume w values and $1^{\overline{\sigma}} = i - 1$, we get the term $wt^n\frac{t^{n-i}-1}{t-1}p_{n-2,i-1}$.

(I) $1 < 2 < 1^\sigma < 2^\sigma$, $Q(e_2) = 1$: $v = e_2 + e_1$ is Q-singular and $C_K(Q)$-stable. In order to apply Lemma 41, we need to modify e_{2^σ} into $e_{2^\sigma} + e_{1^\sigma}$. If $e_2^x = e_2 + e_1$, $e_{2^\sigma}^x = e_{2^\sigma} + e_{1^\sigma}$, and $e_i^x = e_i$, otherwise, then $b^x \setminus \langle v\rangle^\perp = \{z\}$, where $z = e_{1^\sigma}$. Set $\overline{V} = \langle v\rangle^\perp/\langle v\rangle$. By Lemma 44.F $|Q^K| = q^{2n-1-i}|\overline{Q}^{\overline{K}}|$. Since $\langle e_1, e_{1^\sigma}\rangle$ has been replaced by $\langle \overline{e}_1, \overline{e}_{2^\sigma} + \overline{e}_{1^\sigma}\rangle$, then $1^{\overline{\sigma}} = j - 2$. We need to sum for j from $i + 1$ to n.

Since $f(e_2, e_{2^\sigma})$ and $Q(e_2)$ may assume w values each, we get a final contribution of $w^2 t^{2n-1-i} \sum_{j=i+1}^{n} p_{n-2,j-2}$ and (d) follows.

The claim p_n, $p_{ni} \in \mathbb{N}[w, t, u]$ follows easily from the recurrence equations. □

As shown by Isaacs [12], a Sylow 2-subgroup U of $\mathrm{Sp}(2n, F)$ possesses an irreducible character of degree $\frac{|F|}{2}$, when $n = 1$. We extend this result reminding that $U = A \rtimes K_0$, A is isomorphic to the set of symmetric matrices on V, K_0 is isomorphic to the lower unitriangular group K of dimension n over F, and $\mathrm{Irr}(A)$ is K-equivalent to $\mathcal{Q}(V)$. Any $\zeta \in \mathrm{Irr}(A)$ extends to its inertia subgroup I in U. Call ζ_0 such extension, then $\zeta_0^U \in \mathrm{Irr}(U)$ and $\zeta_0^U(1) = |\zeta_0^K| \in \mathrm{cd}(U)$. In particular $s(\mathcal{Q}(V), K) \subseteq \mathrm{cd}(U)$. We now apply Theorem 46 and prove that $\deg_u p_n$ equals $m = \lfloor \frac{n}{2} \rfloor$ and that all monomial $t^k u^j$ occur whenever $0 \leqslant j \leqslant m$ and $\binom{2j}{2} \leqslant k \leqslant \binom{n}{2}$. This refines Theorem 1.8 in [9], where such a result was proved only when $k = \binom{n}{2}$. In particular this implies that

$$s(\mathrm{Irr}(A), K) = \left\{ \frac{q^k}{2^j} \mid 0 \leqslant j \leqslant m, \binom{2j}{2} \leqslant k \leqslant \binom{n}{2} \right\}.$$

Definition 47. Given a polynomial $s(t) = \sum_k s_k t^k \in R[t]$ over some ring R, we define the support, $\mathrm{Supp}(s)$, as the set of all integers k such that $s_k \neq 0$.

Theorem 48. *Let $p_n(w, t, u) = \sum_j s_{nj}(w, t) u^j$ and $m = \lfloor \frac{n}{2} \rfloor$. Then $s_{nj} \neq 0$ for $0 \leqslant j \leqslant m$. More precisely* $\mathrm{Supp}(s_{nj}(w, t)) = \left\{ \binom{2j}{2}, \ldots, \binom{n}{2} \right\}$ *with respect to t. In particular* $s(\mathcal{Q}(\mathbb{F}_q^n), K) = \left\{ \frac{q^k}{2^j} \mid 0 \leqslant j \leqslant m, \binom{2j}{2} \leqslant k \leqslant \binom{n}{2} \right\}$.

Proof. We first introduce explicitly the coefficients of u^j in p_{ni}, namely $p_{ni} = \sum_j s_{nij}(w, t) u^j$. By the recurrence relations in Theorem 46, we see that w occurs only in step c). Using induction on n we immediately deduce that $\deg_u p_n = m$. Moreover, s_{nj} equals

$$\begin{aligned} & s_{n-1,j} + \delta_{j0} w t^{n-1} a_{n-1} + w t^{n-1} \frac{t^{n-1} - 1}{t - 1} s_{n-2,j} + 2 w^2 t^{2n-3} s_{n-2,j-1} \\ & \quad + \sum_{i=3}^{n} \left(t s_{n-1,i-1,j} + \delta_{j0} w^3 t^{3n-4-i} a_{n-3} + w t^{2n-i} \frac{t^{i-3} - 1}{t - 1} s_{n-2,i-2,j} \right. \\ & \quad \left. + w t^n \frac{t^{n-i} - 1}{t - 1} s_{n-2,i-1,j} + w^2 t^{2n-1-i} \sum_{k=i+1}^{n} s_{n-2,k-2,j} \right), \end{aligned} \tag{3}$$

where δ denotes the *Kronecker delta* and we set $s_{nj} = s_{nij} = 0$ if $j < 0$ or $j > m$. By induction we may assume that $\deg_t s_{lj} = \binom{l}{2}$, $l < n$. It follows that $\deg_t s_{lij} \leqslant \binom{l}{2}$. By Eq. (3), we get that $t^{\binom{n}{2}}$ occurs in $w t^{n-1} \frac{t^{n-1}-1}{t-1} s_{n-2,j} + 2 w^2 t^{2n-3} s_{n-2,j-1}$. Since

there is no cancellation ($s_{lj} \in \mathbb{N}[w,t]$) and the degree in t of the other terms is smaller, we obtain $\deg_t s_{nj} = \binom{n}{2}$. Let d_j denote the highest power of t dividing $s_{nj}(w,t)$, $t^{d_j} \| s_{nj}$. We claim that $d_j = \binom{2j}{2}$. In particular, it is independent from n (as long as $0 \leqslant j \leqslant m$). Again the lack of cancellation forces $t^{d_j} \| s_{lij}$. Clearly the claim holds for $j = 0$ using induction and considering the term $s_{n-1,0}$. Assume $j > 0$. Applying induction on n, we see that t^{d_j} occurs only in $s_{n-1,j}$ and $2w^2t^{2n-3}s_{n-2,j-1}$, the latter contributing only when $n = 2m$ and $j = m$. Since there is no cancellation, it follows that $t^{d_j} \| s_{nj}$. Finally assume by induction that $\mathrm{Supp}(s_{lj}) = \left\{\binom{2j}{2}, \ldots, \binom{l}{2}\right\}$, for $l < n$. We first exhibit s_{nj} for $n = 2, 3, 4$ obtained applying the recurrence relations in Theorem 46. We actually implemented some code in `Magma` (see [5]) available at the author web site in order to get in principle any p_n. The results are as follows

$$p_2 = 2w^2tu + 2wt + w + 1,$$

$$s_{3,1} = 2w^2(w+1)t^3 + 2w^2t^2 + 2w^2t,$$

$$s_{3,0} = w(w+1)t^3 + w(w^2+2w+2)t^2 + 2wt + w + 1,$$

$$s_{4,2} = 4w^4t^6,$$

$$s_{4,1} = 6w^3t^6 + 2w^2(w^2+4w+1)t^5 + 2w^2(2w+1)t^4 + 2w^3(1+2w)t^3 + 2w^2t^2 + 2w^2t,$$

and

$$s_{4,0} = 2w^2t^6 + w(w^2+4w+1)t^5 + w(w^2+4w+1)t^4 + w(w^2+3w+3)t^3 + w(w+1)^2t^2 + 2wt + w + 1.$$

Given $S \subseteq \mathbb{N}$, we denote $a + S = \{a + s : s \in S\}$. Assume $j = 0$, then

$$\mathrm{Supp}(s_{nj}) \supseteq \mathrm{Supp}(s_{n-1,j}) \cup (2n-3) + \mathrm{Supp}(s_{n-2,j}).$$

So we are done unless $2n - 3 - \binom{n-1}{2} \geqslant 2$; this happens only if $n = 3, 4$, where the above union misses the term $\binom{n-1}{2} + 1$. It nonetheless occurs as we can see from the explicit information reported above.

Assume $n = 2m$ and $j = m$, then

$$\mathrm{Supp}(s_{nm}) \supseteq (2n-3) + \mathrm{Supp}(s_{n-2,m-1}) = \left\{\binom{n}{2}\right\}$$

and we are done.

So we may assume that $\frac{n-1}{2} \geqslant j \geqslant 1$. Here

$$\mathrm{Supp}(s_{nj}) \supseteq \mathrm{Supp}(s_{n-1,j}) \cup (2n-3) + \mathrm{Supp}(s_{n-2,j-1}).$$

Therefore the claim follows unless $\binom{2j-2}{2} + 2n - 3 \geqslant \binom{n-1}{2} + 2$ iff $2j \geqslant n - 1$ or $2j \leqslant 6 - n$. The second case forces $n \leqslant 4$. Thus $n = 2m + 1$ and $j = m$. We provide a more detailed information here. Using Eq. (3) we get that $s_{2m,m} =$

$2w^2t^{4m-3}s_{n-2,m-1}$: By induction $s_{2m,m} = 2^m w^{2m} t^{\binom{2m}{2}}$. More precisely $s_{2m,m} = s_{2m,2,m}$ and $s_{2m,i,m} = 0$ if $i > 2$. We claim that

$$s_{2m+1,m} = 2^m w^{2m} \left((w+1)t^{\binom{2m+1}{2}} + \sum_{j=\binom{2m}{2}}^{\binom{2m+1}{2}-1} t^j \right).$$

This holds for $m = 0$. By Eq. (3)

$$s_{2m+1,m} = s_{2m,m} + 2w^2 t^{4m-1} s_{2m-1,m-1} + \sum_{i=3}^{2m+1} t s_{2m,i-1,m}.$$

By the previous remark the latter sum reduces only to the term $ts_{2m,2,m}$. Applying the inductive hypothesis the result follows. □

Corollary 49. *Let $\mathcal{Q}(\mathbb{F}_q^n)$, q even, $m = \lfloor \frac{n}{2} \rfloor$. Then the number of orbits of $K_n(q)$ of size $q^{\binom{n}{2}}$ equals $2(q-1)^m$ if $n = 2m$ and $q(q-1)^m$ if $n = 2m+1$. On the other extreme the number of orbits of size $2^{-m}q^{\binom{n}{2}}$ equals $2^m(q-1)^n$, if $n = 2m$, $2^m q(q-1)^m$ if $n = 2m+1$.*

Proof. The proof of the second fact is already given in the previous proof, while the first claim may be obtained by an easy induction. □

As we already pointed out this provides information on character degrees, namely

Corollary 50. *Let $U \in \mathrm{Syl}_2(\mathrm{Sp}(2n, q))$, q even. Then*

$$\mathrm{cd}(U) \supseteq \left\{ \frac{q^k}{2^j} : 0 \leqslant j \leqslant m, \binom{2j}{2} \leqslant k \leqslant \binom{n}{2} \right\}.$$

It might be interesting to investigate whether the above inclusion is really an equality. Notice that by Itô's Theorem $\chi(1) \leqslant q^{\binom{n}{2}}$, for any $\chi \in \mathrm{Irr}(U)$. To answer such a question one needs to control $\mathrm{cd}(C)$, where $C = C_K(Q)$, $Q \in \mathcal{Q}(\mathbb{F}_q^n)$ (see [9]).

5. Unitary groups

In [18] we proved that any irreducible character of a Sylow p-subgroup U of $\mathrm{PSU}(2n, q^2)$, q a p-power, p odd, is a q-power. We show, using a result in [17], that the same holds when $p = 2$. According to Isaacs, we call such groups q-power-degree groups. In [12,18] it was proved that U is a q-power-degree group, whenever U is a Sylow p-subgroup of a classical group G whose natural module M is even

dimensional and p is the natural characteristic. The determination of $\mathrm{cd}(U)$ when G is the general linear, symplectic or orthogonal group was accomplished in [10], [19], and [14], respectively. We close up the gap and find $\mathrm{cd}(U)$ in the unitary case. For reasons which will become clear later we analyze some conditions under which non-degeneracy of sesquilinear forms is preserved restricting to suitable subspaces. Let $\Gamma\mathrm{L}(V)$ be the group of semilinear maps on V. Choose $\tau \in \Gamma\mathrm{L}(V)$ and call $\psi = \psi(\tau)$ the associated automorphism, that is, $(\lambda v)^\tau = \lambda^\psi v^\tau$, $\psi \in \mathrm{Aut}(F)$, $\lambda \in F$, $v \in V$. We are interested in the case $\tau^2 = 1$, then $\psi^2 = 1$. We denote with Sesq(V) the collection of sesquilinear forms on V. Consider $f \in \mathrm{Sesq(V)}$ satisfying a quite strong condition, $\forall v, w \in V$, $\exists \varepsilon \in F$, $\beta \in \mathrm{Aut}(F)$ such that

$$f(v^\tau, w^\tau) = \varepsilon f(v, w)^\beta. \tag{4}$$

We start pointing out

Lemma 51. *Let τ be an involution in $\Gamma\mathrm{L}(V)$, $\psi = \psi(\tau)$, $0 \neq f \in \mathrm{Sesq}(V)$. Suppose $\exists \varepsilon \in F, \beta \in \mathrm{Aut}(F)$ such that $f(v^\tau, w^\tau) = \varepsilon f(v, w)^\beta$, then $\varepsilon^{1+\psi} = 1$ and $\beta = \psi$.*

Proof. Take $v, w \in V$ so that $f(v, w) \neq 0$. Let $\mu = f(v, w)^{-1}$, then $f(\mu v, w) = 1$. So assume $f(v, w) = 1$. It follows that $1 = \varepsilon f(v^\tau, w^\tau)^\beta$, so $\varepsilon \neq 0$. Moreover,

$$\varepsilon \lambda^\beta f(v, w)^\beta = \varepsilon f(\lambda v, w)^\beta = f((\lambda v)^\tau, w^\tau) = f(\lambda^\psi v^\tau, w^\tau) = \lambda^\psi \varepsilon f(v, w).$$

Thus $\beta = \psi$. Since $\tau^2 = 1$,

$$f(v, w) = \varepsilon f(v^\tau, w^\tau)^\psi = \varepsilon^{1+\psi} f(v, w),$$

and $\varepsilon^{1+\psi} = 1$. □

Let $V_\rho = \{u \in V : u^\tau = \rho u\}$. If $F_0 = C_F(\psi(\tau))$, then V_ρ turns out to be an F_0-vector subspace of V. Assume $V_\rho \ni v \neq 0$, then

$$v = v^{\tau^2} = (\rho v)^\tau = \rho^{1+\psi} v$$

so that $\rho^{1+\psi} = 1$. If $v, u \in V_\rho$, then $\varepsilon f(u, v)^\psi = f(u^\tau, v^\tau) = \rho^{1+\alpha} f(u, v)$, where α is the automorphism associated to f. Denote $\eta = \frac{\varepsilon}{\rho^{1+\alpha}}$. Since F is a cyclic extension of any of its subfields, ψ and α commute. So $\eta^{1+\psi} = 1$ and by Hilbert's Satz 90 (see [15]) $\exists a \in F$ such that $a^{1-\psi} = \eta$. Therefore $f(V_\rho, V_\rho) = 0$ or $a^{-\psi} F_0$. We may wonder whether a sesquilinear form satisfying (4) remains non-degenerate when restricting on the eigenspaces V_ρ.

Proposition 52. *Let τ be an involution in $\Gamma\mathrm{L}(V)$, $\psi = \psi(\tau)$, $0 \neq f \in \mathrm{Sesq}(V)$ meeting $f(v^\tau, w^\tau) = \varepsilon f(v, w)^\psi$, and V_ρ an eigenspace for τ. Then unless $\psi = 1$, $\varepsilon = -1$, $\mathrm{Rad}(V) = 0$ implies $\mathrm{Rad}(V_\rho) = 0$.*

Proof. The assertion is trivial if $V_\rho = 0$. Otherwise $\rho \neq 0$. Consider $w = \rho^{-1}v + v^\tau$, then $w^\tau \in V_\rho$. Let $u \in V_\rho$, then $\rho u \in V_{\rho^{-1}}$. Assume that $u \in \mathrm{Rad}(V_\rho)$, then

$$\begin{aligned} 0 &= f(u, \rho^{-1}v + v^\tau) = f(u\rho^{-1}, v) + f((\rho u)^\tau, v^\tau) \\ &= f(u\rho^{-1}, v) + \varepsilon f(\rho u, v)^\psi = \rho^{-\alpha} f(u, v) + \varepsilon\rho^\psi f(u, v)^\psi. \end{aligned}$$

If $\psi = 1$, $(\rho^{-\alpha} + \varepsilon\rho) f(u, v) = 0$. Since $\rho^2 = 1$, $\rho = \pm 1$ and $\rho^\alpha = \rho$, then $\rho(1 + \varepsilon) f(u, v) = 0$. If $\varepsilon \neq -1$, then $u \in \mathrm{Rad}(V) = 0$. If $\psi \neq 1$, substitute v with $\lambda^\alpha v$, then

$$\rho^{-\alpha}\lambda f(u, v) + \varepsilon\rho^\psi \lambda^\psi f(u, v)^\psi = 0.$$

Let $\mu \neq \mu^\psi$, then $\det \begin{pmatrix} \rho^{-\alpha} & \varepsilon\rho^\psi \\ \rho^{-\alpha}\mu & \varepsilon\rho^\psi\mu^\psi \end{pmatrix} = \varepsilon\rho^{\psi-\alpha}(\mu^\psi - \mu) \neq 0$, so $f(u, v) = 0$ and again $u = 0$. □

We provide a couple of examples:

Example 53. Let $V = (F)_n$, the full matrix algebra and $f(v, w) = \mathrm{tr}(vw)$. Let $|\psi| = 2$, $\psi \in \mathrm{Aut}(F)$, and τ defined via $(a_{ij})^\tau = (a_{ij}^\psi)$. Then $f(v^\tau, w^\tau) = \mathrm{tr}(v^\tau w^\tau) = f(v, w)^\psi$, but $\alpha = \alpha(f) = 1$, so that the automorphism associated to f does not coincide with that related to τ.

The next example proves that in the former proposition the exception really occurs.

Example 54. Let $V = \langle a, b\rangle$. Define $\tau \in \mathrm{GL}(V)$ via $a^\tau = a, b^\tau = -b$. Consider the symmetric bilinear form $f = e_{12} + e_{21}$. Then $f(v^\tau, w^\tau) = -f(v, w)$, $\mathrm{Rad}(V) = 0$, but $\mathrm{Rad}(V_\rho) = V_\rho$, for any $\rho \in F$.

Corollary 55. *Let $V = (F)_n$, $\psi \in \mathrm{Aut}(F)$ of order two, $f(a, b) = \mathrm{tr}(ab)$, $(a_{ij})^\tau = (a_{ji}^\psi)$, then* $\mathrm{Rad}(V_1) = 0$.

Proof. Since $\mathrm{Rad}(V) = 0$ and $f(a^\tau, b^\tau) = f(a, b)^\psi$, apply Proposition 52. □

This Corollary is essentially needed to identify the space of hermitian matrices A with its dual $\mathrm{Hom}(A, C_F(\psi))$.

Theorem 56. *Let U be a Sylow p-subgroup of* $\mathrm{U}(2n, F)$, *the unitary group over the field $F = \mathbb{F}_{q^2}$, q a p-power, then U is a q-power-degree group.*

Proof. Let $(a_{ij})^\tau = (a_{ji}^q)$. In [19] we proved that U is isomorphic to the semidirect product $A \rtimes K$, $A = \ker(1 - \tau)$ the set of hermitian matrices on F, and K the unitriangular group on F acting on A via $a^k = kak^\tau$. Let $\phi : F \to \mathbb{F}_p$ be the field trace

and $\chi : \mathbb{F}_p \to \mathbb{C}^*$ a non trivial character. Pick b out of A, then $\lambda_b : a \mapsto \chi\phi\mathrm{tr}(ab)$ lies in $\mathrm{Irr}(A)$. By Corollary 55 the correspondence $b \leftrightarrow \lambda_b$ is a bijection from A to $\mathrm{Irr}(A)$. Routine check shows that $\lambda_b^{k^{-1}} = \lambda_{k^\tau bk}$. As a consequence of Corollary 16 and the weak equivalence of A with $\mathrm{Irr}(A)$ as K-set (compare [19]), $s(\mathrm{Irr}(A), K) \subseteq \{q^j : 0 \leqslant j\}$. By Clifford theory $\mathrm{cd}(U) = \{\beta(1)|\lambda^K| : \lambda \in \mathrm{Irr}(A), \beta \in \mathrm{Irr}(I_U(\lambda)/A)\}$. Using Theorem 4 in [19], it turns out that $I_U(\lambda)/A \simeq C_K(\lambda)$ is a strong $C_F(\psi)$-subgroup of K (see [12]), hence a q-power-degree group and the same holds for U. □

We now provide a complete description for $\mathrm{cd}(U)$.

Theorem 57. *Let U be a Sylow p-subgroup of $\mathrm{SU}(2n, q^2)$, q a p-power, then $\mathrm{cd}(U) = \{q^j : 0 \leqslant j \leqslant n^2 - n\}$.*

Proof. As we already mentioned $s(A, K) = s(\mathrm{Irr}(A), K)$. By Clifford theory $\mathrm{cd}(U) \supseteq s(\mathrm{Irr}(A), K)$. By Itô's Theorem (see [11, p. 84]) $\max \mathrm{cd}(U) \leqslant |K| = \max s(A, K) = q^{2\binom{n}{2}}$. By Theorem 56 $\mathrm{cd}(U) \subseteq \{q^j : 0 \leqslant j\}$. By Theorem 19, $s(A, K) = \{q^j : 0 \leqslant j \leqslant n^2 - n\}$. □

We would like to point out that using techniques from [19] Sangroniz [20] and Szegedy [21] have proved that the maximal unipotent subgroups of classical groups, apart from symplectic or orthogonal groups in even characteristic, are q-power-degree groups.

We conclude with some open problems:

1. determine the *degree polynomial* for U, $\delta_U(t) = \sum_i d_i t^i$, where d_i is the number of irreducible characters of U whose degree is q^i;
2. in particular, if q is even establish whether $\mathrm{cd}(U) = s(\mathrm{Irr}(A), K)$, when G is of symplectic type.

Acknowledgments

I would to thank Prof. Rod Gow and Dr. Martin Marjoram for their helpful suggestions and discussions. I would like to dedicate this paper to the memory of my father.

References

[1] A. Vera-López, J.M. Arregi, Computing in unitriangular matrices over finite fields, Linear Algebra Appl. 387 (2004) 193–219.
[2] A. Vera-López, J.M. Arregi, Conjugacy classes in unitriangular matrices, Linear Algebra Appl. 370 (2003) 85–124.

[3] A. Vera-López, J.M. Arregi, Polynomial properties in unitriangular matrices, J. Algebra 244 (1) (2001) 343–351.
[4] M. Aschbacher, Finite Group Theory, in: Cambridge Studies in Advanced Mathematics, vol. 10, Cambridge University Press, Cambridge–New York, 1986.
[5] W. Bosma, J. Cannon, MAGMA 2.11 Handbook, University of Sydney, 2004. Available from: <http://magma.maths.usyd.edu.au/magma/>.
[6] R.W. Carter, Simple Groups of Lie Type, Wiley–Interscience, New York, 1989.
[7] J. Dieudonné, La Géométrie des Groupes Classiques, Ergebnisse der Mathematik und ihrer Grenzgebiete, Heft 5, Springer-Verlag, Berlin-Göttingen-Heidelberg, 1955.
[8] R.H. Dye, On the Arf invariant, J. Algebra 53 (1) (1978) 36–39.
[9] R. Gow, M. Marjoram, A. Previtali, On the irreducible characters of a Sylow 2-subgroup of the finite symplectic group in characteristic 2, J. Algebra 241 (2001) 393–409.
[10] B. Huppert, A remark on the character-degrees of some p-groups, Arch. Math. 59 (4) (1992) 313–318.
[11] I.M. Isaacs, Character Theory of Finite Groups, in: Pure and Applied Mathematics, vol. 69, Academic Press, New York–London, 1976.
[12] I.M. Isaacs, Characters of groups associated with finite algebras, J. Algebra 177 (3) (1995) 708–730.
[13] W. Koepf, Hypergeometric Summation, Vieweg, Braunschweig-Wiesbaden, 1998.
[14] M. Marjoram, Irreducible characters of a Sylow p-subgroup of the orthogonal group, Comm. Algebra 27 (3) (1999) 1171–1195.
[15] P. Morandi, Field and Galois Theory, in: Graduate Texts in Mathematics, vol. 167, Springer-Verlag, New York.
[16] M. Petkovšek, H.S. Wilf, D. Zeilberger, A=B, A.K. Peters, Wellesley, 1996.
[17] A. Previtali, Orbit lengths and character degrees in p-Sylow subgroups of some classical Lie groups, J. Algebra 177 (3) (1995) 658–675.
[18] A. Previtali, On a conjecture concerning character degrees of some p-groups, Arch. Math. 65 (5) (1995) 375–378.
[19] A. Previtali, Maps behaving like exponentials and maximal unipotent subgroups of groups of Lie type, Comm. Algebra 27 (5) (1999) 2511–2519.
[20] J. Sangroniz, Character degrees of the Sylow p-subgroups of classical groups, London Mathematical Society Lecture Note Series, vol. 305, 2003, pp. 487–493.
[21] B. Szegedy, Characters of the Borel and Sylow subgroups of classical groups, J. Algebra 267 (2003) 130–136.
[22] J.G. Thompson, $\mathrm{k}(U_n(\mathbb{F}_q))$, downloadable from the author web page http://www.math.ufl.edu/fac/thompson.html.
[23] A. Wagner, On the classification of the classical groups, Math. Zeitschrift 97 (1967) 66–76.