Pacific Journal of Mathematics

SUPERCHARACTERS OF THE SYLOW *p*-SUBGROUPS OF THE FINITE SYMPLECTIC AND ORTHOGONAL GROUPS

Carlos A. M. André and Ana Margarida Neto

Volume 239 No. 2 February 2009

PACIFIC JOURNAL OF MATHEMATICS
Vol. 239, No. 2, 2009

SUPERCHARACTERS OF THE SYLOW p-SUBGROUPS OF THE FINITE SYMPLECTIC AND ORTHOGONAL GROUPS

CARLOS A. M. ANDRÉ AND ANA MARGARIDA NETO

We define and study supercharacters of the classical finite unipotent groups of types $B_n(q)$, $C_n(q)$ and $D_n(q)$. We show that the results we proved in 2006 remain valid over any finite field of odd characteristic. In particular, we show how supercharacters for groups of those types can be obtained by restricting the supercharacter theory of the finite unitriangular group, and prove that supercharacters are orthogonal and provide a partition of the set of all irreducible characters. In addition, we prove that the unitary vector space spanned by all the supercharacters is closed under multiplication, and establish a formula for the supercharacter values. As a consequence, we obtain the decomposition of the regular character as an orthogonal linear combination of supercharacters. Finally, we give a combinatorial description of all the irreducible characters of maximum degree in terms of the root system, by showing how they can be obtained as constituents of particular supercharacters.

Introduction

The concept of supercharacter theory for an arbitrary finite group was developed by P. Diaconis and I. M. Isaacs [2008]. Roughly, supercharacter theory replaces irreducible characters by *supercharacters* and conjugacy classes by *superclasses* in such a way that a supercharacter table can be constructed as an almost unitary matrix with properties similar to those of the usual character table (namely, orthogonality of rows and columns). More precisely, given any finite group G, a *supercharacter theory* for G consists of a partition $\mathcal{K}$ of G and a set $\mathcal{X}$ of (complex) characters of G satisfying these three axioms:

(i) $|\mathcal{K}| = |\mathcal{X}|$;

(ii) every irreducible character of G is a constituent of a unique $\xi \in \mathcal{X}$;

MSC2000: primary 20C15; secondary 20G40.

Keywords: finite unipotent group, symplectic group, orthogonal group, supercharacter, positive root, basic set of positive roots.

This research was partially supported by the Fundação para a Ciência e Tecnologia (Lisbon, Portugal) through the project POCTI-ISFL-1-1431. André's research was partially supported by the sabbatical research grant 4/2008 of the Fundação Luso-Americana para o Desenvolvimento (Lisbon).

(iii) the characters in $\mathscr{X}$ are constant on the members of $\mathscr{K}$.

We call the elements of $\mathscr{K}$ *superclasses*, and the elements of $\mathscr{X}$ *supercharacters* of G. (We observe that, by [Diaconis and Isaacs 2008, Lemma 2.1], axiom (ii) is equivalent to requiring that $\{1\} \in \mathscr{K}$.)

Every finite group G has two trivial supercharacter theories: the full character theory (where $\mathscr{X}$ consists of all irreducible characters of G, and $\mathscr{K}$ of all the conjugacy classes of G), and the one where $\mathscr{X} = \{1_G, \rho_G - 1_G\}$ and $\mathscr{K}$ consists of the sets $\{1\}$ and $G - \{1\}$; as usual, we denote by 1_G the trivial character and by ρ_G the regular character of G. Although for some groups these are the only possibilities, there are many groups for which nontrivial supercharacter theories exist, and in many cases it may be possible to obtain useful information using some particular supercharacter theory. An illustrating example can be found in [2004] where E. Arias-Castro, P. Diaconis and R. Stanley showed that a special supercharacter theory can be applied to study a random walk on upper triangular matrices over finite fields using techniques that traditionally required the knowledge of the full character theory.

Supercharacters theories were initially developed for the upper unitrangular group $U_n(q)$ consisting of all unipotent upper-triangular $n \times n$ matrices over the finite field $\mathbb{F}_q$ with q elements (where q is a power of some prime number p). It is known that an explicit description of the irreducible characters and conjugacy classes of $U_n(q)$ is an intractable problem; in fact, [Gudivok et al. 1990] shows that a "nice" description of the conjugacy classes of $U_n(q)$ leads to a nice description of wild quivers. However, in his PhD thesis [André 1992], the first author begun the study of the basic characters of $U_n(q)$ (under the assumption that $p \geq n$), and was able to show that by clumping together some of the conjugacy classes and some of the irreducible characters, one attains a workable approximation to the representation theory of $U_n(q)$. The results, published in a series of papers in the *Journal of Algebra*, showed in particular that the basic characters determine uniquely the superclasses of a supercharacter theory for $U_n(q)$. (The theory of basic characters was renamed by Roger W. Carter to "superclass and supercharacter theory"). We mention that the original theory relies on a construction due to D. Kazhdan [1977] and is based on Kirillov's method of coadjoint orbits (see [Kirillov 1995] for a description of this method for the unitriangular group; J. Sangroniz [2004] gives a general version of Kazhdan's construction for algebra groups defined over finite fields of sufficiently large characteristic). N. Yan [2001] then showed how basic characters can be obtained using more elementary methods that avoid Kazhdan's construction and the algebraic geometry involved in it. Yan's approach is valid for an arbitrary prime, and was generalized later by P. Diaconis and M. Isaacs [2008] so as to extend the theory to an arbitrary finite algebra group defined over $\mathbb{F}_q$ (see also [André and Nicolás 2008], where a generalization was obtained for algebra groups defined over finite radical rings and over certain rings of p-adic integers).

The main goal of this paper is to extend to an arbitrary odd prime the results obtained in our paper [AN 2006], where we started to develop a supercharacter theory for a Sylow p-subgroup U of one of the (nontwisted) Chevalley groups $C_n(q)$, $B_n(q)$, and $D_n(q)$. (We mention that the present paper is a companion of the forthcoming [André and Neto 2008], which establishes a supercharacter theory for U by defining the superclasses of U.) As in [AN 2006], the notion of a supercharacter of U is very similar to the notion of a basic character of the unitriangular group $U_n(q)$, and follows the original idea of parametrizing supercharacters by certain minimal subsets of (positive) roots. In fact, it is known that the supercharacters of $U_n(q)$ can be obtained as certain reduced products of *elementary characters*, which are irreducible characters corresponding to the matrix entries (i, j) for $1 \leq i < j \leq n$, labeled by nonzero elements of $\mathbb{F}_q$; in Yan's thesis, elementary characters were called *primary characters*, and the supercharacters were called *transition characters*. (We mention that the factorization of a supercharacter as a product of elementary characters holds, not only for the unitriangular group, but also for any finite algebra group, as explained in [André and Pinho 2008], where a relation is obtained between factorizations of supercharacters and decomposability of certain cyclic modules.)

Following Yan's method, one can show that the supercharacters of $U_n(q)$ are parametrized by certain combinatorial data consisting of a *basic set* D of matrix entries such that no two elements of D agree in either the first or the second coordinate, and of a map ϕ from D to the nonzero elements of $\mathbb{F}_q$. (There is an alternative way of parametrizing the supercharacters of $U_n(q)$ by labeled set partitions of $\{1, 2, \ldots, n\}$, and we mention that a rich combinatorial structure is arising and appears to have a remarkable analogy with the well-known connection between partitions of n and the representation theory of the symmetric group S_n; see [Marberg and Thiem 2008; Thiem and Venkateswaran 2007].)

In the present paper, as in [AN 2006], we define the supercharacters to be certain *reduced* products of elementary characters (which in general are not necessarily irreducible characters) of the given Sylow p-subgroup U. These reduced products are parametrized by pairs consisting of a conveniently chosen basic subset of roots and of a map to the nonzero elements of $\mathbb{F}_q$. (We note that the roots in the unitriangular case are in one-to-one correspondence with the matrix entries.) In fact, the group U can be naturally identified with a subgroup of a unitriangular group, and we will show that the elementary characters (and supercharacters) of U can be obtained as constituents of the restriction of a supercharacter of that unitriangular group.

The paper is organized as follows. In Section 1, we introduce the necessary notation and define the elementary characters and the supercharacters of the group U. Then in Section 2, we obtain the elementary characters of U by restricting elementary characters of the unitriangular group that contains U, and we use this information to show that the complex vector space spanned by the supercharacters is, in fact, the associative algebra finitely generated by the elementary characters. As a consequence, we deduce that every irreducible character of U is a constituent of a supercharacter. Then in Section 4, we prove the orthogonality of supercharacters (as class functions of U) by using a partition of the dual space of the Lie algebra of U in terms of its basic subvarieties as obtained in [AN 2006, Theorem 4.5]. In Section 5, we deduce a formula for the supercharacters analogous to the one proved in [Diaconis and Isaacs 2008, Theorem 5.6], and obtain a decomposition of the regular character of U as a linear combination (with nonnegative integer coefficients) of supercharacters. Finally, in Section 6, we apply our results on supercharacters to identify the irreducible characters of maximum degree of U. Several times, we refer to results proved for the unitriangular group under the assumption that the prime p is sufficiently large. However, those results are known to be true for arbitrary primes; this follows from Yan's work, but see also [André 2002] or [Diaconis and Isaacs 2008].

1. Supercharacters

Let $p \geq 3$ be a prime number, let $q = p^e$ for $e \geq 1$ be a power of p, and let $\mathbb{F}_q$ be the finite field with q elements. For a fixed positive integer n, let G denote one of the following classical finite groups: the symplectic group $\mathrm{Sp}_{2n}(q)$, the even orthogonal group $\mathrm{O}_{2n}(q)$, or the odd orthogonal group $\mathrm{O}_{2n+1}(q)$ (in alternative notation, these are the (nontwisted) Chevalley groups $C_n(q)$, $B_n(q)$, and $D_n(q)$, respectively). Throughout the paper, we set $U = G \cap U_m(q)$ where

$$m = \begin{cases} 2n & \text{if } G = \mathrm{Sp}_{2n}(q) \text{ or } G = \mathrm{O}_{2n}(q), \\ 2n+1 & \text{if } G = \mathrm{O}_{2n+1}(q) \end{cases}$$

and $U_m(q)$ denotes the upper unitriangular group consisting of all unipotent upper-triangular $m \times m$ matrices over $\mathbb{F}_q$. Then U is a Sylow p-subgroup of G, and it is described as follows. Let $J = J_n$ be the $n \times n$ matrix with ones along the antidiagonal and zeros elsewhere. Then U consists of all (block) matrices of the form

$$\begin{pmatrix} x & xu & xz \\ 0 & I_r & -u^T J \\ 0 & 0 & Jx^{-T} J \end{pmatrix}, \tag{1a}$$

where $x \in U_n(q)$, u is an $n \times r$ matrix over $\mathbb{F}_q$, and

$$\begin{aligned} r &= 0 \quad \text{and} \quad Jz^T - zJ = 0 && \text{if } U \leq \mathrm{Sp}_{2n}(q), \\ r &= 0 \quad \text{and} \quad Jz^T + zJ = 0 && \text{if } U \leq \mathrm{O}_{2n}(q), \\ r &= 1 \quad \text{and} \quad Jz^T + zJ = -uu^T && \text{if } U \leq \mathrm{O}_{2n+1}(q). \end{aligned}$$

As mentioned in the introduction, the supercharacters of U will be parametrized by certain subsets of (positive) roots. Thus, we introduce some notation and recall some elementary facts concerning roots; for details, see the books [1972; 1985] by R. Carter, and see also [Curtis and Reiner 1987, Chapter 8]. Let T be the maximal torus of G consisting of all diagonal matrices, and let Σ be the root system defined by T. The elements of Σ are described as follows. For each $1 \leq i \leq n$, let $\varepsilon_i : T \to \mathbb{F}_q^\times$ be the map defined by $\varepsilon_i(t) = t_i$ for all $t \in T$; here, we denote by $t_i \in \mathbb{F}_q^\times$ the i-th diagonal entry of the matrix $t \in T$. Then $\Sigma = \Phi \cup (-\Phi)$, where

$$\Phi = \{\varepsilon_i \pm \varepsilon_j : 1 \leq i < j \leq n\} \cup \Phi'$$

and

$$\Phi' = \begin{cases} \{2\varepsilon_i : 1 \leq i \leq n\} & \text{if } G = \mathrm{Sp}_{2n}(q), \\ \varnothing & \text{if } G = \mathrm{O}_{2n}(q), \\ \{\varepsilon_i : 1 \leq i \leq n\} & \text{if } G = \mathrm{O}_{2n+1}(q). \end{cases}$$

The roots in Φ are said to be *positive*, and the roots in $-\Phi$ are said to be *negative*. Throughout the paper, "root" will always stand for "positive root".

To Φ we associate the subset of "matrix entries" $\mathscr{E} \subseteq \{(i, j) : -n \leq i, j \leq n\}$ as follows. For any $\alpha \in \Phi$, we set

$$\mathscr{E}(\alpha) = \begin{cases} \{(i, j), (-j, -i)\} & \text{if } \alpha = \varepsilon_i - \varepsilon_j \text{ for } 1 \leq i < j \leq n, \\ \{(i, -j), (j, -i)\} & \text{if } \alpha = \varepsilon_i + \varepsilon_j \text{ for } 1 \leq i < j \leq n, \\ \{(i, -i)\} & \text{if } G = \mathrm{Sp}_{2n}(q) \text{ and } \alpha = 2\varepsilon_i \text{ for } 1 \leq i \leq n, \\ \{(i, 0), (0, -i)\} & \text{if } G = \mathrm{O}_{2n+1}(q) \text{ and } \alpha = \varepsilon_i \text{ for } 1 \leq i \leq n, \end{cases}$$

and we define $\mathscr{E} = \bigcup_{\alpha \in \Phi} \mathscr{E}(\alpha)$. More generally, for each subset $\Psi \subseteq \Phi$, we set $\mathscr{E}(\Psi) = \bigcup_{\alpha \in \Psi} \mathscr{E}(\alpha)$; hence, $\mathscr{E} = \mathscr{E}(\Phi)$.

We consider the mirror order $\prec$ on the set $\{0, \pm 1, \ldots, \pm(n+1)\}$; this ordering is defined as

$$1 \prec 2 \prec \cdots \prec n+1 \prec 0 \prec -(n+1) \prec \cdots \prec -2 \prec -1,$$

and we shall index the rows (from left to right) and columns (from top to bottom) of any $m \times m$ matrix according to this ordering. Hence, the entries of any matrix $x \in U_m(q)$ are indexed by all the pairs $(i, j) \in \mathscr{E}$: For each $(i, j) \in \mathscr{E}$, we shall write $x_{i,j}$ to denote the entry of x that occurs in the i-th row and the j-th column.

For our purposes, it is convenient to consider the set

$$\mathscr{E}^+ = \{(i, j) \in \mathscr{E} \colon 1 \le i \le n,\ i \prec j \preceq -i\},$$

and extend this notation to any subset $\Psi \subseteq \Phi$ by setting $\mathscr{E}^+(\Psi) = \mathscr{E}(\Psi) \cap \mathscr{E}^+$. We observe that there exists a one-to-one correspondence between Φ and $\mathscr{E}^+$.

For any $\alpha \in \Phi$, we define the subgroup U_α of U as follows:

$$\begin{aligned} U_\alpha &= \{x \in U \colon x_{i,k} = 0,\ i < k < j\} \\ &\qquad \text{if } \alpha = \varepsilon_i - \varepsilon_j \text{ for } 1 \le i < j \le n; \\ U_\alpha &= \{x \in U \colon x_{i,k} = x_{j,l} = 0,\ i < k \le n,\ j \prec l \preceq 0\} \\ &\qquad \text{if } \alpha = \varepsilon_i - \varepsilon_j \text{ for } 1 \le i < j \le n; \\ U_\alpha &= \{x \in U \colon x_{i,k} = 0,\ i < k \le n\} \\ &\qquad \text{if either } \alpha = 2\varepsilon_i \text{ for } 1 \le i \le n \text{ (in the case where } U \le \mathrm{Sp}_{2n}(q)) \\ &\qquad\qquad \text{or } \alpha = \varepsilon_i \quad \text{for } 1 \le i \le n \text{ (in the case where } U \le \mathrm{O}_{2n+1}(q)). \end{aligned}$$

Let $\vartheta \colon \mathbb{F}_q \to \mathbb{C}^\times$ be a nontrivial linear character of the additive group $\mathbb{F}_q^+$ of $\mathbb{F}_q$ (this character will be kept fixed throughout the paper; moreover, all characters will be taken over the complex field). For any $r \in \mathbb{F}_q^\times$, the mapping $x \mapsto \vartheta(r x_{i,j})$ defines a linear character $\lambda_{\alpha,r} \colon U_\alpha \to \mathbb{C}^\times$ of U_α, and we define the *elementary character* $\xi_{\alpha,r}$ to be the induced character $\xi_{\alpha,r} = (\lambda_{\alpha,r})^U$ (see [André 1995a] for the corresponding definition in the case of the unitriangular group; see also [Diaconis and Isaacs 2008, Corollary 5.11] and the discussion thereon).

We next define the notion of a "basic subset of roots". To start with, we recall that a subset $\mathscr{D} \subseteq \mathscr{E}$ is said to be *basic* if it contains at most one entry from each row and at most one root from each column; in other words, $\mathscr{D} \subseteq \mathscr{E}$ is basic if

$$|\{j \colon i \prec j \preceq -1,\ (i, j) \in \mathscr{D}\}| \le 1 \quad \text{and} \quad |\{i \colon 1 \preceq i \prec j,\ (i, j) \in \mathscr{D}\}| \le 1$$

for all $-n \le i, j \le n$. Then we say that $D \subseteq \Phi$ is a *basic subset* if $\mathscr{D} = \mathscr{E}(D)$ is a basic subset of $\mathscr{E}$. (We will always use script letters to denote basic subsets of $\mathscr{E}$, in contrast to basic subsets of Φ, which will be mostly denoted by italic letters.)

Given any nonempty basic subset $D \subseteq \Phi$ and any map $\phi \colon D \to \mathbb{F}_q^\times$, we define the supercharacter $\xi_{D,\phi}$ to be the product

$$\xi_{D,\phi} = \prod_{\alpha \in D} \xi_{\alpha,\phi(\alpha)}.$$

For convenience, if D is the empty subset of Φ, we consider the empty map $\phi \colon D \to \mathbb{F}_q^\times$, and define $\xi_{D,\phi}$ to be the unit character 1_U of U. Let

$$U_D = \bigcap_{\alpha \in D} U_\alpha \quad \text{and} \quad \lambda_{D,\phi} = \prod_{\alpha \in D} (\lambda_{\alpha,\phi(\alpha)})_{U_D}.$$

Then $\lambda_{D,\phi}$ is clearly a linear character of U_D and, by [AN 2006, Proposition 2.2], the supercharacter $\xi_{D,\phi}$ can be obtained as the induced character

$$\xi_{D,\phi} = (\lambda_{D,\phi})^U. \tag{1b}$$

We now state the main result of this paper, which extends [AN 2006, Theorem 1.1] for arbitrary odd primes. (Given any finite group G, we denote by $\mathrm{Irr}(G)$ the set of all irreducible characters of G, and by $\langle\cdot,\cdot\rangle$ (or by $\langle\cdot,\cdot\rangle_G$ if necessary) the Frobenius scalar product on the complex vector space of all class functions defined on G.)

Theorem 1.1. *Let χ be an arbitrary irreducible character of U. Then χ is a constituent of a unique supercharacter of U; in other words, there exists a unique basic subset $D \subseteq \Phi$ and a unique map $\phi\colon D \to \mathbb{F}_q^\times$ such that $\langle \chi, \xi_{D,\phi}\rangle \neq 0$.*

Our proof depends strongly on the supercharacter theory of the unitriangular group, and on certain *basic subvarieties* defined by polynomial equations on the dual space of the Lie algebra $\mathfrak{u}$ of U. We recall the definition of the Lie algebra $\mathfrak{u}$. Let $\mathfrak{g}$ denote one of the following classical Lie algebras defined over $\mathbb{F}_q$: the symplectic Lie algebra $\mathfrak{sp}_{2n}(q)$, the even orthogonal Lie algebra $\mathfrak{o}_{2n}(q)$, or the odd orthogonal Lie algebra $\mathfrak{o}_{2n+1}(q)$. Then $\mathfrak{u} = \mathfrak{g} \cap \mathfrak{u}_m(q)$, where $\mathfrak{u}_m(q)$ denotes the upper niltriangular Lie algebra consisting of all nilpotent upper-triangular $m \times m$ matrices over $\mathbb{F}_q$. Thus, $\mathfrak{u}$ consists of all (block) matrices of the form

$$\begin{pmatrix} a & u & w \\ 0 & 0_r & -u^T J \\ 0 & 0 & -Ja^T J \end{pmatrix} \tag{1c}$$

where $a \in \mathfrak{u}_n(q)$, u is an $n \times r$ matrix over $\mathbb{F}_q$, and

$$\begin{array}{llll} r = 0 & \text{and} & Jw^T - wJ = 0 & \text{if } \mathfrak{u} \le \mathfrak{sp}_{2n}(q); \\ r = 0 & \text{and} & Jw^T + wJ = 0 & \text{if } \mathfrak{u} \le \mathfrak{o}_{2n}(q); \\ r = 1 & \text{and} & Jw^T + wJ = -uu^T & \text{if } \mathfrak{u} \le \mathfrak{o}_{2n+1}(q). \end{array}$$

For any $\alpha \in \Phi$, we will denote by e_α the matrix in $\mathfrak{u}$ defined as follows (as usual, $1 \le i < j \le n$):

$$e_\alpha = \begin{cases} e_{i,j} - e_{-j,-i} & \text{if } \alpha = \varepsilon_i - \varepsilon_j, \\ e_{i,-j} + e_{j,-i} & \text{if } \alpha = \varepsilon_i + \varepsilon_j \text{ and } \mathfrak{u} \le \mathfrak{sp}_{2n}(q), \\ e_{i,-j} - e_{j,-i} & \text{if } \alpha = \varepsilon_i + \varepsilon_j \text{ and } \mathfrak{u} \le \mathfrak{o}_{2n}(q) \text{ or } \mathfrak{u} = \mathfrak{o}_{2n+1}(q), \\ e_{i,-i} & \text{if } \mathfrak{u} \le \mathfrak{sp}_{2n}(q) \text{ and } \alpha = 2\varepsilon_i, \\ e_{i,0} - e_{0,-i} & \text{if } \mathfrak{u} \le \mathfrak{o}_{2n+1}(q) \text{ and } \alpha = \varepsilon_i. \end{cases}$$

It is clear that $\{e_\alpha : \alpha \in \Phi\}$ is an $\mathbb{F}_q$-basis of $\mathfrak{u}$. We denote by $\mathfrak{u}^*$ the dual vector space of $\mathfrak{u}$, and let $\{e_\alpha^* : \alpha \in \Phi\}$ be the $\mathbb{F}_q$-basis of $\mathfrak{u}^*$ dual to the basis $\{e_\alpha : \alpha \in \Phi\}$ of $\mathfrak{u}$; hence $e_\alpha^*(e_\beta) = \delta_{\alpha,\beta}$ for all $\alpha, \beta \in \Phi$.

For any $\alpha \in \Phi$, we define the Lie subalgebra $\mathfrak{u}_\alpha$ of $\mathfrak{u}$ by as follows:

$$\begin{aligned}
\mathfrak{u}_\alpha &= \{a \in \mathfrak{u} \colon a_{i,k} = 0,\ i < k < j\} \\
&\qquad \text{if } \alpha = \varepsilon_i - \varepsilon_j \text{ for } 1 \le i < j \le n; \\
\mathfrak{u}_\alpha &= \{a \in \mathfrak{u} \colon a_{i,k} = a_{j,l} = 0,\ i < k \le n,\ j \prec l \preceq 0\} \\
&\qquad \text{if } \alpha = \varepsilon_i + \varepsilon_j \text{ for } 1 \le i < j \le n; \\
\mathfrak{u}_\alpha &= \{a \in \mathfrak{u} \colon a_{i,k} = 0,\ i < k \le n\} \\
&\qquad \text{if either } \alpha = 2\varepsilon_i \text{ for } 1 \le i \le n \text{ (in the case where } \mathfrak{u} \le \mathfrak{sp}_{2n}(q)) \\
&\qquad\qquad \text{or } \alpha = \varepsilon_i \quad \text{for } 1 \le i \le n \text{ (in the case where } \mathfrak{u} \le \mathfrak{o}_{2n+1}(q)).
\end{aligned}$$

We note that

$$\mathfrak{u}_\alpha = \sum_{\beta \in \Phi(\alpha)} \mathbb{F}_q e_\beta,$$

where $\Phi(\alpha) = \{\beta \in \Phi \colon e_\beta \in \mathfrak{u}_\alpha\}$; hence $\{e_\beta : \beta \in \Phi(\alpha)\}$ is a basis of $\mathfrak{u}_\alpha$.

Remark 1.2. In the case where $p \ge 2n$, we have $a^p = 0$ for all $a \in \mathfrak{u}$, and so we may define the usual exponential map

$$\exp \colon \mathfrak{u} \to U, \quad a \mapsto 1 + a + \tfrac{1}{2!}a^2 + \cdots + \tfrac{1}{n!}a^n \quad \text{for all } a \in \mathfrak{u}.$$

It is well known that exp is bijective and that the Campbell–Hausdorff formula holds: For all $a, b \in \mathfrak{u}$, we have $\exp(a)\exp(b) = \exp(a + b + \vartheta(a, b))$, where $\vartheta(a, b) \in [\mathfrak{u}, \mathfrak{u}]$; see [Jacobson 1979, page 175]. It follows that if $\mathfrak{h}$ is any Lie subalgebra of $\mathfrak{u}$, then the exponential image $H = \exp(\mathfrak{h})$ is a subgroup of U. In particular, $U_\alpha = \exp(\mathfrak{u}_\alpha)$ for any $\alpha \in \Phi$.

2. Elementary characters

We start this section by relating the elementary characters of U to the elementary characters of the corresponding unitriangular group $U_m(q)$. First, we fix some notation. To avoid confusion, we shall denote by $\zeta_{i,j,r}$ the elementary character of $U_m(q)$ associated with the entry $(i, j) \in \mathscr{E}$ and the element $r \in \mathbb{F}_q^\times$. By definition, $\zeta_{i,j,r}$ is the induced character

$$\zeta_{i,j,r} = (\mu_{i,j,r})^{U_m(q)},$$

where $\mu_{i,j,r} \colon U_{i,j} \to \mathbb{C}^\times$ is the linear character of the subgroup

$$U_{i,j} = \{x \in U_m(q) \colon x_{i,k} = 0,\ i \prec k \prec j\}$$

defined by $\mu_{i,j,r}(x) = \vartheta(rx_{i,j})$ for all $x \in U_{i,j}$. We observe that, if $1 \preceq i \prec j \preceq 0$ and $\alpha = \varepsilon_i - \varepsilon_j$, then

$$U_{i,j} \cap U = U_\alpha \quad \text{and} \quad U_{i,j} U_\alpha = U_m(q);$$

for simplicity of writing, we set $\varepsilon_0 = 0$. For the remaining cases, the following lemma will be useful.

Lemma 2.1. *Let $(i,-j) \in \mathscr{E}$ for $1 \leq i < j \leq n$, and let $r \in \mathbb{F}_q^\times$. Let*

$$U'_{i,-j} = \{x \in U_m(q) \colon x_{i,b} = x_{-a,-j} = 0,\ i \prec b \preceq 0,\ j \prec a \preceq 0\},$$

and let $\nu_{i,-j,r} \colon U'_{i,-j} \to \mathbb{C}^\times$ be the linear character of $U'_{i,-j}$ defined by

$$\nu_{i,-j,r}(x) = \vartheta(rx_{i,-j}) \quad \textit{for all } x \in U_{i,j}.$$

Then $\zeta_{i,-j,r} = (\nu_{i,-j,r})^{U_m(q)}$.

Proof. For simplicity, we write $H = U_{i,-j}$, $K = U'_{i,-j}$, $\mu = \mu_{i,-j,r}$, $\nu = \nu_{i,-j,r}$ and $\zeta = \zeta_{i,-j,r}$. It is clear that ν is a linear character of K. By Frobenius reciprocity, we have $\langle \zeta, \nu^{U_m(q)} \rangle = \langle \zeta_K, \nu \rangle$, whereas, by Mackey's subgroup theorem (see [Huppert 1998, Theorem 17.4(a)]), we have

$$\zeta_K = (\mu^{U_m(q)})_K = \sum_{x \in X} (\mu^x_{xHx^{-1} \cap K})^K,$$

where $X \subseteq U_m(q)$ is a complete set of representatives of the (H,K)-double classes of $U_m(q)$; without loss of generality, we choose X so that $1 \in X$. Thus, we obtain

$$\langle \zeta, \nu^{U_m(q)} \rangle = \sum_{x \in X} \langle (\mu^x_{xHx^{-1} \cap K})^K, \nu \rangle = \sum_{x \in X} \langle \mu^x, \nu \rangle_{xHx^{-1} \cap K}.$$

In particular, for $x = 1$, we get $\langle \mu, \nu \rangle_{H \cap K} = 1$ (because, both μ and ν are linear), and thus $\langle \zeta, \nu^{U_m(q)} \rangle \neq 0$. Since ζ is irreducible (by [Diaconis and Isaacs 2008, Corollary 5.11]; see also [André 1995a, Lemma 3]), we conclude that ζ is an irreducible constituent of $\nu^{U_m(q)}$. Since $|U_m(q) : K| = |U_m(q) : H|$, we obtain $\zeta = \nu^{U_m(q)}$ as required. □

We observe that if $\alpha = \varepsilon_i + \varepsilon_j$ for $1 \leq i < j \leq n$, then

$$U'_{i,-j} \cap U = U_\alpha \quad \text{and} \quad U'_{i,-j} U_\alpha = U_m(q).$$

As a consequence of this and the observations above, we may prove the following result.

Proposition 2.2. *Let $\alpha \in \Phi$, let $(i,j) \in \mathscr{E}^+(\alpha)$, and suppose that $j \neq -i$ (in the case where $U \leq \mathrm{Sp}_{2n}(q)$). Then $(\zeta_{i,j,r})_U = (\zeta_{-j,-i,r})_U = \xi_{\alpha,r}$ for all $r \in \mathbb{F}_q^\times$.*

Proof. For simplicity, we set $\zeta = \zeta_{i,j,r}$. Let $K = U_{i,j}$ if $j \preceq 0$, and $K = U'_{i,j}$ if $0 \prec j \prec -i$. As we observed above, $K \cap U = U_\alpha$ and $KU = U_m(q)$. On the other hand, let $\mu = \mu_{i,j,r}$ if $j \preceq 0$ and $\mu = \nu_{i,j}$ if $0 \prec j \prec -i$. By Mackey's subgroup theorem, we get $(\mu^{U_m(q)})_U = (\mu_{K\cap U})^U$. Since $K \cap U = U_\alpha$ and $\mu_{K\cap U} = \lambda_{\alpha,r}$, we conclude that $\zeta_U = \xi_{\alpha,r}$, as required. The proof of the equality $(\zeta_{-j,-i,r})_U = \xi_{\alpha,r}$ is analogous. □

The previous lemma is not true in the case where $U \leq \mathrm{Sp}_{2n}(q)$ and $\alpha = 2\varepsilon_i$ for $1 \leq i \leq n$. In fact, we have $U_\alpha \leq U'_{i,-i}$ (hence $U'_{i,-i}U_\alpha = U'_{i,-i} \neq U_m(q)$ whenever $i \geq 2$). In order to deal with these cases, we start by proving the following auxiliary result. (The subsets $K_{\mathfrak{D},\varphi} \subseteq U_m(q)$ are exactly the superclasses of $U_m(q)$ as explained in [Diaconis and Isaacs 2008, Appendix A]; see also [André 2001; Arias-Castro et al. 2004] or [Yan 2001].)

Lemma 2.3. *Let $\mathfrak{D}$ be a basic subset of $\mathscr{E}$, let $\varphi : \mathfrak{D} \to \mathbb{F}_q^\times$ be a map, and let*

$$e_{\mathfrak{D},\varphi} = \sum_{(i,j)\in\mathfrak{D}} \varphi(i,j)e_{i,j} \in \mathfrak{u}_m(q).$$

Let $O_{\mathfrak{D},\varphi} = U_m(q)e_{\mathfrak{D},\varphi}U_m(q) \subseteq \mathfrak{u}_m(q)$ and $K_{\mathfrak{D},\varphi} = 1 + O_{\mathfrak{D},\varphi} \subseteq U_m(q)$. Let

$$z = \begin{pmatrix} x & xv & xw \\ 0 & I_r & -v^TJ \\ 0 & 0 & Jx^{-T}J \end{pmatrix} \in U \qquad \textit{and} \qquad a_z = \begin{pmatrix} u & v & w \\ 0 & 0_r & -v^TJ \\ 0 & 0 & -Ju^TJ \end{pmatrix} \in \mathfrak{u},$$

where $x = 1 + u$. Then $z \in K_{\mathfrak{D},\varphi}$ if and only if $a_z \in O_{\mathfrak{D},\varphi}$. Moreover, the mapping $z \mapsto a_z$ defines a bijection from U to $\mathfrak{u}$.

Proof. We only consider the case $U \leq \mathrm{Sp}_{2n}(q)$ (the others are similar); hence $r = 0$. Since

$$z = \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} x & w \\ 0 & Jx^{-T}J \end{pmatrix} \begin{pmatrix} x^{-1} & 0 \\ 0 & 1 \end{pmatrix}$$

and $K_{\mathfrak{D},\varphi}$ is invariant under $U_m(q)$-conjugation, we conclude that

$$z \in K_{\mathfrak{D},\varphi} \quad \text{if and only if} \quad \begin{pmatrix} x & w \\ 0 & Jx^{-T}J \end{pmatrix} \in K_{\mathfrak{D},\varphi}.$$

Since $x^{-1} - 1 = -ux^{-1}$, we have $Jx^{-T}J - 1 = (Jx^{-T}J)(-Ju^TJ)$, and so

$$\begin{pmatrix} u & w \\ 0 & Jx^{-T}J - 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & Jx^{-T}J \end{pmatrix} \begin{pmatrix} u & w \\ 0 & -Ju^TJ \end{pmatrix}.$$

It follows that

$$a_z \in O_{\mathfrak{D},\varphi} \quad \text{if and only if} \quad \begin{pmatrix} x & w \\ 0 & Jx^{-T}J \end{pmatrix} \in K_{\mathfrak{D},\varphi},$$

and this completes the proof. □

We are now able to prove the following result. Given any $\mathbb{F}_q$-vector space V and any linear map $f \in V^*$, we denote by ϑ_f the composite map $\vartheta \circ f : V \to \mathbb{C}^\times$; it is straightforward to check that ϑ_f is a linear character of the additive group V^+ and that $\mathrm{Irr}(V^+) = \{\vartheta_f : f \in V^*\}$.

Lemma 2.4. *Let $U \leq \mathrm{Sp}_{2n}(q)$, let $\alpha = 2\varepsilon_i$ for $1 \leq i \leq n$, and let $r \in \mathbb{F}_q^\times$. Then $\xi_{\alpha,r}$ is an irreducible constituent of $(\zeta_{i,-i,r})_U$ with multiplicity* 1; *in particular*, $\xi_{\alpha,r} \neq (\zeta_{i,-i,r})_U$.

Proof. For simplicity, we write $\xi = \xi_{\alpha,r}$ and $\zeta = \zeta_{i,-i,r}$. We evaluate the Frobenius product $\langle \zeta_U, \xi \rangle$. Since $\xi = \lambda^U$, where $\lambda = \lambda_{\alpha,r}$, we have $\langle \zeta_U, \xi \rangle = \langle \zeta_{U_\alpha}, \lambda \rangle$. Let $\mathfrak{u}_{2n}(q)^*$ be the dual space of $\mathfrak{u}_{2n}(q)$, define $e^*_{i,-i} \in \mathfrak{u}_{2n}(q)^*$ by $e^*_{i,-i}(a) = a_{i,-i}$ for all $a \in \mathfrak{u}_{2n}(q)$, and let $O \subseteq \mathfrak{u}_{2n}(q)^*$ be the coadjoint $U_{2n}(q)$-orbit containing $re^*_{i,-i}$. Then by [Diaconis and Isaacs 2008, Corollary 5.11], we have

$$\zeta(1+a) = \frac{1}{\sqrt{|O|}} \sum_{f \in O} \vartheta_f(a) \quad \text{for all } a \in \mathfrak{u}_{2n}(q);$$

in fact, $O = U_{2n}(q)(re^*_{i,-i})U_{2n}(q)$.

Let $z \in U_\alpha$ be arbitrary, and let $a_z \in \mathfrak{u}$ be the element defined in the previous lemma; it is clear that $a_z \in \mathfrak{u}_\alpha$. By [André 1995b, Theorem 1], there exists a (unique) basic subset $\mathcal{D} \subseteq \mathcal{E}$ and a (unique) map $\varphi : \mathcal{D} \to \mathbb{F}_q^\times$ such that $z \in K_{\mathcal{D},\varphi}$. By the previous lemma, we have $1 + a_z \in K_{\mathcal{D},\varphi}$, and so

$$\zeta(z) = \zeta(1+a_z) = \frac{1}{\sqrt{|O|}} \sum_{f \in O} \vartheta_f(a_z).$$

Since the mapping $z \mapsto a_z$ defines a bijection from U_α to $\mathfrak{u}_\alpha$, we conclude that

$$\langle \zeta_{U_\alpha}, \lambda \rangle = \frac{1}{\sqrt{|O|}} \sum_{f \in O} \Big(\frac{1}{|\mathfrak{u}_\alpha|} \sum_{a \in \mathfrak{u}_\alpha} \vartheta_f(a) \overline{\vartheta(ra_{i,-i})} \Big) = \frac{1}{\sqrt{|O|}} \sum_{f \in O} \langle \vartheta_f, \vartheta_{re^*_{i,-i}} \rangle_{\mathfrak{u}_\alpha},$$

and thus

$$\langle \zeta_{U_\alpha}, \lambda \rangle = \frac{1}{\sqrt{|O|}} \big| \{ f \in O : f - re^*_{i,-i} \in (\mathfrak{u}_\alpha)^\perp \} \big|,$$

where $(\mathfrak{u}_\alpha)^\perp = \{ h \in \mathfrak{u}_{2n}(q)^* : h(\mathfrak{u}_\alpha) = 0 \}$.

Now, we consider the basis $\{e_\beta : \beta \in \Phi\}$ of $\mathfrak{u}$. Let $\Psi = \Phi - \{\varepsilon_i - \varepsilon_k : i < k \leq n\}$, so that $\{e_\beta : \beta \in \Psi\}$ is a basis for $\mathfrak{u}_\alpha$. By [André 1995b, Lemma 1], in order to describe $O \cap (\mathfrak{u}_\alpha)^\perp$, it is enough to consider vectors e_β for $\beta \in \Psi$ satisfying $(j,k) \in \mathcal{E}(\beta)$ for some $i \preceq j \prec k \preceq -i$. First, suppose that $\beta = \varepsilon_j - \varepsilon_k$ for $i \leq j < k \leq n$. In this case, we have $e_\beta = e_{j,k} - e_{-k,-j}$, and so $h(e_{j,k}) = h(e_{-k,-j})$ for all $h \in (\mathfrak{u}_\alpha)^\perp$. Similarly, if $\beta = \varepsilon_j + \varepsilon_k$ for $i \leq j < k \leq n$, then $e_\beta = e_{j,-k} + e_{k,-j}$, and thus $h(e_{j,-k}) = -h(e_{k,-j})$ for all $h \in (\mathfrak{u}_\alpha)^\perp$. Finally, if $\beta = 2\varepsilon_j$ for $i \leq j \leq n$, then $e_\beta = e_{j,-j}$, and so $h(e_{j,-j}) = 0$ for all $h \in (\mathfrak{u}_\alpha)^\perp$. Now suppose that $h = f - re^*_{i,-i} \in (\mathfrak{u}_\alpha)^\perp$ for $f \in O$.

Then since $f(e_{j,-j}) = r^{-1} f(i,-j) f(e_{j,-i}) = -r^{-1} f(e_{i,-j})^2$ (see [André 1995b, Lemma 1]), we deduce that $f(e_{i,-j}) = -f(e_{j,-i}) = f(e_{j,-j}) = 0$ for all $i < j \le n$, and this clearly implies that

$$\left|\{f \in O\colon\ f - re^*_{i,-i} \in (\mathfrak{u}_\alpha)^\perp\}\right| = q^{2(n-i)}.$$

Since $\sqrt{|O|} = \zeta(1) = q^{2(n-i)}$, we conclude that $\langle \zeta_U, \xi\rangle = 1$, as required. □

A similar argument can be used to prove the following result.

Lemma 2.5. *Suppose $U \le \mathrm{Sp}_{2n}(q)$, let $\alpha = 2\varepsilon_i$ for $1 \le i \le n$, and let $r \in \mathbb{F}_q^\times$. Let $\zeta = \zeta_{i,-i,r}$ be the supercharacter of $U_{2n}(q)$ associated with $(i,-i)$ and r. Also let $\beta = 2\varepsilon_j$ for $i \le j \le n$, and let $s \in \mathbb{F}_q^\times$ be such that $-rs \in (\mathbb{F}_q^\times)^2$. Then the (irreducible) supercharacter $\xi = \xi_{\alpha,r}\xi_{\beta,s}$ is a constituent of ζ_U with multiplicity 2.*

Proof. By definition, we have $\xi = \lambda^U$, where $\lambda = \lambda_{\alpha,r}\lambda_{\beta,s}$ is the linear character of $V = U_\alpha \cap U_\beta$ defined by $\lambda(x) = \vartheta(rx_{i,-i} + sx_{j,-j})$ for all $x \in V$. Thus, $\langle \zeta_U, \xi\rangle_U = \langle \xi_V, \lambda\rangle_V$. For each $z \in U$, let $a_z \in \mathfrak{u}$ be as in Lemma 2.3. Then for $h = re^*_{i,-i} + se^*_{j,-j} \in \mathfrak{u}_{2n}(q)^*$, we have $\lambda(x) = \vartheta_h(a_x)$ for all $x \in V$. Therefore, since $x \mapsto a_x$ defines a bijection from V to $\mathfrak{v} = \mathfrak{u}_\alpha \cap \mathfrak{u}_\beta$, we deduce that

$$\langle \xi_V, \lambda\rangle_V = \frac{1}{\sqrt{|O|}} \sum_{f\in O} \Bigl(\frac{1}{|\mathfrak{v}|}\sum_{a\in\mathfrak{v}} \vartheta_f(a)\overline{\vartheta_h(a)}\Bigr) = \frac{1}{\sqrt{|O|}} \sum_{f\in O} \langle \vartheta_f, \vartheta_h\rangle_{\mathfrak{v}},$$

where $O = U_{2n}(q)(re^*_{i,-i})U_{2n}(q)$. Thus, we get

$$\langle \xi_V, \lambda\rangle = \frac{1}{\sqrt{|O|}}\left|\{f \in O\colon\ f - h \in \mathfrak{v}^\perp\}\right|.$$

Now, let $\Psi = \Phi - \{\varepsilon_i - \varepsilon_k, \varepsilon_j - \varepsilon_l \colon i < k \le n,\ j < l \le n\}$, so that $\{e_\beta \colon \beta \in \Psi\}$ is a basis for $\mathfrak{v}$. As in the previous proof, for an arbitrary element $g \in \mathfrak{v}^\perp$, we find

$$\begin{aligned} g(e_{k,l}) &= g(e_{-l,-k}) && \text{for all } \beta = \varepsilon_k - \varepsilon_l \in \Psi \text{ with } i < k < l \le n,\\ g(e_{k,-l}) &= -g(e_{l,-k}) && \text{for all } \beta = \varepsilon_k + \varepsilon_l \in \Psi \text{ with } i \le k < l \le n,\\ g(e_{k,-k}) &= 0 && \text{for all } \beta = 2\varepsilon_k \in \Psi \quad \text{ with } i \le k \le n. \end{aligned}$$

Suppose that $f - h \in \mathfrak{v}^\perp$ for some $f \in O$. Then since

$$f(e_{k,-k}) = r^{-1} f(i,-k) f(e_{k,-i}) = -r^{-1} f(e_{i,-k})^2,$$

we deduce that $f(e_{i,-k}) = -f(e_{k,-i}) = f(e_{k,-k}) = 0$ whenever $i \prec k \preceq n$ and $k \ne j$. On the other hand, $s = h(e_{j,-j}) = f(e_{j,-j}) = -r^{-1} f(e_{i,-j})^2 \in -r^{-1}(\mathbb{F}_q^\times)^2$, and thus $-rs \in (\mathbb{F}_q^\times)^2$. Moreover $f(e_{i,-j})$ must be nonzero. Thus we conclude that

$$\left|\{f \in O\colon\ f - h \in \mathfrak{v}^\perp\}\right| = 2q^{2(n-i)},$$

and this completes the proof. □

In the notation of the two previous lemmas, we deduce that

$$\xi_U = \xi_{\alpha,r} + 2 \sum_{i<j\leq n} \sum_{s\subseteq -r^{-1}(\mathbb{F}_q^\times)^2} \xi_{\alpha,r}\xi_{2\varepsilon_j,s} + \eta,$$

where η is either the zero function or a character of U. Taking degrees, we obtain

$$q^{2(n-i)} = q^{n-i}\Bigl(1 + 2\sum_{i<j\leq n} \tfrac{1}{2}(q-1)q^{n-j}\Bigr) + \eta(1) = q^{2(n-i)} + \eta(1).$$

It follows that $\eta(1) = 0$, and this proves the following result.

Proposition 2.6. *Let $U \leq \mathrm{Sp}_{2n}(q)$, let $\alpha = 2\varepsilon_i$ for $1 \leq i \leq n$, and let $r \in \mathbb{F}_q^\times$. Let $\zeta = \zeta_{i,-i,r}$ be the supercharacter of $U_{2n}(q)$ associated with $(i, -i)$ and r. Then*

$$\zeta_U = \xi_{\alpha,r} + 2 \sum_{i<j\leq n} \sum_{s\in -r^{-1}(\mathbb{F}_q^\times)^2} \xi_{\alpha,r}\xi_{2\varepsilon_j,s}.$$

3. The algebra of superclass functions

The main goal of this section is to prove the existence part of Theorem 1.1. We start by proving a result on the decomposition of the product of two elementary characters of U. The argument of the proof uses the corresponding decompositions in the case of the unitriangular group $U_m(q)$, which can be found in [André 1995a, Lemmas 6, 7, 8 and 11]. (The proofs in that paper use the assumption $p \geq m$, but can be easily adapted for an arbitrary prime; see [Yan 2001]. In fact, every irreducible constituent of any of the given decompositions is a supercharacter of $U_m(q)$, and thus is a Kirillov function; see [Diaconis and Isaacs 2008, Theorem 5.10] or [André 2004, Theorem 3].)

Proposition 3.1. *Let $\alpha, \beta \in \Phi$ and $r, s \in \mathbb{F}_q^\times$. Then the product $\xi_{\alpha,r}\xi_{\beta,s}$ decomposes as a sum of supercharacters.*

Proof. The result is obvious in the case where $\{\alpha, \beta\}$ is a basic subset of Φ. Thus we assume that $\{\alpha, \beta\}$ is not basic. Let $(i, j) \in \mathscr{E}^+(\alpha)$ and $(k, l) \in \mathscr{E}^+(\beta)$; without loss of generality, we may assume that $i \leq k$. We observe that, by the definition of basic subset of roots, $\mathscr{E}(\{\alpha, \beta\}) = \{(i, j), (-j, -i), (k, l), (-l, -k)\}$ is not a basic subset of $\mathscr{E}$.

First, we assume that $j \neq -i$ and $l \neq -k$ (in the case where $U = \mathrm{Sp}_{2n}(q)$). Suppose that $\{(i, j), (k, l)\}$ is a basic subset of $\mathscr{E}$. Hence we must have $k = -j$. By the previous lemma, we have $\xi_{\alpha,r}\xi_{\beta,s} = (\zeta_{i,j,r})_U(\zeta_{-j,l,s})_U = (\zeta_{i,j,r})_U(\zeta_{-l,j,s})_U$, and thus, by [André 1995a, Lemma 7], we obtain

$$\begin{aligned}\xi_{\alpha,r}\xi_{\beta,s} &= (\zeta_{i,j,r})_U + \sum_{-l\prec b\prec j}\sum_{t\in\mathbb{F}_q^\times}(\zeta_{i,j,r})_U(\zeta_{-l,b,t})_U \\ &= \xi_{\alpha,r} + \sum_{-l\prec b\prec j}\sum_{t\in\mathbb{F}_q^\times}\xi_{\alpha,r}(\zeta_{-l,b,t})_U.\end{aligned}$$

The result follows by Propositions 2.2 and 2.6.

On the other hand, suppose that $\{(i,j),(k,l)\}$ is not a basic subset of $\mathscr{E}$. First, we consider the case where $i=k$ and $j>l$. By [André 1995a, Lemma 6], we obtain

$$\xi_{\alpha,r}\xi_{\beta,s} = \xi_{\alpha,r} + \sum_{i\prec a\prec l}\sum_{t\in\mathbb{F}_q^\times}\xi_{\alpha,r}(\zeta_{a,l,t})_U,$$

and the result follows because the subsets $\{(i,j),(a,l)\}$ for $i\prec a\prec l$ are all basic. The case where $i<k$ and $j=l$ is similar, because

$$\xi_{\alpha,r}\xi_{\beta,s} = \xi_{\alpha,r} + \sum_{k\prec b\prec j}\sum_{t\in\mathbb{F}_q^\times}\xi_{\alpha,r}(\zeta_{k,b,t})_U$$

(by [André 1995a, Lemma 6]) and because the subsets $\{(i,j),(k,b)\}$ for $k\prec b\prec j$ are all basic.

Finally, suppose that $i=k$ and $j=l$; hence $\alpha=\beta$. On the one hand, if $s\neq -r$, then $\xi_{\alpha,r}\xi_{\alpha,s}$ is equal to

$$(1+(q-1)(j-i-1))(\zeta_{i,j,r+s})_U + \sum_{i\prec a,b\prec j-1}\sum_{t\in\mathbb{F}_q^\times}(q-1)(\zeta_{i,j,r+s})_U(\zeta_{a,b,t})_U$$

(by [André 1995a, Lemma 11]), and the result follows as in the previous cases. On the other hand, suppose that $s=-r$. In this case, [André 1995a, Lemma 8] implies that $\xi_{\alpha,r}\xi_{\alpha,-r}$ is equal to

$$1_U + \sum_{i\prec a\prec j}\sum_{t\in\mathbb{F}_q^\times}(\zeta_{a,j,t})_U + \sum_{i\prec b\prec j}\sum_{t'\in\mathbb{F}_q^\times}(\zeta_{i,b,t'})_U + \sum_{i\prec a,b\prec j}\sum_{t,t'\in\mathbb{F}_q^\times}(\zeta_{a,j,t})_U(\zeta_{i,b,t'})_U,$$

and thus the result follows by the same reason.

Next we assume that $U=\mathrm{Sp}_{2n}(q)$ and $l=-k$. Since $\{\alpha,\beta\}$ is not basic, neither is the subset $\{(i,j),(k,-k)\}$. Recall that $\mathscr{E}(\{\alpha,\beta\})=\{(i,j),(-j,-i),(k,-k)\}$. We start by considering the case where $i\neq k$ and $j=-k$. By [André 1995a, Lemma 6], we obtain

$$\xi_{\alpha,r}(\zeta_{k,-k,s})_U = \xi_{\alpha,r} + \sum_{k\prec b\prec -k}\sum_{t\in\mathbb{F}_q^\times}\xi_{\alpha,r}(\zeta_{k,b,t})_U.$$

Since $\xi_{\alpha,r}\xi_{\beta,s}$ is a constituent of $\xi_{\alpha,r}(\zeta_{k,-k,s})_U$ (by Lemma 2.4), it is a sum of some of the irreducible constituents of the characters $\xi_{\alpha,r}$ and $\xi_{\alpha,r}(\zeta_{k,b,t})_U$ for $k \prec b \prec -k$ and $t \in \mathbb{F}_q^\times$; we observe that $\xi_{\alpha,r}(\zeta_{k,b,t})_U = (\zeta_{i,-k,r})_U(\zeta_{k,b,t})_U = (\zeta_{k,-i,r})_U(\zeta_{k,b,t})_U$ is reducible (in general). Let $k \prec b \prec -k$ and $t \in \mathbb{F}_q^\times$ be arbitrary. Then by [André 1995a, Lemma 6], we obtain

$$\xi_{\alpha,r}(\zeta_{k,b,t})_U = (\zeta_{k,-i,r})_U(\zeta_{k,b,t})_U = \xi_{\alpha,r} + \sum_{k\prec a\prec b}\ \sum_{t'\in\mathbb{F}_q^\times} \xi_{\alpha,r}(\zeta_{a,b,t'})_U.$$

Using Propositions 2.2 and 2.6, it is now easy to conclude that the irreducible constituents of $\xi_{\alpha,r}(\zeta_{k,b,t})_U$ are supercharacters of U, and so the result also follows in this situation.

Now, suppose that $(i, j) = (k, -k) = (i, -i)$; hence, $\alpha = \beta$. On the one hand, suppose that $s = -r$. Then by [André 1995a, Lemma 8], $(\zeta_{i,-i,r})_U(\zeta_{i,-i,-r})_U$ decomposes as a sum of terms of the form $(\zeta_{a,-i,t})_U(\zeta_{i,b,t'})_U = (\zeta_{i,a,t})_U(\zeta_{i,b,t'})_U$ for $i \prec a, b \prec -i$ and $t, t' \in \mathbb{F}_q$; for simplicity, we set $\zeta_{u,v,0} = 1_{U_m(q)}$ for all $(u, v) \in \mathscr{E}$. By the above, each character $(\zeta_{i,a,t})_U(\zeta_{i,b,t'})_U$ decomposes as a sum of irreducible supercharacters, and thus $\xi_{\alpha,r}\xi_{\alpha,-r}$ also decomposes as a sum of irreducible supercharacters (because $\xi_{\alpha,r}\xi_{\alpha,-r}$ is a constituent of $(\zeta_{i,-i,r})_U(\zeta_{i,-i,-r})_U$).

On the other hand, suppose that $s \neq -r$. Then by [André 1995a, Lemma 11], $(\zeta_{i,-i,r})_U(\zeta_{i,-i,s})_U$ decomposes as a sum of terms of the form $(\zeta_{i,-i,r+s})_U(\zeta_{a,b,t})_U$ for $i \prec a \prec b \prec -i$ and $t \in \mathbb{F}_q$. Let $i \prec a \prec b \prec -i$ and $t \in \mathbb{F}_q^\times$; we observe that, by Proposition 2.2, we may assume that $1 \le a \le n$ and $a \prec b \preceq -a$. By Proposition 2.6, the irreducible constituents of $(\zeta_{i,-i,r+s})_U(\zeta_{a,b,t})_U$ are also irreducible constituents of characters with the form $\xi_{\alpha,r}(\zeta_{c,-c,u})_U(\zeta_{a,b,t})_U$ for some $i \prec c \preceq n$ and some $u \in \mathbb{F}_q$. Using a simple induction argument, we may assume that each character $(\zeta_{c,-c,u})_U(\zeta_{a,b,t})_U$ decomposes as a sum of irreducible supercharacters, and this clearly implies that $\xi_{\alpha,r}(\zeta_{c,-c,u})_U(\zeta_{a,b,t})_U$ also decomposes as a sum of irreducible supercharacters. The result follows because $\xi_{\alpha,r}\xi_{\alpha,s}$ is a constituent of $(\zeta_{i,-i,r})_U(\zeta_{i,-i,s})_U$.

Finally, we assume that $i = k$ and $j \prec -k = -i$ (we recall that $i \prec j \preceq -i$). In this case, [André 1995a, Lemma 6] implies that

$$\xi_{\alpha,r}(\zeta_{i,-i,s})_U = (\zeta_{i,-i,s})_U + \sum_{i\prec a\prec j}\ \sum_{t\in\mathbb{F}_q^\times} (\zeta_{i,-i,s})_U(\zeta_{a,j,t})_U.$$

As in the previous case, since $\xi_{\alpha,r}\xi_{\beta,s}$ is a constituent of $\xi_{\alpha,r}(\zeta_{i,-i,s})_U$, it is a sum of irreducible constituents of the characters $(\zeta_{i,-i,s})_U$ and $(\zeta_{i,-i,s})_U(\zeta_{a,j,t})_U$ for $i \prec a \prec j$ and $t \in \mathbb{F}_q^\times$. Using Propositions 2.2 and 2.6, we easily conclude that the irreducible constituents of $(\zeta_{i,-i,s})_U$ and $(\zeta_{i,-i,s})_U(\zeta_{a,j,t})_U$ for $i \prec a \prec j$, $a \neq -j$, and $t \in \mathbb{F}_q^\times$ are supercharacters of U. It remains to consider the irreducible constituents of $(\zeta_{i,-i,s})_U(\zeta_{-j,j,t})_U$ for $t \in \mathbb{F}_q^\times$. However, by Proposition 2.6 and by one of the cases considered previously, all these irreducible constituents are supercharacters.

The proof is complete. □

Next we prove that the product of supercharacters is a linear combination (with nonnegative integer coefficients) of supercharacters. For the (inductive) proof, we need to endow the set of roots with the total order $\preceq$ defined as follows. Given $\alpha, \beta \in \Phi$, we choose $(i, j) \in \mathscr{E}^+(\alpha)$ and $(k, l) \in \mathscr{E}^+(\beta)$, and we set $\alpha \prec \beta$ if and only if either $l \prec j$ or $j = l$ and $i \prec j$. The following observation will also be very useful (and is an immediate consequence of the previous proof).

Lemma 3.2. *Let $\alpha, \beta \in \Phi$ be roots with $\alpha \preceq \beta$, and let $r, s \in \mathbb{F}_q^\times$. Let $D \subseteq \Phi$ be a basic subset, and suppose that the supercharacter $\xi_{D,\phi}$ is a constituent of $\xi_{\alpha,r}\xi_{\beta,s}$ for some map $\phi\colon D \to \mathbb{F}_q^\times$. Let $\gamma \in D$ be the smallest root in D. Then $\alpha \preceq \gamma$, and $\alpha \neq \gamma$ if and only if $\alpha = \beta$ and $s = -r$.*

We may now proceed with the proof of the following result. We denote by $\mathrm{cf}(U)$ the unitary vector space consisting of all class functions of U, and by $\mathrm{scf}(U)$ the vector subspace of $\mathrm{cf}(U)$ spanned by all supercharacters of U. (The symbol scf is an abbreviation of "superclass function"; superclasses of U will be defined in the forthcoming paper [André and Neto 2008].)

Theorem 3.3. *The product of two supercharacters of U decomposes as a sum of supercharacters. In other words*, $\mathrm{scf}(U)$ *is a subalgebra of* $\mathrm{cf}(U)$. *Also*, $\mathrm{scf}(U)$ *is finitely generated* (*as an algebra*) *by the elementary characters of U.*

Proof. Let $D, D' \subseteq \Phi$ be nonempty basic subsets, and let $\xi_{D,\phi}$ and $\xi_{D',\phi'}$ be supercharacters of U associated with maps $\phi\colon D \to \mathbb{F}_q^\times$ and $\phi'\colon D' \to \mathbb{F}_q^\times$. Let $\alpha \in D'$ and $D'_0 = D' - \{\alpha\}$. By definition, we have $\xi_{D',\phi'} = \xi_{\alpha,r}\xi_{D'_0,\phi'_0}$, where $r = \phi'(\alpha)$ and ϕ'_0 is the restriction of ϕ' to D'_0, and thus we may use induction on $|D'|$ to conclude that $\xi_{D'_0,\phi'_0}\xi_{D,\phi}$ decomposes as a sum of supercharacters. Therefore, we are reduced to the case where $\xi_{D',\phi'} = \xi_{\alpha,r}$; in other words, we must prove that the product $\xi_{\alpha,r}\xi_{D,\phi}$ decomposes as a sum of supercharacters. To see this, we will proceed by reverse induction on the set of all basic subsets of Φ endowed with the lexicographic order $\preceq$ that is naturally determined by the total order $\preceq$ on Φ (as defined above). We observe that the maximal basic subset of Φ (with respect to this order) is $\{\varepsilon_1 - \varepsilon_2\}$.

Let D and ϕ be as above. Let $\alpha \in \Phi$ and $r \in \mathbb{F}_q^\times$ be arbitrary, and consider the product $\xi_{\alpha,r}\xi_{D,\phi}$. Let $\beta \in D$ be the smallest root in D, and let $s = \phi(\beta) \in \mathbb{F}_q^\times$. If $D = \{\beta\}$, then $\xi_{\alpha,r}\xi_{D,\phi} = \xi_{\alpha,r}\xi_{\beta,s}$ decomposes as a product of supercharacters (by Proposition 3.1). Thus we assume that $|D| \geq 2$. Let $D_0 = D - \{\beta\}$, and let $\phi_0\colon D_0 \to \mathbb{F}_q^\times$ be the restriction of ϕ to D_0.

First, suppose that $\alpha \prec \beta$. Since $D \prec D_0$, the product $\xi_{\alpha,r}\xi_{D_0,\phi_0}$ decomposes as a sum of supercharacters (by reverse induction). Let $D'' \subseteq \Phi$ be a basic subset such that $\xi_{D'',\phi''}$ is a constituent of $\xi_{\alpha,r}\xi_{D_0,\phi_0}$ for some map $\phi''\colon D'' \to \mathbb{F}_q^\times$. Since $\alpha \notin D$ (by the minimal choice of β), α is strictly smaller than all the roots in D_0. Therefore, Lemma 3.2 implies that $\alpha \in D''$, and so $D \prec D''$. By reverse induction, we conclude that the product $\xi_{\beta,s}\xi_{D'',\phi''}$ decomposes as a sum of supercharacters, and thus $\xi_{\alpha,r}\xi_{D,\phi} = \xi_{\beta,\phi(\beta)}(\xi_{\alpha,r}\xi_{D_0,\phi_0})$ also decomposes as a sum of supercharacters.

On the other hand, suppose that $\beta \prec \alpha$. As in the prior case, the product $\xi_{\alpha,r}\xi_{D_0,\phi_0}$ decomposes as a sum of supercharacters, and so we may choose a basic subset $D'' \subseteq \Phi$ such that $\xi_{D'',\phi''}$ is a constituent of $\xi_{\alpha,r}\xi_{D_0,\phi_0}$ for some map $\phi''\colon D'' \to \mathbb{F}_q^\times$. By Lemma 3.2, we see that the smallest root in $D_0 \cup \{\alpha\}$ is smaller than or equal to the smallest root in D'', and so β is strictly smaller than the smallest root in D'', which means that $D \prec D''$. Thus, as before, we conclude that the product $\xi_{\beta,s}\xi_{D'',\phi''}$ decomposes as a sum of supercharacters, and thus $\xi_{\alpha,r}\xi_{D,\phi} = \xi_{\beta,\phi(\beta)}(\xi_{\alpha,r}\xi_{D_0,\phi_0})$ also decomposes as a sum of supercharacters.

Finally, suppose that $\beta = \alpha$. In this case, we have $\xi_{\alpha,r}\xi_{D,\phi} = (\xi_{\alpha,r}\xi_{\alpha,s})\xi_{D_0,\phi_0}$. By Proposition 3.1 and Lemma 3.2, $\xi_{\alpha,r}\xi_{\alpha,s}$ decomposes as a product of supercharacters of the form $\xi_{\alpha,t}\xi_{D'',\phi''}$, where $D'' \subseteq \Phi$ is a basic subset such that α is strictly smaller than all of its roots, $\phi''\colon D'' \to \mathbb{F}_q^\times$ is a map, and $t \in \mathbb{F}_q$. For simplicity, we write $\xi_{\alpha,0} = 1_U$. By successively repeating the arguments above, we deduce that $\xi_{D'',\phi''}\xi_{D_0,\phi_0}$ decomposes as a sum of supercharacters, each one corresponding to a basic subset with smallest root larger than α. Therefore D is smaller than all of these basic subsets, and so we may use reverse induction to conclude that $\xi_{\alpha,t}\xi_{D'',\phi''}\xi_{D_0,\phi_0}$ also decomposes as a sum of supercharacters. It follows that $\xi_{\alpha,r}\xi_{D,\phi}$ decomposes as a sum of supercharacters, and this completes the proof. □

As a corollary, we obtain the following result.

Corollary 3.4. *The restriction ζ_U of any supercharacter ζ of $U_m(q)$ decomposes as a sum of supercharacters of U.*

Proof. Since ζ is a product of elementary characters of $U_m(q)$, Propositions 2.2 and 2.6 imply that ζ_U is a product of elementary characters of U, and the result follows by the previous theorem. □

We are now able to prove the existence part of Theorem 1.1.

Theorem 3.5. *Every irreducible character χ of U is a constituent of a supercharacter of U. In other words, there exists a basic subset D of Φ and a map $\phi\colon D \to \mathbb{F}_q^\times$ such that $\langle \chi, \xi_{D,\phi} \rangle \neq 0$.*

Proof. Let ψ be an irreducible character of $U_m(q)$ with $\langle \chi, \psi_U \rangle \neq 0$. Let $\mathfrak{D} \subseteq \mathfrak{E}$ be the (unique) basic subset, and let $\varphi\colon \mathfrak{D} \to \mathbb{F}_q^\times$ be the (unique) map such that ψ is a constituent of the supercharacter $\zeta = \zeta_{\mathfrak{D},\varphi}$ of $U_m(q)$. Then ψ_U is a constituent of

ζ_U, hence χ is an irreducible constituent of ζ_U. The result follows by the previous corollary. □

4. Orthogonality of supercharacters

In this section, we prove the orthogonality of supercharacters and thus complete the proof of Theorem 1.1. The proof depends on the decomposition of $\mathfrak{u}^*$ as a disjoint union of its *basic subvarieties*, as defined in [AN 2006]. We start with the definition.

We fix an arbitrary nonempty basic subset $D \subseteq \Phi$, and define the D-singular and D-regular entries as follows. For any $(i, j) \in \mathscr{E}$, we set

$$S(i, j) = \{(i, k) \in \mathscr{E} : k \prec j\} \cup \{(k, j) \in \mathscr{E} : i \prec k\},$$

and define, for any $\alpha \in \Phi$, the subsets

$$\mathscr{E}_S(\alpha) = \bigcup_{(i,j)\in\mathscr{E}(\alpha)} S(i, j) \quad \text{and} \quad \mathscr{E}_R(\alpha) = \mathscr{E} - \mathscr{E}_S(\alpha)$$

of $\mathscr{E}$. We say that an entry $(k,l) \in \mathscr{E}$ is *α-singular* if $(k,l) \in \mathscr{E}_S(\alpha)$; otherwise, we say that (k,l) is *α-regular*. More generally, given an arbitrary basic subset $\mathscr{D} \subseteq \mathscr{E}$, we define

$$S(\mathscr{D}) = \bigcup_{(i,j)\in\mathscr{D}} S(i, j) \quad \text{and} \quad R(\mathscr{D}) = \mathscr{E} - S(\mathscr{D}).$$

The entries in $S(\mathscr{D})$ are said to be *$\mathscr{D}$-singular*, and the entries in $R(\mathscr{D})$ are said to be *$\mathscr{D}$-regular*. We observe that, for any $\alpha \in \Phi$, an entry $(k,l) \in \mathscr{E}$ is α-singular if and only if it is $\mathscr{E}(\alpha)$-singular; likewise an entry $(k,l) \in \mathscr{E}$ is α-regular if and only if it is $\mathscr{E}(\alpha)$-regular. Now, since $D \subseteq \Phi$ is a basic subset, $\mathscr{E}(D) = \bigcup_{\alpha\in D} \mathscr{E}(\alpha)$ is a basic subset of $\mathscr{E}$ (by definition). We say an entry $(i, j) \in \mathscr{E}$ is *D-singular* if it is $\mathscr{E}(D)$-singular, and call it *D-regular* if it $\mathscr{E}(D)$-regular. We denote by $\mathscr{E}_S(D)$ the subset of $\mathscr{E}$ consisting of all D-singular entries, and by $\mathscr{E}_R(D)$ the subset of $\mathscr{E}$ consisting of all D-regular entries. It is clear that

$$\mathscr{E}_S(D) = \bigcup_{\alpha\in D} \mathscr{E}_S(\alpha) \quad \text{and} \quad \mathscr{E}_R(D) = \mathscr{E} - \mathscr{E}_S(D).$$

(This definition can be extended to the empty (basic) subset of Φ, in which case all entries in $\mathscr{E}$ are regular.)

For an arbitrary basic subset $\mathscr{D} \subseteq \mathscr{E}$ and an arbitrary entry $(i, j) \in \mathscr{E}$, we denote by $\mathscr{D}(i, j)$ the subset

$$\mathscr{D}(i, j) = \{(k,l) \in \mathscr{D} : 1 \preceq k \prec i,\ \ j \prec l \preceq -1\};$$

it is clear that $\mathscr{D}(i, j)$ is a basic subset of $\mathscr{E}$. Let $\mathscr{D}(i, j) = \{(i_1, j_1), \dots, (i_t, j_t)\}$ and suppose that $j_1 \prec \cdots \prec j_t$. Let $\sigma \in S_t$ be the (unique) permutation such that

$i_{\sigma(1)} \prec \cdots \prec i_{\sigma(t)}$; as usual, we denote by S_t the symmetric group of degree t. Then for any $f \in \mathfrak{u}_m(q)^*$, we define $\Delta^{\mathcal{D}}_{i,j}(f) \in \mathbb{F}_q$ to be the determinant

(4d) $$\Delta^{\mathcal{D}}_{i,j}(f) = \begin{vmatrix} f(e_{i_{\sigma(1)},j}) & f(e_{i_{\sigma(1)},j_1}) & \cdots & f(e_{i_{\sigma(1)},j_t}) \\ \vdots & \vdots & & \vdots \\ f(e_{i_{\sigma(t)},j}) & f(e_{i_{\sigma(t)},j_1}) & \cdots & f(e_{i_{\sigma(t)},j_t}) \\ f(e_{i,j}) & f(e_{i,j_1}) & \cdots & f(e_{i,j_t}) \end{vmatrix}.$$

We note that, if $\mathcal{D}(i, j)$ is empty, then $\Delta^{\mathcal{D}}_{i,j}(f) = f(e_{i,j})$; in particular, if $\mathcal{D}$ is empty, then $\Delta^{\mathcal{D}}_{i,j}(f) = f(e_{i,j})$ for all $(i, j) \in \mathcal{E}$.

Now, for any $f \in \mathfrak{u}^*$, we define the element $u(f) \in \mathfrak{u}$ by

$$u(f) = \sum_{\alpha \in \Phi} u(f)_\alpha e_\alpha,$$

where, for each $\alpha \in \Phi$, we set

$$u(f)_\alpha = \begin{cases} \frac{1}{2} f(e_\alpha) & \text{if } \alpha = \varepsilon_i \pm \varepsilon_j \text{ for } 1 \le i < j \le n, \\ f(e_\alpha) & \text{if } \mathfrak{u} \le \mathfrak{sp}_{2n}(q) \text{ and } \alpha = 2\varepsilon_i \text{ for } 1 \le i \le n, \\ \frac{1}{2} f(e_\alpha) & \text{if } \mathfrak{u} \le \mathfrak{o}_{2n+1}(q) \text{ and } \alpha = \varepsilon_i \text{ for } 1 \le i \le n. \end{cases}$$

It is easy to see that $f(v) = \mathrm{Tr}(u(f)^T v)$ for all $v \in \mathfrak{u}$, and that the map $f \mapsto u(f)$ defines a vector space isomorphism from $\mathfrak{u}^*$ to $\mathfrak{u}$. Finally we define $\hat{f} \in \mathfrak{u}_m(q)^*$ by

$$\hat{f}(v) = \mathrm{Tr}(u(f)^T v) \quad \text{for all } v \in \mathfrak{u}_m(q).$$

Then for any basic subset $D \subseteq \Phi$ and any entry $(i, j) \in \mathcal{E}$, we set

$$\Delta^{D}_{i,j}(f) = \Delta^{\mathcal{E}(D)}_{i,j}(\hat{f}) \quad \text{for all } f \in \mathfrak{u},$$

and, for any map $\phi\colon D \to \mathbb{F}_q^\times$, we define the *basic subvariety*

$$O^*_{D,\phi} = \{f \in \mathfrak{u}^* \colon \Delta^{D}_{i,j}(f) = \Delta^{D}_{i,j}(f_{D,\phi}) \text{ for all } (i, j) \in \mathcal{E}_R(D)\},$$

where

(4e) $$f_{D,\phi} = \sum_{\alpha \in D} \phi(\alpha) e^*_\alpha \in \mathfrak{u}^*.$$

The following result is [AN 2006, Theorem 4.5] (the proof given there is valid for an arbitrary odd prime).

Theorem 4.1. *For any basic subset $D \subseteq \Phi$ and any map $\phi\colon D \to \mathbb{F}_q^\times$, the basic subvariety $O^*_{D,\phi} \subseteq \mathfrak{u}^*$ is U-invariant (for the usual coadjoint action). Moreover, the vector space $\mathfrak{u}^*$ decomposes as the disjoint union $\mathfrak{u}^* = \bigcup_{D,\phi} O^*_{D,\phi}$ of all its basic subvarieties.*

As a particular case, let $\alpha \in \Phi$ and $r \in \mathbb{F}_q^\times$. Then for $D = \{\alpha\}$ and $\phi\colon D \to \mathbb{F}_q^\times$ defined by $\phi(\alpha) = r$, we obtain the *elementary subvariety* $\mathcal{O}^*_{\alpha,r} = \mathcal{O}^*_{D,\phi}$. By [AN 2006, Theorem 5.5], we have

$$\mathcal{O}^*_{D,\phi} = \sum_{\alpha \in D} \mathcal{O}^*_{\alpha,\phi(\alpha)} \tag{4f}$$

for any basic subset $D \subseteq \Phi$ and any map $\phi\colon D \to \mathbb{F}_q^\times$. The elementary subvarieties of $\mathfrak{u}^*$ determine the elementary supercharacters of U (and vice versa) as shown by the formula of Corollary 3.4 below. The following observation will be useful for the proof.

Let D be a basic subset of Φ, and let $\phi\colon D \to \mathbb{F}_q^\times$ be a map. Let $f_{D,\phi} \in \mathfrak{u}^*$ be defined as in (4e), and write $\hat{f}_{D,\phi} = \widehat{f_{D,\phi}} \in \mathfrak{u}_m(q)^*$. By definition, for any $f \in \mathfrak{u}^*$,

$$f \in \mathcal{O}^*_{D,\phi} \text{ if and only if } \Delta^{\mathscr{E}(D)}_{i,j}(\hat{f}) = \Delta^{\mathscr{E}(D)}_{i,j}(\hat{f}_{D,\phi}) \quad \text{for all } (i,j) \in \mathscr{E}_R(D).$$

Henceforth, we denote by φ_D the map

$$\varphi_D\colon \mathscr{E}(D) \to \mathbb{F}_q^\times, \quad (i,j) \mapsto \hat{f}_{D,\phi}(e_{i,j}) \quad \text{for all } (i,j) \in \mathscr{E}(D).$$

Let $\mathcal{O}^*_{\mathscr{E}(D),\varphi_D} = U_m(q)\hat{f}_{D,\phi}U_m(q) \subseteq \mathfrak{u}_m(q)^*$. By [André 1995b, Propositions 1 and 2] (see also the discussion in [Diaconis and Isaacs 2008, Appendix 2]), we know that

$$\mathcal{O}^*_{\mathscr{E}(D),\varphi_D} = \{f \in \mathfrak{u}_m(q)^*\colon \Delta^{\mathscr{D}}_{i,j}(f) = \Delta^{\mathscr{D}}_{i,j}(\hat{f}_{D,\phi}) \text{ for all } (i,j) \in \mathscr{E}_R(D)\}, \tag{4g}$$

and thus

$$\mathcal{O}^*_{D,\phi} = \{f \in \mathfrak{u}^*\colon \hat{f} \in \mathcal{O}^*_{\mathscr{E}(D),\varphi_D}\}.$$

In particular, let $\alpha \in \Phi$, $(i,j) \in \mathscr{E}^+(\alpha)$ and $r \in \mathbb{F}_q^\times$ be arbitrary. Then for $D = \{\alpha\}$ and $\phi\colon D \to \mathbb{F}_q^\times$ defined by $\phi(\alpha) = r$, we have

$$f_{D,\phi} = re^*_\alpha \quad \text{and} \quad \hat{f}_{D,\phi} = (r/2)(e^*_{i,j} \pm e^*_{-j,-i})$$

(where the sign is well determined by $\mathfrak{u}$). By [André 1995b, Proposition 1 and 2], we know that $\mathcal{O}^*_{\mathscr{E}(\alpha),\varphi_\alpha} = \mathcal{O}^*_{i,j,r/2} + \mathcal{O}^*_{-j,-i,\pm r/2}$ where $\varphi_\alpha = \varphi_D = \varphi_{\{\alpha\}}$, and thus

$$\mathcal{O}^*_{\alpha,r} = \{f \in \mathfrak{u}^*\colon \hat{f} \in \mathcal{O}^*_{i,j,r/2} + \mathcal{O}^*_{-j,-i,\pm r/2}\}. \tag{4h}$$

We are now able to proceed with the proof of the following result.

Proposition 4.2. *Let $\alpha \in \Phi$ and let $r \in \mathbb{F}_q^\times$. For any $z \in U$, we denote by a_z the element of $\mathfrak{u}$ given by Lemma 2.3. Then*

$$\xi_{\alpha,r}(z) = \frac{\xi_{\alpha,r}(1)}{|\mathcal{O}^*_{\alpha,r}|} \sum_{f \in \mathcal{O}^*_{\alpha,r}} \vartheta_f(a_z) \quad \textit{for all } z \in U.$$

Proof. Let $(i,j)\in\mathscr{E}^+(\alpha)$. First we consider the case $j\neq -i$. By Proposition 2.6, we have $\xi_{\alpha,r}=(\zeta_{i,j,r})_U$. Let $O^*_{i,j,r}=U_m(q)(re^*_{i,j})U_m(q)\subseteq\mathfrak{u}_m(q)^*$. Then by Lemma 2.3 and by [Diaconis and Isaacs 2008, Corollary 5.11], we deduce that

$$\xi_{\alpha,r}(z)=\zeta_{i,j,r}(z)=\zeta_{i,j,r}(1+a_z)=\frac{1}{\sqrt{|O^*_{i,j,r}|}}\sum_{f\in O^*_{i,j,r}}\vartheta_f(u_z)\quad\text{for all } z\in U.$$

Let $f\in O^*_{i,j,r}$ be arbitrary, and consider the restriction $f_\mathfrak{u}$ of f to $\mathfrak{u}$. As above, define $u(f_\mathfrak{u})\in\mathfrak{u}$ and $\hat{f}=\widehat{f_\mathfrak{u}}\in\mathfrak{u}_m(q)^*$; hence

$$\hat{f}(v)=\operatorname{Tr}(u(f_\mathfrak{u})^Tv)\quad\text{for all } v\in\mathfrak{u}_m(q).$$

Let $\varphi\colon\mathscr{E}(\alpha)\to\mathbb{F}_q^\times$ be the map defined by $\varphi(i,j)=u(f)_{i,j}=u(f)_\alpha=r/2$ and $\varphi(-j,-i)=u(f)_{-j,-i}=\pm r/2$. Using (4g), it is straightforward to check that $\hat{f}\in O^*_{i,j,r/2}+O^*_{-j,-i,\pm r/2}$, and hence $f_\mathfrak{u}\in O^*_{\alpha,r}$, by (4h). Since the map $f\mapsto f_\mathfrak{u}$ is clearly an injection map from $O^*_{i,j,r}$ to $\mathfrak{u}$ and since $|O^*_{\alpha,r}|=|O^*_{i,j,r}|$ (by direct computation), we conclude that $O^*_{\alpha,r}=\{f_\mathfrak{u}\colon f\in O^*_{i,j,r}\}$. The result follows because $\xi_{\alpha,r}(1)=\sqrt{|O^*_{\alpha,r}|}$.

On the other hand, suppose that $U\leq\mathrm{Sp}_{2n}(q)$ and $\alpha=2\varepsilon_i$ for some $1\leq i\leq n$. In this case, by [AN 2006, Proposition 3.1 and Theorem 5.5], $O^*_{\alpha,r}\subseteq\mathfrak{u}^*$ is the coadjoint U-orbit that contains re^*_α. Let $z\in U$ be fixed. By the definition of induced character, we have

$$\xi_{\alpha,r}(z)=(\lambda_{\alpha,r})^U(z)=\frac{1}{|U_\alpha|}\sum_{\substack{x\in U\\ xzx^{-1}\in U_\alpha}}\lambda_{\alpha,r}(xzx^{-1}).$$

Since $\lambda_{\alpha,r}(xzx^{-1})=\lambda_{\alpha,r}(xa_zx^{-1})$ for all $x\in U$ with $xzx^{-1}\in U_\alpha$, we deduce that

$$\begin{aligned}\xi_{\alpha,r}(z)&=\frac{1}{|U_\alpha|}\sum_{\substack{x\in U\\ xzx^{-1}\in U_\alpha}}\vartheta_{re^*_\alpha}(xa_zx^{-1})\\&=\frac{1}{|U_\alpha|}\sum_{x\in U}\vartheta_{re^*_\alpha}(xa_zx^{-1})\Big(\frac{1}{|\mathfrak{u}:\mathfrak{u}_\alpha|}\sum_{g\in(\mathfrak{u}_\alpha)^\perp}\vartheta_g(xa_zx^{-1})\Big)\\&=\frac{1}{|U|}\sum_{g\in(\mathfrak{u}_\alpha)^\perp}\sum_{x\in U}\vartheta_{re^*_\alpha+g}(xa_zx^{-1})=\frac{1}{|U|}\sum_{h\in re^*_\alpha+(\mathfrak{u}_\alpha)^\perp}\sum_{x\in U}\vartheta_{x\cdot h}(a_z).\end{aligned}$$

Now, it is straightforward to check that $re^*_\alpha+(\mathfrak{u}_\alpha)^\perp\subseteq O^*_{\alpha,r}$, and so

$$\sum_{x\in U}\vartheta_{x\cdot h}(a_z)=|C_U(re^*_\alpha)|\sum_{f\in O^*_{\alpha,r}}\vartheta_f(a_z)\quad\text{for all } h\in re^*_\alpha+(\mathfrak{u}_\alpha)^\perp;$$

as usual, $C_U(re_\alpha^*)$ denotes the centralizer of re_α^* under the coadjoint action of U. It follows that

$$\xi_{\alpha,r}(z) = \frac{|C_U(re_\alpha^*)|\,|U : U_\alpha|}{|U|} \sum_{f \in O_{\alpha,r}^*} \vartheta_f(a_z) = \frac{|U : U_\alpha|}{|O_{\alpha,r}^*|} \sum_{f \in O_{\alpha,r}^*} \vartheta_f(a_z).$$

The result follows because $\xi_{\alpha,r}(1) = |U : U_\alpha|$ (by definition). □

Remark 4.3. We observe that, by [AN 2006, Proposition 2.1], a basic subvariety $O_{\alpha,r}^*$ for $\alpha \in \Phi$ and $r \in \mathbb{F}_q^\times$ is a coadjoint U-orbit in all cases, except when U is orthogonal and $\alpha = \varepsilon_i + \varepsilon_j$ for some $1 \le i, j \le n$. In this case, by [AN 2006, Theorem 5.5], we have

$$O_{\alpha,r}^* = \bigcup_{s \in \mathbb{F}_q} O_s,$$

where $O_s = O(re_\alpha^* + se_\beta^*)$ with $\beta = \varepsilon_i - \varepsilon_j$ denotes the coadjoint U-orbit that contains $re_\alpha^* + se_\beta^* \in \mathfrak{u}^*$. At the same time, an argument similar to the one above shows that, for any $s \in \mathbb{F}_q$, the expression

$$\chi_s(z) = \frac{\chi_s(1)}{|O_s|} \sum_{f \in O_s} \vartheta_f(a_z) \quad \text{for all } z \in U,$$

defines an irreducible character of U. In fact, we may consider the subgroup

$$V = \{z \in U : a_z \in \mathfrak{u}_\alpha + \mathbb{F}_q e_\beta\}$$

of U, and define the linear character $\mu_s\colon V \to \mathbb{C}^\times$ by $\mu_s(z) = \vartheta(rz_{i,-j} + sz_{i,j})$ for all $z \in V$. Then we may show that $\chi_s = (\mu_s)^U$ for all $s \in \mathbb{F}_q$, and that the decomposition of $\xi_{\alpha,r}$ into q distinct irreducible constituents is $\xi_{\alpha,r} = \sum_{s \in \mathbb{F}_q} \chi_s$; see [AN 2006, Proposition 2.1].

Next, we prove the orthogonality of supercharacters, thus concluding the proof of Theorem 1.1.

Theorem 4.4. *Let D and D' be basic subsets of Φ, and let $\phi\colon D \to \mathbb{F}_q^\times$ and $\phi'\colon D' \to \mathbb{F}_q^\times$ be maps. Then $\langle \xi_{D,\phi}, \xi_{D',\phi'} \rangle \neq 0$ if and only if $(D,\phi) = (D',\phi')$.*

Proof. Let $z \in U$ be arbitrary, and let $a_z \in \mathfrak{u}$ be the element given by Lemma 2.3. By definition, we have $\xi_{D,\phi} = \prod_{\alpha \in D} \xi_{\alpha,\phi(\alpha)}$, and so (by the previous proposition)

$$\xi_{D,\phi}(z) = \frac{\xi_{D,\phi}(1)}{|\Omega_{D,\phi}^*|} \sum_{(f_1,\dots,f_d) \in \Omega_{D,\phi}^*} \vartheta_{f_1}(a_z) \cdots \vartheta_{f_d}(a_z) = \frac{\xi_{D,\phi}(1)}{|\Omega_{D,\phi}^*|} \sum_{f \in O_{D,\phi}^*} m_f \vartheta_f(a_z),$$

where $d = |D|$, $\Omega_{D,\phi}^* = \prod_{\alpha \in D} O_{\alpha,\phi(\alpha)}^*$, and

$$m_f = \left|\{(f_1,\dots,f_d) \in \Omega_{D,\phi}^* : f_1 + \cdots + f_d = f\}\right| \quad \text{for all } f \in O_{D,\phi}^*.$$

We recall from (4f) that $O^*_{D,\phi} = \sum_{\alpha \in D} O^*_{\alpha,\phi(\alpha)}$. Similarly,

$$\xi_{D',\phi'}(z) = \frac{\xi_{D',\phi'}(1)}{|\Omega^*_{D',\phi'}|} \sum_{g \in O^*_{D',\phi'}} m'_g \vartheta_g(a_z)$$

where $\Omega^*_{D',\phi'} = \prod_{\beta \in D'} O^*_{\beta,\phi(\beta)}$, and

$$m'_g = \left|\{(g_1, \ldots, g_{d'}) \in \Omega^*_{D',\phi'} \colon g_1 + \cdots + g_{d'} = g\}\right| \quad \text{for all } g \in O^*_{D',\phi'}.$$

Here, $d' = |D'|$. Since the mapping $z \mapsto a_z$ is a bijection $U \to \mathfrak{u}$, we deduce that

$$\begin{aligned}
\langle \xi_{D,\phi}, \xi_{D',\phi'} \rangle &= \frac{\xi_{D,\phi}(1)\xi_{D',\phi'}(1)}{|\Omega^*_{D,\phi}|\,|\Omega^*_{D',\phi'}|} \sum_{f \in O^*_{D,\phi}} \sum_{g \in O^*_{D',\phi'}} \left(\frac{1}{|U|} \sum_{z \in U} \vartheta_f(a_z)\overline{\vartheta_g(a_z)} \right) \\
&= \frac{\xi_{D,\phi}(1)\xi_{D',\phi'}(1)}{|\Omega^*_{D,\phi}|\,|\Omega^*_{D',\phi'}|} \sum_{f \in O^*_{D,\phi}} \sum_{g \in O^*_{D',\phi'}} \langle \vartheta_f, \vartheta_g \rangle_{\mathfrak{u}} \\
&= \frac{\xi_{D,\phi}(1)\xi_{D',\phi'}(1)}{|\Omega^*_{D,\phi}|\,|\Omega^*_{D',\phi'}|} \left| O^*_{D,\phi} \cap O^*_{D',\phi'} \right|,
\end{aligned}$$

and the result follows by [AN 2006, Theorem 4.5]. □

5. A supercharacter formula

In this section, we establish a formula for the values of a supercharacter $\xi_{D,\phi}$ as a sum over the basic subvariety $O^*_{D,\phi} \subseteq \mathfrak{u}^*$ (which extends Proposition 4.2). In fact, we have the following result.

Theorem 5.1. *Let D be a basic subset of Φ, and let $\phi \colon D \to \mathbb{F}_q^\times$ be a map. For any $z \in U$, we denote by a_z the element of $\mathfrak{u}$ given by Lemma 2.3. Then*

$$\xi_{D,\phi}(z) = \frac{\xi_{D,\phi}(1)}{|O^*_{D,\phi}|} \sum_{f \in O^*_{D,\phi}} \vartheta_f(a_z) \quad \textit{for all } z \in U.$$

Proof. Let $z \in U$ be arbitrary. As in the previous proof, we have

$$\xi_{D,\phi}(z) = \frac{\xi_{D,\phi}(1)}{|\Omega^*_{D,\phi}|} \sum_{f \in O^*_{D,\phi}} m_f \vartheta_f(a_z),$$

where

$$\begin{aligned}
\Omega^*_{D,\phi} &= \prod_{\alpha \in D} O^*_{\alpha,\phi(\alpha)}, \\
m_f &= \left|\{(f_\alpha)_{\alpha \in D} \in \Omega^*_{D,\phi} \colon \textstyle\sum_{\alpha \in D} f_\alpha = f\}\right| \quad \text{for all } f \in O^*_{D,\phi}.
\end{aligned}$$

Now, let $\mathfrak{D} = \mathscr{E}^+(D)$, let $\varphi : \mathfrak{D} \to \mathbb{F}_q^\times$ be the map defined by $\varphi(i, j) = \phi(\alpha)$ for all $(i, j) \in \mathfrak{D}$ with $(i, j) \in \mathscr{E}(\alpha)$, and consider the supercharacter $\zeta_{\mathfrak{D},\varphi}$ of $U_m(q)$.

By Lemma 2.3 and [Diaconis and Isaacs 2008, Theorem 5.6], we have

$$\zeta_{\mathscr{D},\varphi}(z)=\zeta_{\mathscr{D},\varphi}(1+a_z)=\frac{\zeta_{\mathscr{D},\varphi}(1)}{|O^*_{D,\phi}|}\sum_{f\in O^*_{\mathscr{D},\varphi}}\vartheta_f(a_z).$$

Let $\pi:\mathfrak{u}_m(q)^*\to\mathfrak{u}^*$ be the natural projection (given by restriction of functions). Since π clearly defines an injective map $\pi: O^*_{\mathscr{D},\varphi}\to\mathfrak{u}^*$, we obtain

$$\zeta_{\mathscr{D},\varphi}(z)=\frac{\zeta_{\mathscr{D},\varphi}(1)}{|O^*_{\mathscr{D},\varphi}|}\sum_{f\in\pi(O^*_{\mathscr{D},\varphi})}\vartheta_f(a_z).$$

It is straightforward to check that $O^*_{D,\phi}\subseteq\pi_{\mathfrak{u}}(O^*_{\mathscr{D},\varphi})$; in fact, $\pi(O^*_{i,j,r})\subseteq O^*_{\alpha,r}$ for all $\alpha\in\Phi$, all $(i,j)\in\mathscr{E}(\alpha)$ and all $r\in\mathbb{F}_q^\times$ (the equality holds whenever $j\neq -i$; see the proof of Proposition 4.2). The claim follows because $O^*_{D,\phi}=\sum_{\alpha\in D}O^*_{\alpha,\phi(\alpha)}$, by [AN 2006, Theorem 5.5]. Since $\pi(O^*_{\mathscr{D},\varphi})$ and $O^*_{D,\phi}$ are U-invariant, we conclude that $\pi_{\mathfrak{u}}(O^*_{\mathscr{D},\varphi})$ decomposes as the disjoint union

$$\pi_{\mathfrak{u}}(O^*_{\mathscr{D},\varphi})=O^*_{D,\phi}\cup\mathscr{V}$$

for some U-invariant subset of $\mathscr{V}\subseteq\mathfrak{u}^*$. Therefore, we get

$$\zeta_{\mathscr{D},\varphi}(z)=\frac{\zeta_{\mathscr{D},\varphi}(1)}{|O^*_{\mathscr{D},\varphi}|}\Bigl(\sum_{f\in O^*_{D,\phi}}\vartheta_f(a_z)+\sum_{f\in\mathscr{V}}\vartheta_f(a_z)\Bigr).$$

On the other hand, by Proposition 3.1 and Theorem 1.1, we know that

$$(\zeta_{\mathscr{D},\varphi})_U=m_{D,\phi}\xi_{D,\phi}+\eta,$$

where η is a linear combination (with nonnegative integer coefficients) of supercharacters satisfying $\langle\xi_{D,\phi},\eta\rangle=0$. Arguing as in the proof of Theorem 4.1, we obtain $\eta(z)=\sum_{f\in\mathscr{V}'}n_f\vartheta_f(a_z)$ for some subset $\mathscr{V}'\subseteq\mathfrak{u}^*$ and some positive integers n_f for $f\in\mathscr{V}'$. Therefore, we get

$$\zeta_{\mathscr{D},\varphi}(z)=m_{D,\phi}\xi_{D,\phi}(z)+\eta(z)=\frac{m_{D,\phi}\xi_{D,\phi}(1)}{|\Omega^*_{D,\phi}|}\sum_{f\in O^*_{D,\phi}}m_f\vartheta_f(a_z)+\sum_{f\in\mathscr{V}'}n_f\vartheta_f(a_z).$$

Since $z\in U$ is arbitrary and the map $z\mapsto a_z$ defines a bijection, we conclude that

$$\frac{\zeta_{\mathscr{D},\varphi}(1)}{|O^*_{\mathscr{D},\varphi}|}\Bigl(\sum_{f\in O^*_{D,\phi}}\vartheta_f(a)+\sum_{f\in\mathscr{V}}\vartheta_f(a)\Bigr)=\frac{m_{D,\phi}\xi_{D,\phi}(1)}{|\Omega^*_{D,\phi}|}\sum_{f\in O^*_{D,\phi}}m_f\vartheta_f(a)+\sum_{f\in\mathscr{V}'}n_f\vartheta_f(a)$$

for all $a\in\mathfrak{u}$, and hence

$$\frac{\zeta_{\mathscr{D},\varphi}(1)}{|O^*_{\mathscr{D},\varphi}|}\Bigl(\sum_{f\in O^*_{D,\phi}}\vartheta_f+\sum_{f\in\mathscr{V}}\vartheta_f\Bigr)=\frac{m_{D,\phi}\xi_{D,\phi}(1)}{|\Omega^*_{D,\phi}|}\sum_{f\in O^*_{D,\phi}}m_f\vartheta_f+\sum_{f\in\mathscr{V}'}n_f\vartheta_f$$

(as linear characters of the abelian group $\mathfrak{u}^+$). Since $O^*_{D,\phi} \cap \mathcal{V} = O^*_{D,\phi} \cap \mathcal{V}' = \varnothing$, we deduce that

$$\frac{\zeta_{\mathfrak{D},\varphi}(1)}{|O^*_{\mathfrak{D},\varphi}|} = \frac{m_{D,\phi}\xi_{D,\phi}(1)m_f}{|\Omega^*_{D,\phi}|} \quad \text{for all } f \in O^*_{D,\phi}.$$

Therefore, the coefficients m_f do not depend on $f \in O^*_{D,\phi}$, and thus, for a well-determined positive integer m, we have

$$\xi_{D,\phi}(z) = \frac{\xi_{D,\phi}(1)m}{|\Omega^*_{D,\phi}|} \sum_{f \in O^*_{D,\phi}} \vartheta_f(a_z).$$

Taking degrees, we obtain $m = |\Omega^*_{D,\phi}|/|O^*_{D,\phi}|$, and so

$$\xi_{D,\phi}(z) = \frac{\xi_{D,\phi}(1)}{|O^*_{D,\phi}|} \sum_{f \in O^*_{D,\phi}} \vartheta_f(a_z). \qquad \square$$

As an immediate consequence, we obtain the following result.

Corollary 5.2. *Let $D \subseteq \Phi$ be a basic subset, and let $\phi\colon D \to \mathbb{F}_q^\times$ be a map. Then $\langle \xi_{D,\phi}, \xi_{D,\phi}\rangle = \xi_{D,\phi}(1)^2/|O^*_{D,\phi}|$; hence, $|O^*_{D,\phi}| = \xi_{D,\phi}(1)^2/\langle \xi_{D,\phi}, \xi_{D,\phi}\rangle$.*

Proof. Using the formula of the previous theorem, we evaluate

$$\langle \xi_{D,\phi}, \xi_{D,\phi}\rangle = \frac{1}{|U|}\sum_{z\in U} \xi_{D,\phi}(z)\overline{\xi_{D,\phi}(z)} = \frac{\xi_{D,\phi}(1)^2}{|O^*_{D,\phi}|^2} \sum_{f,g \in O^*_{D,\phi}} \langle \vartheta_f, \vartheta_g\rangle_{\mathfrak{u}} = \frac{\xi_{D,\phi}(1)^2}{|O^*_{D,\phi}|},$$

as required. $\square$

Finally, we obtain the following decomposition of the regular character of U.

Theorem 5.3. *Let ρ be the regular character of U. Then*

$$\rho = \sum_{D,\phi} \frac{\xi_{D,\phi}(1)}{\langle \xi_{D,\phi}, \xi_{D,\phi}\rangle} \xi_{D,\phi},$$

where the sum is over all basic subsets $D \subseteq \Phi$ and all maps $\phi\colon D \to \mathbb{F}_q^\times$.

Proof. Let $z \in U$ be arbitrary. Then

$$\begin{aligned}\sum_{D,\phi} \frac{\xi_{D,\phi}(1)}{\langle \xi_{D,\phi}, \xi_{D,\phi}\rangle} \xi_{D,\phi}(z) &= \sum_{D,\phi} \frac{\xi_{D,\phi}(1)}{\langle \xi_{D,\phi}, \xi_{D,\phi}\rangle}\Bigl(\frac{\xi_{D,\phi}(1)}{|O^*_{D,\phi}|} \sum_{f \in O^*_{D,\phi}} \vartheta_f(a_z)\Bigr) \\ &= \frac{\xi_{D,\phi}(1)^2}{\langle \xi_{D,\phi}, \xi_{D,\phi}\rangle |O^*_{D,\phi}|} \sum_{D,\phi}\sum_{f \in O^*_{D,\phi}} \vartheta_f(a_z) \\ &= \sum_{D,\phi}\sum_{f \in O^*_{D,\phi}} \vartheta_f(a_z).\end{aligned}$$

Since $\mathfrak{u}^*$ is the disjoint union $\mathfrak{u}^* = \bigcup_{D,\phi} O^*_{D,\phi}$, we obtain

$$\sum_{D,\phi} \sum_{f \in O^*_{D,\phi}} \vartheta_f(a_z) = \sum_{f \in \mathfrak{u}^*} \vartheta_f(a_z) = \delta_{a_z,0}|\mathfrak{u}| = \delta_{z,1}|U|,$$

and the result follows. □

6. Irreducible characters of maximum degree

As a final remark, we observe that the description of the irreducible characters of maximum degree of U as given in [AN 2006, Section 6] remains valid for arbitrary odd primes. The proofs given there can be adapted (and simplified) using the results of the present paper and also some properties of the Kirillov functions associated with coadjoint U-orbits. Given an arbitrary U-orbit $O \subseteq \mathfrak{u}^*$, we define the *Kirillov function* $\phi_O \colon U \to \mathbb{C}$ by the rule

$$\phi_O(z) = \frac{1}{\sqrt{|O|}} \sum_{f \in O} \vartheta_f(a_z) \quad \text{for all } z \in U$$

(see [Diaconis and Isaacs 2008, Section 5] for the similar definition in the case of finite algebra groups). In fact, it can be shown that every irreducible character of maximum degree is precisely the Kirillov function associated with a (unique) coadjoint U-orbit of maximum cardinality. We should mention that similar results have been obtained recently by J. Sangroniz [2008], where the author uses Kirillov's method of coadjoint orbits and shows that, for sufficiently large orbits, the associated Kirillov functions are in fact irreducible characters. In this section, we shall use Sangroniz's results to resume the description given in [AN 2006].

We start by considering the symplectic case $U \le \mathrm{Sp}_{2n}(q)$. Let

$$\Gamma = \{2\varepsilon_i : 1 \le i \le n\} \cup \{\varepsilon_i + \varepsilon_{i+1} : 1 \le i < n\} \subseteq \Phi.$$

Then for any basic subset $D \subseteq \Gamma$ and any map $\phi \colon D \to \mathbb{F}_q^\times$, the supercharacter $\xi_{D,\phi}$ is irreducible (by Corollary 5.2). In particular, if either D or $D \cup \{2\varepsilon_n\}$ is a maximal basic subset of Γ, then $\xi_{D,\phi}$ is irreducible and has maximum degree $q^{n(n-1)/2}$ (see the proof of [AN 2006, Proposition 6.3]). On the other hand, it is easy to see that the number d_n of all these pairs (D,ϕ) can be computed by the "Fibonacci" recurrence relation

$$\begin{cases} d_1 = q, \\ d_2 = q^2 - 1, \\ d_n = (q-1)(d_{n-1} + d_{n-2}) \quad \text{for } n \ge 3. \end{cases}$$

Therefore, by [Sangroniz 2008, Theorem 12], we obtain the following result.

Theorem 6.1. *Let χ be an irreducible character of $U \leq \mathrm{Sp}_{2n}(q)$. Then χ has maximum degree if and only if $\chi = \xi_{D,\phi}$, where either D or $D \cup \{2\varepsilon_n\}$ is a maximal basic subset of Γ and $\phi\colon D \to \mathbb{F}_q^\times$ is any map.*

Next, we consider the even orthogonal case $U \leq \mathrm{O}_{2n}(q)$. Let

$$\Gamma = \{\varepsilon_i + \varepsilon_{i+1} : 1 \leq i < n\},$$

$D \subseteq \Gamma$ be a basic subset, and $\phi\colon D \to \mathbb{F}_q^\times$ be a map. Then by Corollary 5.2, we easily conclude that $\langle \xi_{D,\phi}, \xi_{D,\phi} \rangle = q^{|D|}$, and a repetition of the proof of [AN 2006, Proposition 6.5] shows that $\xi_{D,\phi}$ is multiplicity free; hence, it has $q^{|D|}$ irreducible constituents, each with degree equal to $q^{-|D|}\xi_{D,\phi}(1)$. In particular, for

$$D = \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \ldots, \varepsilon_{2r-1} + \varepsilon_{2r}\},$$

where $r = \lfloor n \rfloor$, the supercharacter $\xi_{D,\phi}$ has q^r (distinct) irreducible constituents, each with degree equal to $q^{f(n)}$, where

$$f(n) = \begin{cases} n(n-2)/2 & \text{if } n \text{ is even,} \\ (n-1)^2/2 & \text{if } n \text{ is odd.} \end{cases}$$

On the other hand, if $n = 2r$ is even and

$$D = \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \ldots, \varepsilon_{2r-3} + \varepsilon_{2r-2}\} \subseteq \Gamma,$$

the supercharacter $\xi_{D,\phi}$ has q^{r-1} (distinct) irreducible constituents, each with degree equal to $q^{n(n-2)/2}$. Therefore, for the basic subset

$$D = \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \ldots, \varepsilon_{2r-3} + \varepsilon_{2r-2}\} \cup \{\varepsilon_{2r-1} - \varepsilon_{2r}\} \subseteq \Phi$$

and any map $\phi\colon D \to \mathbb{F}_q^\times$, the supercharacter $\xi_{D,\phi}$ also has q^{r-1} (distinct) irreducible constituents, each with degree equal to $q^{n(n-2)/2}$. Now, by Theorem 1.1, we may repeat the proof of [AN 2006, Proposition 6.6] to conclude that $q^{f(n)}$ is the maximum degree of an irreducible character of U, and thus we have obtained d_n irreducible characters of maximum degree, where

$$d_n = \begin{cases} q^{(n+2)/2}(q-1)^{(n-2)/2} & \text{if } n \text{ is even,} \\ q^{(n-1)/2}(q-1)^{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

Using [Sangroniz 2008, Theorem 13], we conclude the proof of the following result.

Theorem 6.2. *Suppose that $U \leq \mathrm{O}_{2n}(q)$, and let χ be an irreducible character of U. Let $D \subseteq \Phi$ be the (unique) basic subset and $\phi\colon D \to \mathbb{F}_q^\times$ the (unique) map such that $\langle \chi, \xi_{D,\phi} \rangle \neq 0$.*

- *If n is even, then χ has maximum degree if and only if*

$$D = \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \ldots, \varepsilon_{n-3} + \varepsilon_{n-2}\} \cup D_1,$$

where $D_1 \subsetneq \{\varepsilon_{n-1} - \varepsilon_n, \varepsilon_{n-1} + \varepsilon_n\}$.

- *If* n *is odd, then* χ *has maximum degree if and only if*

$$D = \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \dots, \varepsilon_{n-1} + \varepsilon_n\}.$$

Finally, we consider the odd orthogonal case $U \leq \mathrm{O}_{2n+1}(q)$. Let

$$\Gamma = \{\varepsilon_i + \varepsilon_{i+1} \colon 1 \leq i < n\},$$

let $D \subseteq \Gamma$ be a basic subset, and let $\phi \colon D \to \mathbb{F}_q^\times$ be a map. Then as in the even case, we conclude that, for

$$D = \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \dots, \varepsilon_{2r-1} + \varepsilon_{2r}\} \subseteq \Gamma,$$

where $r = \lfloor n \rfloor$, the supercharacter $\xi_{D,\phi}$ has q^r (distinct) irreducible constituents, each with degree equal to $q^{n(n-1)/2}$. On the other hand, using Corollary 5.2 (see also [AN 2006, page 423]), we conclude that, for the basic subset

$$D = \begin{cases} \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \dots, \varepsilon_{n-3} + \varepsilon_{n-2}\} \cup \{\varepsilon_{n-1}\} & \text{if } n = 2r \text{ is even,} \\ \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \dots, \varepsilon_{n-2} + \varepsilon_{n-1}\} \cup \{\varepsilon_n\} & \text{if } n = 2r+1 \text{ is odd,} \end{cases}$$

and any map $\phi \colon D \to \mathbb{F}_q^\times$, the supercharacter $\xi_{D,\phi}$ has either q^{r-1} or q^r (distinct) irreducible constituents, each with degree equal to $q^{n(n-1)/2}$. Finally, as in the even case, we conclude that $q^{n(n-1)/2}$ is the maximum degree of an irreducible character of U, and thus we have obtained d_n irreducible characters of maximum degree, where

$$d_n = \begin{cases} q^{(n-2)/2}(q+1)(q-1)^{n/2} & \text{if } n \text{ is even,} \\ q^{(n+1)/2}(q-1)^{(n-1)/2} & \text{if } n \text{ is odd.} \end{cases}$$

Using [Sangroniz 2008, Theorem 13], we conclude the proof of the following result.

Theorem 6.3. *Suppose that* $U \leq \mathrm{O}_{2n+1}(q)$, *and let* χ *be an irreducible character of* U. *Let* $D \subseteq \Phi$ *be the (unique) basic subset and* $\phi \colon D \to \mathbb{F}_q^\times$ *the (unique) map such that* $\langle \chi, \xi_{D,\phi} \rangle \neq 0$.

- *If* n *is even, then* χ *has maximum degree if and only if*

$$D = \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \dots, \varepsilon_{n-3} + \varepsilon_{n-2}\} \cup D_1$$

where either $D_1 = \{\varepsilon_{n-1} + \varepsilon_n\}$ *or* $D_1 = \{\varepsilon_n\}$.

- *If* n *is odd, then* χ *has maximum degree if and only if*

$$D = \{\varepsilon_1 + \varepsilon_2, \varepsilon_3 + \varepsilon_4, \dots, \varepsilon_{n-2} + \varepsilon_{n-1}\} \cup D_1$$

where $D_1 \subseteq \{\varepsilon_n\}$.

Acknowledgments

This research was made within the activities of the Centro de Estruturas Lineares e Combinatórias at the University of Lisbon, Portugal. A large part of André's research done while he was visiting Stanford University and participating in the special program on combinatorial representation theory at the MSRI in Berkeley, CA, whose hospitality is gratefully acknowledged. André also expresses his sincere gratitude to Persi Diaconis for his invitation to visit Stanford, and for many enlightening discussions regarding supercharacters and their applications.

References

[AN 2006] C. A. M. André and A. M. Neto, "Super-characters of finite unipotent groups of types B_n, C_n and D_n", *J. Algebra* **305**:1 (2006), 394–429. MR 2007j:20013 Zbl 1104.20041

[André 1992] C. A. M. André, *Irreducible characters of the unitriangular group and coadjoint orbits*, thesis, University of Warwick, 1992.

[André 1995a] C. A. M. André, "Basic characters of the unitriangular group", *J. Algebra* **175**:1 (1995), 287–319. MR 96h:20081a Zbl 0835.20052

[André 1995b] C. A. M. André, "Basic sums of coadjoint orbits of the unitriangular group", *J. Algebra* **176**:3 (1995), 959–1000. MR 96h:20081b Zbl 0837.20050

[André 2001] C. A. M. André, "The basic character table of the unitriangular group", *J. Algebra* **241**:1 (2001), 437–471. MR 2002e:20082 Zbl 1013.20037

[André 2002] C. A. M. André, "Basic characters of the unitriangular group (for arbitrary primes)", *Proc. Amer. Math. Soc.* **130**:7 (2002), 1943–1954. MR 2003g:20075 Zbl 1005.20034

[André 2004] C. A. M. André, "Hecke algebras for the basic characters of the unitriangular group", *Proc. Amer. Math. Soc.* **132**:4 (2004), 987–996. MR 2005b:20009 Zbl 1064.20005

[André and Neto 2008] C. A. M. André and A. M. Neto, "A supercharacter theory for the Sylow p-subgroups of the finite symplectic and orthogonal groups", preprint, 2008. arXiv 0810.3761v1

[André and Nicolás 2008] C. A. M. André and A. P. Nicolás, "Supercharacters of the adjoint group of a finite radical ring", *J. Group Th.* **11**:5 (2008), 709–746.

[André and Pinho 2008] C. A. M. André and O. Pinho, "Factorization of supercharacters of finite algebra groups", preprint, 2008.

[Arias-Castro et al. 2004] E. Arias-Castro, P. Diaconis, and R. Stanley, "A super-class walk on upper-triangular matrices", *J. Algebra* **278**:2 (2004), 739–765. MR 2005f:60101 Zbl 1056.60006

[Carter 1972] R. W. Carter, *Simple groups of Lie type*, Pure and Applied Mathematics **28**, Wiley, London, 1972. MR 53 #10946 Zbl 0248.20015

[Carter 1985] R. W. Carter, *Finite groups of Lie type: Conjugacy classes and complex characters*, Wiley, New York, 1985. MR 87d:20060 Zbl 0567.20023

[Curtis and Reiner 1987] C. W. Curtis and I. Reiner, *Methods of representation theory, II: With applications to finite groups and orders*, Wiley, New York, 1987. MR 88f:20002 Zbl 0616.20001

[Diaconis and Isaacs 2008] P. Diaconis and I. M. Isaacs, "Supercharacters and superclasses for algebra groups", *Trans. Amer. Math. Soc.* **360**:5 (2008), 2359–2392. MR 2373317 Zbl 1137.20008

[Gudivok et al. 1990] P. M. Gudivok, Y. V. Kapitonova, S. S. Polyak, V. P. Rud'ko, and A. I. Tsitkin, "Classes of conjugate elements of a unitriangular group", *Kibernetika* (*Kiev*) 1 (1990), 40–48, 133. In Russian; translated in *Cybernetics* **26**:1 (1990), 47–57. MR 91d:20054 Zbl 0761.20022

[Huppert 1998] B. Huppert, *Character theory of finite groups*, de Gruyter Expositions in Mathematics **25**, de Gruyter, Berlin, 1998. MR 99j:20011 Zbl 0932.20007

[Jacobson 1979] N. Jacobson, *Lie algebras*, Dover, New York, 1979. MR 80k:17001 Zbl 0121.27504

[Kazhdan 1977] D. Kazhdan, "Proof of Springer's hypothesis", *Israel J. Math.* **28**:4 (1977), 272–286. MR 58 #5959 Zbl 0391.22006

[Kirillov 1995] A. A. Kirillov, "Variations on the triangular theme", pp. 43–73 in *Lie groups and Lie algebras: E. B. Dynkin's Seminar*, edited by S. G. Gindikin and E. B. Vinberg, Amer. Math. Soc. Transl. Ser. 2 **169**, Amer. Math. Soc., Providence, RI, 1995. MR 97a:20072 Zbl 0840.22015

[Marberg and Thiem 2008] E. Marberg and N. Thiem, "Superinduction for pattern groups", preprint, 2008. arXiv 0712.1228v1

[Sangroniz 2004] J. Sangroniz, "Characters of algebra groups and unitriangular groups", pp. 335–349 in *Finite groups 2003* (Gainesville, FL), edited by C. Y. Ho et al., de Gruyter, Berlin, 2004. MR 2006e:20012 Zbl 1103.20005

[Sangroniz 2008] J. Sangroniz, "Irreducible characters of large degree of Sylow p-subgroups of classical groups", preprint, 2008.

[Thiem and Venkateswaran 2007] N. Thiem and V. Venkateswaran, "Restricting supercharacters of the finite group of unipotent uppertriangular matrices", preprint, 2007. arXiv 0712.1237v1

[Yan 2001] N. Yan, *Representation theory of the finite unipotent linear groups*, thesis, University of Pennsylvannia, 2001.

Received April 26, 2008.

CARLOS A. M. ANDRÉ
DEPARTAMENTO DE MATEMÁTICA
FACULDADE DE CIÊNCIAS
UNIVERSIDADE DE LISBOA
CAMPO GRANDE, EDIFÍCIO C6, PISO 2
1749-016 LISBOA
PORTUGAL

caandre@fc.ul.pt

ANA MARGARIDA NETO
INSTITUTO SUPERIOR DE ECONOMIA E GESTÃO
UNIVERSIDADE TÉCNICA DE LISBOA
RUA DO QUELHAS 6
1200-781 LISBOA
PORTUGAL

ananeto@iseg.utl.pt