COMBINATORIAL PROPERTIES OF SUBGROUP LATTICES OF FINITE GROUPS

BY JOHN SHARESHIAN

A dissertation submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Mathematics

Written under the direction of

Richard Lyons

and approved by

New Brunswick, New Jersey

May, 1996

ABSTRACT OF THE DISSERTATION

Combinatorial Properties of Subgroup Lattices of Finite Groups

by John Shareshian
Dissertation Director: Richard Lyons

The purpose of this thesis is to investigate certain combinatorial and topological properties of subgroup lattices of almost simple finite groups. In particular, we determine the Möbius number $\mu(1, G)$ when G is a two or three dimensional projective general linear or projective special linear group over a field of odd order, a three dimensional projective general unitary group or projective special unitary group over a field of odd order or a Suzuki group. When G is a symmetric group whose degree is either a power of two or has at most two prime factors counting multiplicities, we give a formula for $\mu(1, G)$ which involves the Möbius numbers of certain primitive subgroups of G. This formula is used to determine $\mu(1, G)$ if the degree of G is prime, twice a prime, or a power of two. In addition, we give a formula for the Möbius numbers of certain orthogonal groups in prime dimension over fields of odd order. This formula involves the Möbius numbers of certain absolutely irreducible almost simple subgroups. Also, we determine the Lefschetz characters for the actions of certain projective linear, unitary and orthogonal groups in prime dimension over fields of odd order on the partially ordered sets consisting of the nontrivial reducible subgroups of each of the given groups.

Acknowledgements

I cannot imagine having a better advisor than Richard Lyons. To mention all the instances in which he has provided valuable assistance to me would require the addition of another chapter to this thesis. Richard's infectious enthusiasm for mathematics and his remarkable sense of professionalism have amazed and inspired me many times over the last three years. The amount of time he spent discussing and carefully examining my work and attempting to share some of his seemingly boundless knowledge with me far exceeded all reasonable expectations. It has been a privilege and a pleasure to work with such a fine scholar and decent person.

Many other members of the mathematics faculty at Rutgers have been generous with their time and advice. Most notably, Michael Saks has often given me useful help and encouragement. In addition, I have learned much of what I know about good mathematical exposition simply by sitting in his lectures. The faculty as a whole has created an atmosphere in which an ambitious student can thrive.

I have made many good friends during my years here. Saša Pekeč and Tom Bohman have been great housemates for four years. We had more fun than one could imagine to be possible given the amount of hard work we did. It was a pleasure and a challenge to study combinatorics with such bright colleagues. I have benefited greatly from many enjoyable and productive discussions on group theory and other topics with Gretchen Ostheimer and Eddie Lo. Gretchen has also been a great source of friendship and support when I most needed it. Most of all, I'd like to thank Shari Moskow for all of the wonderful time we have spent together. My life here would not have been the same without Shari's kindness, friendship and companionship.

Jeff Steif has been a great friend and a role model for me for many years. I don't know if I would have finally chosen mathematics as a career had I not met Jeff.

My entire extended family has always been a source of support and inspiration. I certainly learned the necessity of carefully thought out and clearly presented arguments at family gatherings.

Finally, I'd like to thank my oldest and closest friends, who are probably quite amazed that I could produce 175 pages of coherent writing. Thanks to Beth, Bruce, Jeff, Max, and most of all JoAnn.

Dedication

This thesis is dedicated to my family. My parents, Helga and Richard Shareshian, provided me with a great education, taught me right from wrong, and stood by me while I struggled to find a fulfilling path in life. The one which I finally found was one which they had the wisdom to prepare me for long before I realized that it was right for me. My brother, Steven Shareshian, and my grandmother, Lily Hearst, have also given their love and support throughout my life, for which I am deeply grateful.

Table of Contents

Abstract ii

Acknowledgements iii

Dedication v

COMBINATORIAL PROPERTIES OF SUBGROUP LATTICES OF FINITE GROUPS

BY JOHN SHARESHIAN

A thesis submitted to the

Graduate School—New Brunswick

Rutgers, The State University of New Jersey

in partial fulfillment of the requirements

for the degree of

Doctor of Philosophy

Graduate Program in Mathematics

Written under the direction of

Richard Lyons

and approved by

New Brunswick, New Jersey

May, 1996

ABSTRACT OF THE THESIS

Combinatorial Properties of Subgroup Lattices of Finite Groups

by John Shareshian

Thesis Director: Richard Lyons

The purpose of this thesis is to investigate certain combinatorial and topological properties of subgroup lattices of almost simple finite groups. In particular, we determine the Möbius number $\mu(1, G)$ when G is a two or three dimensional projective general linear or projective special linear group over a field of odd order, a three dimensional projective general unitary group or projective special unitary group over a field of odd order or a Suzuki group. When G is a symmetric group whose degree is either a power of two or has at most two prime factors counting multiplicities, we give a formula for $\mu(1, G)$ which involves the Möbius numbers of certain primitive subgroups of G. This formula is used to determine $\mu(1, G)$ if the degree of G is prime, twice a prime, or a power of two. In addition, we give a formula for the Möbius numbers of certain orthogonal groups in prime dimension over fields of odd order. This formula involves the Möbius numbers of certain absolutely irreducible almost simple subgroups. Also, we determine the Lefschetz characters for the actions of certain projective linear, unitary and orthogonal groups in prime dimension over fields of odd order on the partially ordered sets consisting of the nontrivial reducible subgroups of each of the given groups.

Acknowledgements

I cannot imagine having a better advisor than Richard Lyons. To mention all the instances in which he has provided valuable assistance to me would require the addition of another chapter to this thesis. Richard's infectious enthusiasm for mathematics and his remarkable sense of professionalism have amazed and inspired me many times over the last three years. The amount of time he spent discussing and carefully examining my work and attempting to share some of his seemingly boundless knowledge with me far exceeded all reasonable expectations. It has been a privilege and a pleasure to work with such a fine scholar and decent person.

Many other members of the mathematics faculty at Rutgers have been generous with their time and advice. Most notably, Michael Saks has often given me useful help and encouragement. In addition, I have learned much of what I know about good mathematical exposition simply by sitting in his lectures. The faculty as a whole has created an atmosphere in which an ambitious student can thrive.

I have made many good friends during my years here. Saša Pekeč and Tom Bohman have been great housemates for four years. We had more fun than one could imagine to be possible given the amount of hard work we did. It was a pleasure and a challenge to study combinatorics with such bright colleagues. I have benefited greatly from many enjoyable and productive discussions on group theory and other topics with Gretchen Ostheimer and Eddie Lo. Gretchen has also been a great source of friendship and support when I most needed it. Most of all, I'd like to thank Shari Moskow for all of the wonderful time we have spent together. My life here would not have been the same without Shari's kindness, friendship and companionship.

Jeff Steif has been a great friend and a role model for me for many years. I don't know if I would have finally chosen mathematics as a career had I not met Jeff.

My entire extended family has always been a source of support and inspiration. I certainly learned the necessity of carefully thought out and clearly presented arguments at family gatherings.

Finally, I'd like to thank my oldest and closest friends, who are probably quite amazed that I could produce 175 pages of coherent writing. Thanks to Beth, Bruce, Jeff, Max, and most of all JoAnn.

Dedication

This thesis is dedicated to my family. My parents, Helga and Richard Shareshian, provided me with a great education, taught me right from wrong, and stood by me while I struggled to find a fulfilling path in life. The one which I finally found was one which they had the wisdom to prepare me for long before I realized that it was right for me. My brother, Steven Shareshian, and my grandmother, Lily Hearst, have also given their love and support throughout my life, for which I am deeply grateful.

Table of Contents

Chapter 1

Introduction and statement of the main results

The purpose of this thesis is to investigate combinatorial properties of partially ordered sets associated with certain almost simple finite groups, and to relate these properties to either the representation theory of these groups or the group theoretic properties of their maximal subgroups. All of the questions that will be studied are related to the following general construction.

To each finite partially ordered set P there is associated an abstract simplicial complex $\Delta = \Delta(P)$. The k-simplices of $\Delta(P)$ are the linearly ordered subsets of P of size $k+1$. The topological properties of (an arbitrary geometric realization of) $\Delta(P)$ give information about the combinatorial properties of P. In particular, if $\hat{P}$ is the poset obtained by adjoining a minimum element $\hat{0}$ and a maximum element $\hat{1}$ to P, then $\mu_{\hat{P}}(\hat{0}, \hat{1}) = \tilde{\chi}(\Delta(P))$, where $\tilde{\chi}$ is the reduced Euler characteristic of a simplicial complex, and μ is the Möbius function of a poset. The chain complex $C_*(\Delta)$ and the associated reduced homology $\tilde{H}_*(\Delta)$ are defined in the standard manner. If a group G acts on P, then each chain group $C_i(\Delta)$ is a permutation module for G. The action of G commutes with the boundary map δ on $C_*(\Delta)$, and it follows that each reduced homology group $\tilde{H}_i(\Delta)$ is a G-module. It is well-known that $\sum_i (-1)^i C_i(\Delta)$ and $\sum_i (-1)^i \tilde{H}_i(\Delta)$ are equal in the Grothendieck ring of G, and that the generalized character Λ of these modules (called the Lefschetz character) is given by $\Lambda(g) = \mu_{\hat{P}^g}(\hat{0}, \hat{1}) = \tilde{\chi}(\Delta(P^g))$, where P^g is the poset of points of P fixed by $g \in G$ (with order inherited from P). This construction will be described in more detail in the following chapter, and the reader may refer to either [13] or [48] for further explanation.

1.1 The Lefschetz character on the ideal of reducible subgroups

The main results in this thesis are of two types. The results of the first type are contained in Chapter 3. In that chapter, G is one of the classical groups $PGL_d(q)$, $L_d(q)$, $PGU_d(q)$, $U_d(q)$, $SO_d(q)$ or $\Omega_d(q)$, where d is an odd prime number and q is an odd prime power. We study the Lefschetz character for the action of G on a large ideal in its subgroup lattice. Namely, let V be a vector space of dimension d over a field $\mathbf{F}_q$ of odd order, and let h and s be nondegenerate hermitian and symmetric forms on V, respectively. If G is any of the groups given above, there is an embedding $\phi : G \hookrightarrow PGL(V)$ such that the preimage of $\phi(G)$ in $GL(V)$ preserves the appropriate form on V. This embedding determines an action of G on the projective space associated with V. A subgroup of G is called reducible if it stabilizes some subspace of V in this action. Let $\mathcal{I}_1(G)$ be the collection of nontrivial reducible subgroups of G. Note that $\mathcal{I}_1(G) \cup \{1\}$ is an ideal in the subgroup lattice of G which is invariant under conjugation by elements of G. We will determine the Lefschetz character for the action of G on $\mathcal{I}_1(G)$ by conjugation, which we will call $\Lambda_{\mathcal{I}_1(G),G}$. We will show that the negative of this Lefschetz character turns out to be an actual character, induced from a linear character of a subgroup of G which is either cyclic or metacyclic. Recall that a Coxeter torus of one of the linear or unitary groups described above is an irreducible cyclic subgroup which is maximal in G with respect to having those properties. If G is a linear or unitary group, the normalizer of a Coxeter torus $C \leq G$ is a split extension of C by a cyclic group F_d of order d, which is generated by an element f_d. We may choose a basis for V so that $f_d \in PGL(V)$ is the image under the natural projection from $GL(V)$ of a permutation matrix. We will show that for any of the groups G under consideration, we may choose our embedding ϕ so that $f_d \in G$. We can now state the main results of Chapter 3.

Theorem 1.1 *(Linear case) Let V be a linear space of odd prime dimension d over a field $\mathbf{F}_q$ of odd order. Let G be one of $L(V)$ or $PGL(V)$. Let D be a Coxeter torus of $PGL(V)$ which is normalized by F_d, and set $C = D \cap G$. Let N be the normalizer of C in G, so $N = F_dC$. Let θ be the character of N defined by $ker(\theta) = C$ and*

$\theta(f_d) = e^{2\pi i/d}$. *Then* $-\Lambda_{\mathcal{I}_1(G),G}$ *is the induced character* θ^G.

Theorem 1.2 *(Unitary case) Let* V *be a nondegenerate unitary space of odd prime dimension* d *over a field* $\mathbf{F}_q$ *of odd order. Let* G *be one of* $PSU(V)$ *or* $PGU(V)$*. Let* D *be a Coxeter torus of* $PGU(V)$ *which is normalized by* F_d *and set* $C = D \cap G$*. Let* N *be the normalizer of* C *in* G*, so* $N = F_dC$*. Let* θ *be the character of* N *defined by* $ker(\theta) = C$ *and* $\theta(f_d) = e^{2\pi i/d}$*. Then* $-\Lambda_{\mathcal{I}_1(G),G}$ *is the induced character* θ^G.

Theorem 1.3 *(Orthogonal case) Let* V *be a nondegenerate orthogonal space of odd prime dimension* d *over a field* $\mathbf{F}_q$ *of odd order.*

(A) Let $G = SO(V)$*. Let* θ *be the linear character of* F_d *defined by* $\theta(f_d) = e^{2\pi i/d}$*. Then* $-\Lambda_{\mathcal{I}_1(G),G}$ *is the induced character* θ^G.

(B) Let $G = \Omega(V)$ *and assume* $q > 3$*. Then there exist* $Y_d \leq G$ *with* Y_d *conjugate to* F_d *in* $SO(V)$ *and faithful linear characters* $\theta_1 : F_d \to \mathbf{C}$ *and* $\theta_2 : Y_d \to \mathbf{C}$ *such that* $-\Lambda_{\mathcal{I}_1(G),G} = \theta_1^G + \theta_2^G$.

The proofs of these theorems will depend heavily on the fact that d is prime, and it can be shown by lengthy calculations which we do not include in this thesis that if $d = 4$ then the degree of $\Lambda_{\mathcal{I}_1(PGL(V)),PGL(V)}$ is not the index of the normalizer of a Coxeter torus. Determination of the appropriate analogue of the theorems given above might lead to many interesting results, as these theorems bear a remarkable resemblance to a well-studied theorem of Stanley. In [46], Stanley determined the Lefschetz character for the natural action of the symmetric group S_n on the poset $\overline{\Pi}_n$ of nontrivial proper partitions of $[n]$, ordered by refinement. Using a theorem of Hanlon [21], he showed that up to a sign, this Lefschetz character is an actual character, induced from a linear character of a cyclic subgroup of order n. Indeed, if $g \in S_n$ is an n-cycle, σ is the character of $\langle g \rangle$ defined by $g \mapsto e^{2\pi i/n}$ and ϵ is the alternating character, then

$$\Lambda_{\Pi_n,S_n} = (-1)^{n-1}(\epsilon\sigma)^{S_n}.$$

This result is further studied and explained from various viewpoints in [36], [30], [5], [4], and [49]. It can be related to the theorems of Chapter 3 as follows. Let $\mathcal{IN}_n$ be the poset of nontrivial intransitive subgroups of S_n. Then S_n acts on $\mathcal{IN}_n$ by conjugation. By a result of Quillen (see [40], (1.3)), the map from $\mathcal{IN}_n$ to Π_n which sends an intransitive group to the partition determined by its orbits induces an S_n-equivariant homotopy between the associated order complexes. It follows that the Lefschetz characters for the actions of S_n on $\mathcal{IN}_n$ and Π_n are the same. Theorem 1.1 above becomes particularly interesting in this light, given the natural correspondence between the conjugacy classes of S_n and conjugacy classes of maximal tori in $PGL_n(q)$ in which the class of $g \in S_n$ as described above corresponds to the class of Coxeter tori in $PGL(V)$ (see [43], II). It should be noted that in the case of the symmetric group, the fact that Π_n is a geometric lattice guarantees that all of the reduced homology groups for the associated order complex are trivial except for possibly the top homology group (see [17]). It then follows easily that, up to a sign, the associated Lefschetz character is an actual character. There is no known corresponding result for the classical groups. That is, the dimensions in which the homology of the order complex of $\mathcal{I}_1(G)$ does not vanish are not known.

1.2 Möbius numbers of almost simple groups

The second type of result involves the determination of $\mu(1, G)$ for certain almost simple groups G. This can be viewed as the determination of $\Lambda(1)$, where Λ is the Lefschetz character for the action of G on the poset of nontrivial proper subgroups of G by conjugation. If G is simple, it is easy to see that $\Lambda(g) = 0$ for all $g \neq 1$, so Λ is an integer multiple of the regular representation. That multiple is determined by $\mu(1, G)$. More generally, if G is almost simple with simple normal subgroup S, $\Lambda(g) = 0$ for all $g \in G$ such that $\langle g \rangle \cap S \neq 1$ (see Lemma 2.4 of [22]).

It should be noted at this point that a formula for $\mu(1, G)$ when G is solvable was given by Kratzer and Thévenaz, who proved the following theorem.

Theorem 1.4 ([29], Théorème 2.6) *Let* $1 = G_n \lhd G_{n-1} \ldots \lhd G_1 \lhd G_0 = G$ *be a chief series for a solvable group* G*, and let* m_i *be the number of complements to* G_i/G_{i+1} *in* G/G_{i+1}*. Then*

$$\mu(1, G) = (-1)^n \prod_{i=1}^{n-1} m_i.$$

Kratzer and Thévenaz also prove the following result, from which it follows immediately that if G is an almost simple group with simple normal subgroup S, then $\mu(1, G)$ is a multiple of $|S|$.

Theorem 1.5 ([29], Théorème 3.1) *For a positive integer* n*, define* n_0 *to be the product of all the prime numbers dividing* n*. For a finite group* G*, let* G' *be the commutator subgroup of* G*. Then* $\mu(1, G)$ *is a multiple of* $\frac{|G|}{[G:G']_0}$*.*

The results of the first type and the definition $\mu(1, G) = -\sum_{H<G} \mu(1, H)$ lead immediately to the following strategy. If a large ideal $\mathcal{I}$ in the subgroup lattice of G can be found so that $\sum_{H \in \mathcal{I}} \mu(1, H)$ can be calculated relatively easily, it may be possible to calculate the remaining sum $\sum_{H<G, H \notin \mathcal{I}} \mu(1, H)$ using ad-hoc methods. If $\mathcal{I}$ is generated by some "natural" set of maximal subgroups of G, a relation between $\mu(1, G)$ and the maximal subgroups of G which are not contained in $\mathcal{I}$ can be determined, even when the second sum cannot be calculated.

If G is a finite classical group, the maximal subgroups of G lie in the union $\bigcup_{i=1}^{9} \mathcal{C}_i(G)$ of nine classes of subgroups by a theorem of Aschbacher (see [3]). One of these classes is the class $\mathcal{C}_1(G)$ of subgroups which are maximal among all reducible subgroups of G. These are simply the maximal elements of the ideal $\hat{\mathcal{I}}_1(G) = \mathcal{I}_1(G) \cup \{1\}$ described above, and if G is one of the groups studied in Chapter 3, we have

$$\sum_{H \in \hat{\mathcal{I}}_1(G)} \mu(1, H) = -\Lambda_{\mathcal{I}_1(G), G}(1).$$

Thus $\hat{\mathcal{I}}_1(G)$ is a good candidate for the ideal described in the above paragraph. One must then examine the remaining classes of maximal subgroups of G given in [3]. Seven of the nine classes of maximal subgroups described in Aschbacher's theorem are subgroups which stabilize some standard object associated with the natural vector space V associated with G, such as a subspace, a decomposition into a direct sum or tensor product of subspaces, or a nondegenerate form. The remaining classes are the class $\mathcal{C}_7(G)$ of normalizers of extraspecial p-groups and the class $\mathcal{C}_9(G)$ of almost simple groups which do not lie in any of the first eight classes. By Aschbacher's theorem, the elements of $\mathcal{C}_9(G)$ act absolutely irreducibly on the natural projective module for G, are not defined over any proper subfield of the smallest field over which G is defined, and do not preserve any nondegenerate bilinear or hermitian form on V which is not preserved by G. When $d = dim(V)$ is prime, many of these classes are empty.

1.3 Orthogonal groups in prime dimension

In particular, if $G = SO_d(q)$ or $\Omega_d(q)$ with d an odd prime, the only nonempty classes are the class $\mathcal{C}_1(G)$ of maximal reducible subgroups, the class $\mathcal{C}_2(G)$ of maximal imprimitive subgroups, and the class $\mathcal{C}_5(G)$ of maximal subfield subgroups, and possibly the class $\mathcal{C}_9(G)$. These classes will be described in Chapter 4, in which the following theorem will be proved.

Theorem 1.6 *Fix an odd prime $p > 3$ and an odd prime d such that every transitive proper subgroup of A_d is solvable. Let a be any natural number. Let V be a nondegenerate orthogonal space of dimension d over a field of order p^a. Set*

$$\omega(a) := \frac{\mu(1, \Omega(V)) + \sum_{H \in \mathcal{C}_9(\Omega(V))} \mu(1, H)}{|\Omega(V)|}$$

and

$$\sigma(a) := \frac{\mu(1, SO(V)) + \sum_{H \in \mathcal{C}_9(SO(V))} \mu(1, H)}{|\Omega(V)|}.$$

Then

$$\omega(a) = \begin{cases} -1 & p \equiv 3, 5 \bmod 8 \textit{ and } a = 1 \\ 0 & \textit{otherwise} \end{cases}$$

Furthermore, $\sigma(a) = -\omega(a)$.

Results such as this are in some sense the best possible ones for classical groups. That is, the presence and structure of maximal subgroups of a classical group $G = G(d,q)$ defined in dimension d over $\mathbf{F}_q$ are determined by straightforward number theoretical conditions on d and q, with the exception of the subgroups in $\mathcal{C}_9(G)$. The presence and structure of these subgroups is determined by the modular representation theory of finite simple groups. A complete description of the elements of $\mathcal{C}_9(G)$ in terms of d, q and the isomorphism type of G is not currently available, and it is unlikely that such a description could be as uniform as the descriptions of the members of the other eight classes. Thus it seems likely that the best possible general formulas for Möbius numbers of classical groups would be of the form

$$\mu(1, G(d,p^a)) = f_{G,d,p}(a) + \sum_{H \in \mathcal{C}_9(G(d,p^a))} \mu(1,H),$$

where $f_{G,d,p}$ is some nice function defined over a class of groups in a given dimension and characteristic, all of which are of the same classical type.

Note that the results above require that every transitive subgroup of A_d be solvable. This requirement arises from a problem similar to the one described in the previous paragraph. Namely, if $G = SO_d(q)$ or $\Omega_d(q)$ then the elements of $\mathcal{C}_2(G)$ are split extensions of elementary abelian 2-groups by groups isomorphic to A_d or S_d. Now every transitive proper subgroup of A_d is either solvable or almost simple. If there are no almost simple transitive subgroups, then the elements of $\mathcal{C}_2(G)$ which are not contained in $\mathcal{I}_1(G)$ are easily described, and the sum of their Möbius numbers can be calculated exactly. The presence of almost simple transitive subgroups prevents such a calculation from being completed, although this problem is somewhat different from the problem of determining the elements of $\mathcal{C}_9(G)$ in that there exists a nice description of all transitive almost simple permutation groups of prime degree (see [19]). The calculation of the sum of the Möbius numbers of the elements of $\mathcal{C}_2(G) \setminus \mathcal{C}_1(G)$ can be completed if the Möbius numbers of all of the almost simple transitive groups of degree d are known, but at present this is not the case for most primes d for which such groups not containing A_d exist. A further discussion of this phenomenon appears in Chapter 4.

1.4 Linear and unitary groups of small dimension

If d is small, then all the elements of $\mathcal{C}_9(G)$ may be known. This is certainly the case if G is one of $SO_3(q) \cong PGL_2(q)$, $\Omega_3(q) \cong L_2(q)$, $PGL_3(q)$, $L_3(q)$, $PGU_3(q)$ or $U_3(q)$. Indeed, all subgroups of $L_2(q)$ are described in [14], and all maximal subgroups of $L_3(q)$ and $U_3(q)$ are listed in [34]. If G is one of the groups just listed, it is possible to complete the calculation of $\mu(1, G)$ after beginning with the results of Chapter 3. In Chapter 5, we prove the following results.

Theorem 1.7 *Fix a prime $p > 3$. For a positive integer a, define*

$$\lambda(a) := \frac{\mu(1, L_2(p^a))}{|L_2(p^a)|}$$

and

$$\rho(a) := \frac{\mu(1, PGL_2(p^a))}{|L_2(p^a)|}.$$

Then

$$\rho(a) = \begin{cases} 1 & a = 1,\ p \equiv 3, 5 \pmod 8 \\ 0 & \textit{otherwise} \end{cases}$$

and

$$\lambda(1) = \begin{cases} 2 & q \equiv 1, 4 \pmod 5 \quad q \equiv 1, 7 \pmod 8 \\ 1 & q \equiv 1, 4 \pmod 5 \quad q \equiv 3, 5 \pmod 8 \\ 0 & q \equiv 2, 3 \pmod 5 \quad q \equiv 1, 7 \pmod 8 \\ -1 & q \equiv 0, 2, 3 \pmod 5 \quad q \equiv 3, 5 \pmod 8 \end{cases}$$

$$\lambda(2) = \begin{cases} 0 & p \equiv 0, 1, 4 \pmod 5 \\ 2 & p \equiv 2, 3 \pmod 5 \end{cases}$$

$$\lambda(a) = 0 \textit{ if } a > 2$$

Theorem 1.8 *For a positive integer a, define*

$$\lambda(a) := \frac{\mu(1, L_2(3^a))}{|L_2(3^a)|}$$

and

$$\rho(a) := \frac{\mu(1, PGL_2(3^a))}{|L_2(3^a)|}.$$

Then

$$\rho(a) = \begin{cases} -\mu(a) & a \text{ odd} \\ 0 & a \text{ even} \end{cases}$$

and

$$\lambda(a) = \begin{cases} \frac{1}{3} & a = 1 \\ 2 & a = 2 \\ \mu(a) & a > 1 \text{ odd} \\ 0 & a > 2 \text{ even.} \end{cases}$$

For $G = \Omega_3(q) \cong L_2(q)$, these results were obtained previously by Downs (see [16]).

Chapter 5 contains one additional theorem, which gives the Möbius number of the extension of $L_2(p^2)$ by a field automorphism of order two for certain primes p. This result will be used in the determination of $\mu(1, S_n)$ for certain values of n.

Using the above results and the results of Chapter 3, we obtain the following results in Chapter 6.

Theorem 1.9 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ or a 3-dimensional unitary space over $\mathbf{F}_{q^2}$, where $q = p^a$ and p is an odd prime. If V is a linear space and $L(V) < PGL(V)$ then $\mu(1, PGL(V)) = 0$. If V is a unitary space and $U(V) < PGU(V)$ then $\mu(1, PGU(V)) = 0$.*

Theorem 1.10 *Let p be an odd prime and let a be a positive integer. Then*

$$\mu(1, L_3(p^a)) = \begin{cases} -6|L_3(p^a)| & \text{if } a = 1 \text{ and } p \equiv 1, 4 \bmod 15 \\ -6|L_3(p^a)| & \text{if } a = 2 \text{ and } p \equiv 2, 7, 8, 13 \bmod 15 \\ 0 & \text{otherwise} \end{cases}$$

Also,

$$\mu(1, U_3(p^a)) = \begin{cases} -6|U_3(p^a)| & \text{if } a = 1 \text{ and } p \equiv 11, 14 \bmod 15 \\ 0 & \text{otherwise} \end{cases}$$

Note that the results we have stated above deal for the most part with projective classical groups. Although the orthogonal groups we have studied are described as $SO_d(q)$ and $\Omega_d(q)$, since d is odd we have $SO_d(q) \cong PGO_d(q) \cong PSO_d(q)$ and $\Omega_d(q) \cong P\Omega_d(q)$. There is a reason for examining these projective groups rather then their covering groups. Namely, if G is a classical group with nontrivial center Z, then usually G contains no complement to Z. In this case, Crapo's complement theorem, which will be stated in the next chapter, gives $\mu(1, G) = 0$. In cases where a complement to Z does exist, Crapo's theorem can be used to determine $\mu(1, G)$ if one knows $\mu(1, G/Z)$. The following result appears in Chapter 4.

Proposition 1.11 *Let V be a nondegenerate orthogonal space of odd dimension d over a field $\mathbf{F}_q$ of odd order. Let Z be the subgroup of $GO(V)$ generated by -1_V. Let $X = \{-g : g \in SO(V) \setminus \Omega(V)\}$, and define $TO(V) := \Omega(V) \cup X$. Then*

(1) If $\Omega(V) < G < GO(V)$ then G is one of $SO(V), TO(V)$ or $\Omega(V) \times Z$.

(2) $TO(V) \cong SO(V)$, so $\mu(1, TO(V)) = \mu(1, SO(V))$.

(3) $\mu(1, \Omega(V) \times Z) = -\mu(1, \Omega(V))$.

(4) $\mu(1, GO(V)) = -2\mu(1, SO(V))$.

1.5 Suzuki groups

Chapter 7 is a short chapter in which the Möbius numbers of the Suzuki groups $Sz(2^a)$ are determined. This is routine, since a complete description of the maximal subgroups of the Suzuki groups exists. The result is as follows.

Theorem 1.12 *For an odd integer $a > 1$, define*

$$\sigma(a) := \frac{\mu(1, Sz(2^a))}{|Sz(2^a)|}.$$

Then for all such a,

$$\sigma(a) = \mu(a),$$

where μ is the usual number theoretic Möbius function.

1.6 Symmetric groups

The theorem of Stanley on the Lefschetz character for the actions of S_n on Π_n and $\mathcal{IN}_n$ can be used as a starting point for the investigation of $\mu(1, S_n)$ in the same manner that the results of Chapter 3 were used in the attempt to determine the Möbius numbers of the classical groups. However, it turns out to be more useful to work with the ideal which is the union of $\mathcal{IN}_n$ and all subgroups of A_n. The first result in Chapter 8 is the determination of the sum of the Möbius numbers of all of the subgroups in this ideal. The version of this result that will be most useful to us is stated below.

Proposition 1.13 *For $n \in \mathbf{N}$, let $\mathcal{C}_n$ be the set of proper subgroups of S_n which are transitive and contain an involution from $S_n \setminus A_n$. Then*

$$\mu(1, S_n) = (-1)^{n-1}\frac{n!}{2} - \sum_{H \in \mathcal{C}_n} \mu(1, H)$$

The maximal subgroups of S_n are naturally divided into three classes. That is, if $M < S_n$ is maximal then one of the following three cases holds. In the first case, M is intransitive, so $M \cong S_k \times S_l$ with $n = k + l$. In the second case, M is imprimitive, so M is isomorphic to the wreath product $S_k[S_l]$ with $n = kl$. In the final case, M is primitive. Although it is not true that every primitive subgroup of S_n is known for every natural number n, the O'Nan-Scott Theorem (see [31]) gives a general description of primitive permutation groups, further dividing this class of groups into five subclasses. One of these subclasses is the class of almost simple primitive groups. This class can be viewed as the analogue for permutation groups of the class $\mathcal{C}_9$ of almost simple maximal subgroups of the classical groups. As with the classical groups, the best result that can be expected in the determination of $\mu(1, S_n)$ is probably one of the form

$$\mu(1, S_n) = f(n) + \sum_{H \in \mathcal{P}'} \mu(1, H),$$

where f is some nice function of n and $\mathcal{P}'$ is some easily described subset of the set of primitive subgroups of S_n. Given Proposition 1.13 above, the obvious candidate for f is $f(n) = (-1)^{n-1}\frac{n!}{2}$. Indeed, it has been verified that $\mu(1, S_n) = (-1)^{n-1}\frac{|Aut(S_n)|}{2}$ for $1 < n \leq 11$ (see [53], [37]). In [45], it is asked whether this last formula holds for all $n > 1$. This turns out to be false, although the formula does hold for infinitely many values of n.

With Proposition 1.13 and the above description of the maximal subgroups in hand, the natural next step in any attempt to determine $\mu(1, S_n)$ is to try to find the sum of the Möbius numbers of the elements of $\mathcal{C}_n$ which are imprimitive. This turns out to be feasible when n has few prime factors, counting multiplicity, or n is a power of two. The following result appears in Chapter 8.

Theorem 1.14 *For $n \in \mathbf{N}$, let $\mathcal{P}_n$ be the set of primitive proper subgroups of S_n which contain an involution from $S_n \setminus A_n$. For the following values of n,*

$$\mu(1, S_n) = (-1)^{n-1}\frac{n!}{2} - \sum_{H \in \mathcal{P}_n} \mu(1, H)$$

(1) $n = p$ *p prime*

(2) $n = p^2$ *p prime*

(3a) $n = 2p$ *p an odd prime*

(3b) $n = pr$ *p, r distinct odd primes*

(4) $n = 2^a$ $a \in \mathbf{N}$

At this time there are no values of n for which the formula given in Theorem 1.14 is known not to hold. It can be shown through lengthy and tedious calculations which are not included in this thesis that the formula does hold for $n = 12$. The proof of this theorem involves using the inclusion-exclusion principle to show that the sum of the Möbius numbers of the elements of $\mathcal{C}_n$ which are imprimitive is zero. The success of this method in cases (1), (2) and (3) depends heavily on the fact that n has very few factors, and it is unlikely that the method can be applied when this condition is not satisfied.

Using Theorem 1.14, the O'Nan-Scott Theorem and the classification of finite simple groups, one can complete the calculation of $\mu(1, S_n)$ in cases (1),(3a) and (4). The results are given below.

Theorem 1.15 *Let p be prime. Then*

$$\mu(1, S_p) = (-1)^{p-1}\frac{p!}{2}.$$

Theorem 1.16 *Let $n = 2p$, p an odd prime.*

$$\mu(1, S_n) = \begin{cases} -n! & \text{if } n-1 \text{ is prime and } p \equiv 3 \pmod 4; \\ \frac{n!}{2} & \text{if } n = 22; \\ -\frac{n!}{2} & \text{otherwise.} \end{cases}$$

Theorem 1.17 *Let $n = 2^a$, $a \in \mathbf{N}$. Then*

$$\mu(1, S_n) = -\frac{n!}{2}.$$

Chapter 8 also contains a discussion of $\mu(1, A_n)$ in the case $n = 2p$. It turns out that in that case, one can show that the sum of the Möbius numbers of all of the primitive subgroups of S_n is zero. Thus if $\mu(1, S_n)$ and the Möbius numbers of all primitive subgroups of S_n which do not contain A_n are known, one can immediately calculate $\mu(1, A_n)$. This result is used to provide counterexamples to two recent conjectures on the Möbius numbers of S_n and A_n.

The next chapter contains basic results from group theory and the theory of partially ordered sets. The reader who is already familiar with these subjects may skip that chapter and refer back to it when necessary, although Lemma 2.17 should be read before reading Chapter 3.

We close this chapter with some questions which arise from some of the results stated above.

Question 1.18 *Let V be a nondegenerate orthogonal space of odd prime dimension over $\mathbf{F}_3$. Let $G = \Omega(V)$ and define $\mathcal{I}_1(G)$ as above. What is the Lefschetz character $\Lambda_{\mathcal{I}_1(G),G}$?*

Question 1.19 *Let V be a linear space or a nondegenerate unitary or orthogonal space of odd prime dimension d over a finite field of even order. Let G be one of $L(V)$, $PGL(V)$, $U(V)$, $PGU(V)$, $P\Omega(V)$, $PSO(V)$ or $PGO(V)$. Define $\mathcal{I}_1(G)$ as above. What is the Lefschetz character $\Lambda_{\mathcal{I}_1(G),G}$?*

Question 1.20 *Let V be a linear space or a nondegenerate unitary or orthogonal space of finite dimension over a finite field. Let G be one of $L(V)$, $PGL(V)$, $U(V)$, $PGU(V)$, $P\Omega(V)$, $PSO(V)$ or $PGO(V)$. Define $\mathcal{I}_1(G)$ as above. What is the Lefschetz character $\Lambda_{\mathcal{I}_1(G),G}$?*

Question 1.21 *Let V be a linear space or a nondegenerate unitary or orthogonal space of finite dimension over a finite field. Let G be one of the groups given in the previous question, and for $1 \leq i \leq 9$ define $\mathcal{C}_i(G)$ as above. Is there some $J \subseteq [9]$ such that if $\mathcal{I}$ is the ideal in the subgroup lattice of G generated by the elements of J then the Lefschetz character for the action of G on $\mathcal{I}$ by conjugation is induced from a linear character of the normalizer of a Coxeter torus in the linear and unitary cases and induced from a cyclic subgroup generated by an element of G which transitively permutes an orthogonal frame in the orthogonal case?*

Question 1.22 *Fix a dimension d and a prime $p > 3$. Does there exist a natural number M such that for all $a > M$ we have $\mu(1, L_d(p^a)) = 0$?*

Note that when $d = 2$ or 3 then we may take $M = 2$. Of course, one may state the same question for other classical groups.

Question 1.23 *Does the formula of Theorem 1.14 hold for all natural numbers? That is, is it true that for all n we have*

$$\mu(1, S_n) = (-1)^{n-1}\frac{n!}{2} - \sum_{H \in \mathcal{P}_n} \mu(1, H)?$$

Chapter 2

Preliminaries

We begin by stating some definitions and theorems about partially ordered sets and finite groups that will be used throughout this thesis. Some knowledge of the rudiments of linear algebra, group theory, topology and the theory of partially ordered sets will be assumed. The reader may refer to [23], [2], [45] and [35], respectively, for the necessary background on these topics.

Definition 2.1 *Let P be a locally finite poset.*

(1) The zeta function ζ and the Möbius function μ are defined on $P \times P$ as follows.

$$\zeta(x,y) = \begin{cases} 1 & \text{if } x \leq y \\ 0 & \text{otherwise.} \end{cases}$$

$$\mu(x,y) = \begin{cases} 0 & \text{if } x \not\leq y \\ 1 & \text{if } x = y \\ -\sum_{x \leq z < y} \mu(x,z) & \text{if } x < y. \end{cases}$$

The Möbius function on P will often be written as μ_P.

(2) If P has a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$ then $\mu_P(\hat{0},\hat{1})$ is called the Möbius number of P.

(3) A chain in P is a subset $C \subseteq P$ such that $x \leq y$ or $y \leq x$ for all $x, y \in C$. An antichain in P is a subset $A \subseteq P$ such that neither $x \leq y$ nor $y \leq x$ holds for any pair of distinct elements $x, y \in A$.

(4) For $x, y \in P$, we say y covers x if $x < y$ and there is no $z \in P$ such that $x < z < y$.

(5) A closure on P is a function $^{-}: P \to P$ satisfying the following three conditions.

(a) $x \leq \overline{x}$ for all $x \in P$.

(b) If $x, y \in P$ with $x \leq y$ then $\overline{x} \leq \overline{y}$.

(c) $\overline{\overline{x}} = \overline{x}$ for all $x \in P$.

(6) If $^{-}$ is a closure map on P then $\overline{P} := \{x \in P : \overline{x} = x\}$.

Note that if $^{-}: P \to P$ is a closure map, then $\overline{P}$ is a poset with order induced by the order on P.

Definition 2.2 *Let L be a finite lattice.*

(1) $\hat{0}$ and $\hat{1}$ will denote, respectively, the unique minimum element of L and the unique maximum element of L.

(2) An atom of L is an element which covers $\hat{0}$. A coatom of L is an element which is covered by $\hat{1}$.

(3) A complement to $x \in L$ is an element $y \in L$ such that $x \wedge y = \hat{0}$ and $x \vee y = \hat{1}$. Also, $x^{\perp}$ will denote the set of complements to x in L.

The closure and complement theorems of Crapo, which are stated below, will be used many times.

Theorem 2.3 ([12], Theorem 1) *Let P be a finite poset and let $^{-}: P \to P$ be a closure map. Fix $x, y \in P$ such that $y \in \overline{P}$. Then*

$$\sum_{\overline{z}=y} \mu_P(x, z) = \begin{cases} \mu_{\overline{P}}(x, y) & \text{if } \overline{x} = x \\ 0 & \text{otherwise.} \end{cases}$$

Theorem 2.4 ([11], Theorem 3) *Let L be a finite lattice and fix $x \in L$. Then*

$$\mu_L(\hat{0}, \hat{1}) = \sum_{y,z \in x^\perp} \mu_L(\hat{0}, y)\zeta_L(y, z)\mu_L(z, \hat{1}).$$

In particular, if $x^\perp$ is an antichain, then

$$\mu_L(\hat{0}, \hat{1}) = \sum_{y \in x^\perp} \mu_L(\hat{0}, y)\mu_L(y, \hat{1}).$$

The next two results appear as Corollaries 3.9.3 and 3.9.4, respectively, in [45]. The second of the two will be extremely useful for us.

Theorem 2.5 (Weisner) *Let L be a finite lattice with $|L| > 1$, and let $a \in L$ with $a \neq \hat{1}$. Then*

$$\sum_{x \wedge a = \hat{0}} \mu(x, \hat{1}) = 0.$$

Lemma 2.6 *Let L be a finite lattice and let $X \subseteq L$ contain all the coatoms of L. Set $\mathcal{Y} = \left\{Y \subseteq X : \bigwedge_{y \in Y} y = \hat{0}\right\}$. Then*

$$\mu_L(\hat{0}, \hat{1}) = \sum_{Y \in \mathcal{Y}} (-1)^{|Y|}.$$

The following lemma will be used in the calculation of the Möbius numbers of subgroup lattices of some symmetric groups and some orthogonal groups over finite fields. A proof appears on page 128 of [45].

Lemma 2.7 *Let Π_n be the lattice of partitions of $[n]$ into subsets, ordered by refinement, so $[A_1; \ldots; A_k] \leq [B_1; \ldots; B_l]$ if and only if each A_i is a subset of some B_j. Then*

$$\mu_{\Pi_n}(\hat{0}, \hat{1}) = (-1)^{n-1}(n-1)!$$

If P is a finite poset, there is a finite dimensional abstract simplicial complex naturally associated to P, as described below.

Definition 2.8 *Let P be a finite poset. The order complex of P, denoted by $\Delta(P)$ is the abstract simplicial complex whose i-simplices are the chains $x_1 < x_2 < \ldots < x_{i+1}$ from P.*

In the cases which will be of most interest to us, we will examine $\Delta(P)$ when P is obtained by removing $\hat{0}$ and $\hat{1}$ from a finite lattice. Hence we make the following definitions.

Definition 2.9 *Let P be a finite poset.*

(1) If P has a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$ then P^* is the poset $P \setminus \left\{\hat{0}, \hat{1}\right\}$.

(2) $\hat{P}$ is the poset obtained by adjoining a minimum element $\hat{0}$ and a maximum element $\hat{1}$ to P.

Now for any poset P, one defines the chain space $C_i = C_i(\Delta(P))$ to be the complex vector space whose basis is the set of i-simplices from $\Delta(P)$. The linear transformation $\partial_i : C_i \to C_{i-1}$ is defined as follows. If $X = x_1 < \ldots < x_{i+1}$ is an i-simplex from $\Delta(P)$, and thereby an element of our basis of C_i, then

$$\partial_i(X) = \sum_{j=1}^{i+1}(-1)^{j-1}(X \setminus x_j) \in C_{i-1}.$$

It is well-known that the composition $\partial_i \circ \partial_{i+1}$ is the zero map (see for example [35], p. 15) and that $\delta_0 = 0$, so one defines for each $i \geq 0$ the reduced homology group $\tilde{H}_i(\Delta(P)) := ker(\partial_i)/im(\partial_{i+1})$. Furthermore, $\tilde{H}_{-1}(\Delta(P))$ is defined to be zero unless $P = \left\{\hat{0}, \hat{1}\right\}$, in which case $\tilde{H}_{-1}(\Delta(P)) := C_{-1}(\Delta(P))$ has dimension one.

Definition 2.10 *Let P be a finite poset with a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$, and let r be the length of the longest chain from P. For $-1 \leq i \leq r-2$, $C_i(P) := C_i(\Delta(P^*))$ and $\tilde{H}_i(P) := \tilde{H}_i(\Delta(P^*))$.*

There are two reasons that the definition above uses P^* rather than P. The first is that it can be shown that if P has a unique maximum or minimum element then $\tilde{H}_i(\Delta(P)) = 0$ for all i (see [40], 1.5). The second, which is of more interest to us, is that a well-known topological invariant of $\Delta(P^*)$ is intimately related with the Möbius function on P.

Theorem 2.11 (P. Hall) *Let P be a finite poset with a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$. Let r be the length of the longest chain from P. For $-1 \leq i \leq r-2$, let $c_i = c_i(P)$ be the number of chains $\hat{0} = x_0 < x_1 < \ldots < x_{i+1} < x_{i+2} = \hat{1}$ from P. Then*

$$\mu_P(\hat{0}, \hat{1}) = \sum_{i=-1}^{r-2} (-1)^i c_i.$$

Proof: See [20], 2.2. □

Note that $c_i(P) = dim(C_i(P^*))$. Therefore, $\mu_P(\hat{0}, \hat{1})$ is equal to the reduced Euler characteristic $\tilde{\chi}(\Delta(P^*))$ (see [35], p.124 for the definition of the Euler characteristic). We digress from our discussion of order complexes to give two results on Möbius functions which follow from this theorem.

Corollary 2.12 *Let P be a finite poset. Let Q be the dual poset of P, so P and Q have the same underlying set and $y \leq_Q x$ if and only if $x \leq_P y$. Then for all $x, y \in P$, $\mu_Q(y, x) = \mu_P(x, y)$.*

Proof: We apply Hall's theorem to the intervals $[x, y]_P$ and $[y, x]_Q$. Clearly, the number of chains of a given length is the same in both intervals. □

The following well-known lemma is often helpful in calculating the Möbius function of a lattice. It allows one to ignore all elements which are not meets of coatoms.

Lemma 2.13 *Let L be a finite lattice and let $\mathcal{M}$ be the set of coatoms of L. Define $\hat{L}$ to be the meet semilattice generated by $\mathcal{M}$ with $\hat{1}$ adjoined. Then for all $x \in L$,*

$$\mu_L(x,\hat{1}) = \begin{cases} \mu_{\hat{L}}(x,\hat{1}) & \textit{if } x \in \hat{L} \\ 0 & \textit{otherwise} \end{cases}$$

Proof: We use induction on the length of the longest chain from x to $\hat{1}$. If $x = \hat{1}$ the claim clearly holds. Now assume that $x < \hat{1}$. Using the definition of μ and Corollary 2.12, along with the inductive hypothesis, we get

$$\mu_L(x,\hat{1}) = -\sum_{x<y\leq\hat{1}} \mu_L(y,\hat{1}) = -\sum_{\substack{x<y\leq\hat{1}\\ y\in\hat{L}}} \mu_{\hat{L}}(y,\hat{1}).$$

Now if $x \in \hat{L}$, this last sum is equal to $\mu_{\hat{L}}(x,\hat{1})$. If $x \notin \hat{L}$, let $\hat{x}$ be the meet of all of the coatoms $c \in L$ such that $x < c$. In this case we have

$$-\sum_{\substack{x<y\leq\hat{1}\\ y\in\hat{L}}} \mu_{\hat{L}}(y,\hat{1}) = -\sum_{\substack{\hat{x}\leq y\\ y\in\hat{L}}} \mu_{\hat{L}}(y,\hat{1}) = 0,$$

and the proof is complete. □

We now return to our discussion of order complexes. Some of the main results in this thesis involve the action of a finite group G on a poset P. We say G acts on the poset P if G acts on the set P so that if $x, y \in P$ with $x \leq y$ and $g \in G$ then $x^g \leq y^g$. If G acts on P, there is a generalized character of G arising from this action, as described below.

Theorem 2.14 (Hopf trace formula) *Let P be a finite poset with a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$. Let r be the length of the longest chain in P. Let G be a group acting on P. Then for each $i \in [-1, r-2]$, the action of G on P determines a permutation representation of G on $C_i(P)$. The subspaces $ker(\partial_i)$ and $im(\partial_{i+1})$ are invariant under the action of G, so G also acts as a group of linear transformations on $\tilde{H}_i(P)$. Furthermore, for all $g \in G$ we have*

$$\sum_{i=-1}^{r-2} (-1)^i tr(g, C_i(P)) = \sum_{i=-1}^{r-2} (-1)^i tr(g, \tilde{H}_i(P)).$$

A proof of this theorem can be found in [48]. This theorem leads to the following definition.

Definition 2.15 *Let P be a finite poset with a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$. Let G be a finite group acting on P. The Lefschetz character for this action, denoted by $\Lambda_{P,G}$ is defined by*

$$\Lambda_{P,G}(g) = \sum_{i \geq -1} (-1)^i tr(g, \tilde{H}_i(P^*)).$$

Combining Theorems 2.11 and 2.14 gives the following well-known result.

Corollary 2.16 *Let P be a finite poset with a unique minimum element $\hat{0}$ and a unique maximum element $\hat{1}$. Let G be a finite group acting on P. For each $g \in G$, let $P^g = \{x \in P : x^g = x\}$. Then*

$$\Lambda_{P,G}(g) = \mu_{P^g}(\hat{0}, \hat{1}).$$

Furthermore, $\Lambda_{P,G}$ is a generalized character of G. That is, there exist characters χ_1 and χ_2 of G such that $\Lambda_{P,G} = \chi_1 - \chi_2$.

Proof: Note that $tr(g, C_i(P))$ is simply the number of chains of length i from P which are fixed by g. Since P is finite and G preserves order on P, any chain from P fixed by $g \in G$ is a chain from P^g. The first claim now follows from the two theorems. The second claim is obvious, since $\Lambda_{P,G}$ is defined to be a difference of permutation characters. □

It turns out that the action of a group G on a poset P can provide useful information about the Möbius number of the subgroup lattice of G. In particular, assume that there is no $x \in P$ which is fixed by all $g \in G$, and let $\mathcal{I}$ be the ideal in the subgroup lattice of G consisting of subgroups which fix at least one point from P. If this ideal is large and $\sum_{H \in \mathcal{I}} \mu(1, H)$ can be calculated with the aid of P, but without explicit knowledge of all of the elements of $\mathcal{I}$, then one might hope to determine $\mu(1, G)$ by calculating the sum of the Möbius numbers of the proper subgroups of G not contained in $\mathcal{I}$ using ad hoc methods. The following lemma, when combined with Lemma 2.6, gives a method which can be useful in determining $\sum_{H \in \mathcal{I}} \mu(1, H)$.

Lemma 2.17 *Let G be a finite group acting on a finite set P. For $x \in P$, let $G_x = \{g \in G : x^g = x\}$. Set $\mathcal{I} = \{G_x : x \in P\}$. Define $\mathcal{S} = \{E \subseteq \mathcal{I} : \bigcap_{H \in E} H \neq 1\}$ and $\mathcal{T} = \left\{Q \subseteq P : \bigcap_{x \in Q} G_x \neq 1\right\}$. Then*

$$\sum_{E \in \mathcal{S}} (-1)^{|E|} = \sum_{Q \in \mathcal{T}} (-1)^{|Q|}.$$

Proof: For $E \in \mathcal{S}$, let $\mathcal{T}_E = \{Q \in \mathcal{T} : E = \{G_x : x \in Q\}\}$. Then

$$\mathcal{T} = \dot{\bigcup}_{E \in \mathcal{S}} \mathcal{T}_E,$$

and it is sufficient to show that for each $E \in \mathcal{S}$ we have $\sum_{Q \in \mathcal{T}_E} (-1)^{|Q|} = (-1)^{|E|}$. Fix $E \in \mathcal{S}$, and for each $H \in E$ let $P_H = \{x \in P : G_x = H\}$. Then $Q \in \mathcal{T}_E$ if and only if $Q = \dot{\bigcup}_{H \in E} Q_H$, where each Q_H is an arbitrary nonempty subset of P_H. Using the principle of inclusion-exclusion and the fact that the Q_H are chosen independently, we get

$$\sum_{Q \in \mathcal{T}_E} (-1)^{|Q|} = \prod_{H \in E} \sum_{\emptyset \neq Q_H \subseteq P_H} (-1)^{|Q_H|} = \prod_{H \in E} (-1) = (-1)^{|E|},$$

and the proof is complete. $\square$

Chapter 3

A Lefschetz character for projective classical groups in prime dimension

In this chapter, some Lefschetz characters for projective classical groups defined in odd prime dimensions over fields of odd order will be determined. These characters will arise from the actions of these groups on the posets of their nontrivial reducible subgroups. We will begin with the definitions of the three families of classical groups which we will consider and a review of some of their properties which will be important to us.

3.1 Definitions and statement of the main theorems

3.1.1 The linear groups

A linear space is simply a vector space over some field $\mathbf{F}$. We will be interested in linear spaces over finite fields of odd order.

Definition 3.1 *Let n be a positive integer and let q be an odd prime power. Let V be a linear space of dimension n over $\mathbf{F}_q$.*

(1) $GL(V)$ is the group of nonsingular linear transformations on V.

(2) Z is the center of $GL(V)$, so Z consists of the scalar transformations.

(3) For $G \leq GL(V)$, $\overline{G}$ will always denote the quotient group GZ/Z.

(4) $PGL(V) := \overline{GL(V)}$.

(5) For $G \leq PGL(V)$, G^* will always denote the complete preimage of G in $GL(V)$, and for $g \in PGL(V)$, g^* will denote an element of $GL(V)$ such that $g^*Z = g$. This element g^* may be arbitrary or it may be specified.

(6) $SL(V) := \{x \in GL(V) : det(x) = 1\}$.

(7) $L(V) := PSL(V) := \overline{SL(V)}$

Let $V(n, q)$ be the space of $1 \times n$ row vectors over $\mathbf{F}_q$, and let $e_1, \ldots, e_n$ be the standard basis for $V(n, q)$. For any basis $v_1, \ldots, v_n$ of any n-dimensional vector space V over $\mathbf{F}_q$, the map $v_i \mapsto e_i$ determines an isomorphism between V and $V(n, q)$ and an isomorphism between $GL(V)$ and the group $GL_n(q)$ of nonsingular $n \times n$ matrices over $\mathbf{F}_q$.

3.1.2 The unitary groups

Recall (or see [2]. Chapter 7) that if $\mathbf{F}$ is a field with an automorphism a of order two and V is a vector space over $\mathbf{F}$, a hermitian form on V associated with a is a map $f : V \times V \to \mathbf{F}$ which is biadditive and satisfies the conditions $f(\alpha v, w) = \alpha f(v, w)$, $f(v, \alpha w) = \alpha^a f(v, w)$ and $f(w, v) = f(v, w)^a$ for all $v, w \in V$ and $\alpha \in \mathbf{F}$. Frequently we will suppress the symbol f and write (v, w) for $f(v, w)$. A unitary space (V, f) is a linear space V over some field $\mathbf{F}$, along with a hermitian form $f : V \times V \to \mathbf{F}$. We will be concerned with the case in which $\mathbf{F} = \mathbf{F}_{q^2}$ and a is the automorphism $\alpha \mapsto \alpha^q$. Note that this is the only automorphism of $\mathbf{F}$ which has order two.

Definition 3.2 *Let n be a positive integer and let q be an odd prime power. Let V be a unitary space of dimension n over $\mathbf{F}_{q^2}$.*

(1) $GU(V) := GU(V, f) := \{g \in GL(V) : (vg, wg) = (v, w)$ for all $v, w \in V\}$.

(2) $PGU(V) := PGU(V, f) := \overline{GU(V, f)}$.

(3) $SU(V) := SU(V, f) := GU(V, f) \cap SL(V)$.

(4) $PSU(V) := PSU(V,f) := \overline{SU(V,f)}$.

Given the above definition, it is not immediately clear what is the relation between $GU(V,f)$ and $GU(V',f')$ if (V,f) and (V',f') are both n-dimensional unitary spaces over $\mathbf{F}_q$, so we will quote some well-known results.

Definition 3.3 *Let (V,f) be a unitary space.*

(1) For $v \in V$, $v^\perp := \{w \in V : (v,w) = 0\}$.

(2) For $W \leq V$, $W^\perp := \{v \in V : (v,w) = 0 \textit{ for all } w \in W\}$.

(3) For $W \leq V$, $rad(W) := W \cap W^\perp$.

(4) $W \leq V$ *is called nondegenerate if* $rad(W) = 0$.

.

We now recall the above-mentioned well-known results. They all appear in Chapter 7 of [2]. Let $v = (v_i)$ and $x = (x_{ij})$ be a row vector and a matrix with entries in the field $\mathbf{F}_{q^2}$. Then $v^{(q)} := (v_i^q)$ and $x^{(q)} := (x_{ij}^q)$ are the vector and matrix obtained by raising the entries of v and x to the q^{th} power. If J is an $n \times n$ matrix over $\mathbf{F}_{q^2}$ such that $J^{(q)} = {}^tJ$ then a Hermitian form f_J on $V(n,q^2)$ is determined by setting $f_J(v,w) = vJ({}^tw^{(q)})$. Conversely, every Hermitian form corresponds to such a matrix. In particular, if (V,f) is a unitary space over $\mathbf{F}_{q^2}$ with basis $x_1, \ldots, x_n$, define $J = (a_{ij})$ by $a_{ij} = (x_i, x_j)$. It is easily seen that $J^{(q)} = {}^tJ$. Also, the map $x_i \mapsto e_i$ now determines an isometry, that is, a linear isomorphism $\alpha : V \to V(n,q^2)$ such that $f(v,w) = \alpha(v)J({}^t\alpha(w)^{(q)})$ for all $v, w \in V$. Now (V,f) is nondegenerate if and only if the associated matrix J is nonsingular. For any two forms on $V = V(n,q^2)$ given by matrices J and K, there is an isometry between (V,f_J) and (V,f_K) if and only if there exists some $A \in GL_n(q^2)$ such that $K = AJ({}^tA)$. If such an A exists, the map $g \mapsto AgA^{-1}$ determines an isomorphism between $GU(V,f_J)$ and $GU(V,f_K)$. If J is nonsingular and $J^{(q)} = {}^tJ$, then there exists some $A \in GL_n(q^2)$ such that $AJ({}^tA) = I$, the identity matrix. Thus all nondegenerate unitary spaces of a given dimension are isometric, and so $GU(V,f) \cong GU(V',f')$ for any two nondegenerate unitary spaces of the same dimension over $\mathbf{F}_{q^2}$. This justifies writing $GU(V)$ for $GU(V,f)$ once a unitary space (V,f) has been given. Also, if V is an n-dimensional unitary space over $\mathbf{F}_{q^2}$, then $GU(V)$ is isomorphic to the group $GU(V(n,q),f_I) = \left\{g \in GL_n(q^2) : g^{-1} = {}^tg^{(q)}\right\}$.

The following result appears in [43] and will be very useful.

Lemma 3.4 *Let V be a unitary space of finite dimension over $\mathbf{F}_q$. If $g,h \in GU(V)$ are conjugate in $GL(V)$ then they are already conjugate in $GU(V)$.*

3.1.3 The orthogonal groups

Recall (or see [2], Chapter 7) that if V is a vector space over a field $\mathbf{F}$, a symmetric form on V is a bilinear map $f : V \times V \to F$ such that $f(v,w) = f(w,v)$ for all $v,w \in V$. We are interested in the case $\mathbf{F} = \mathbf{F}_q$ with q odd. In that case, an orthogonal space (V,f) over F is a linear space V, along with a symmetric from f on V.

Definition 3.5 *Let n be a positive integer and q an odd prime power. Let (V,f) be an orthogonal space of dimension n over $\mathbf{F}_q$.*

(1) $GO(V) := GO(V,f) := \{g \in GL(V) : (vg,wg) = (v,w)$ for all $v,w \in V\}$.

(2) $PGO(V) := PGO(V,f) := \overline{GO(V,f)}$.

(3) $SO(V) := SO(V,f) := GO(V,f) \cap SL(V)$.

(4) $PSO(V) := PSO(V,f) := \overline{SO(V,f)}$.

(5) $\Omega(V) := \Omega(V,f)$ is the commutator subgroup of $GO(V,f)$. Note that since any commutator in $GL(V)$ is contained in $SL(V)$, $\Omega(V,f) \leq SO(V,f)$.

(6) $P\Omega(V) := P\Omega(V, f) := \overline{\Omega(V, f)}$.

As in the unitary case, for any orthogonal space (V, f) of dimension n over $\mathbf{F}_q$ there is an isometry $\alpha : (V, f) \to (V(n, q), f_J)$, where now the matrix J satisfies $J = {}^tJ$. However, in the orthogonal case, for each pair (n, q), there are two isometry classes of nondegenerate orthogonal forms on $V(n, q)$, as described in the results below.

Definition 3.6 *Let $V = (V, f)$ be a 2-dimensional orthogonal space over $\mathbf{F}_q$ with q odd. V is a hyperbolic plane if V has a basis x, y such that $(x, x) = (y, y) = 0$ and $(x, y) = 1$. V is anisotropic if $(x, x) \neq 0$ for all $0 \neq x \in V$.*

Definition 3.7 *Let $V = (V, f)$ be an orthogonal space of finite dimension over $\mathbf{F}_q$, with q odd.*

(1) V has type $+$ if $dim(V) = 2k$ and $V = \perp_{i=1}^{k} H_i$ with each $(H_i, f_{|H_i})$ a hyperbolic plane.

(2) V has type $-$ if $dim(V) = 2k$ and $V = (\perp_{i=1}^{k-1} H_i) \perp U$ with each $(H_i, f_{|H_i})$ a hyperbolic plane and $(U, f_{|U})$ anisotropic.

(3) V has type $\diamond$ if $dim(V) = 2k + 1$ and $V = (\perp_{i=1}^{k} H_i) \perp \langle x \rangle$ with each $(H_i, f_{|H_i})$ a hyperbolic plane and $(x, x) \neq 0$ a square in $\mathbf{F}_q$.

(4) V has type $\triangle$ if $dim(V) = 2k + 1$ and $V = (\perp_{i=1}^{k} H_i) \perp \langle x \rangle$ with each $(H_i, f_{|H_i})$ a hyperbolic plane and (x, x) a nonsquare in $\mathbf{F}_q$.

(5) $\mathcal{J}$ is the set of decomposition types $\{+, -, \diamond, \triangle\}$. Also, $\mathcal{J}_e := \{+, -\}$ and $\mathcal{J}_o := \{\diamond, \triangle\}$. For $n \in \mathbf{N}$, $\mathcal{J}_n := \mathcal{J}_e$ if n is even and $\mathcal{J}_o$ if n is odd.

The next lemma is well-known. A proof can be found in [28] on page 28.

Lemma 3.8 *An orthogonal space V over a field of odd order is of exactly one of the decomposition types $+, -, \diamondsuit, \triangle$.*

We will use the following Lemma several times. The proof follows immediately from Definition 3.7 and the fact that if J is the matrix of a nondegenerate symmetric form on an orthogonal space V over $\mathbf{F}_q$ with respect to some basis, the condition $det(J) \in \mathbf{F}_q^2$ is independent of the given basis (see [28], Section 2.5).

Lemma 3.9 *Fix an odd prime power q. There is a group structure $\mathcal{J}(q)$ defined on $\mathcal{J}$ with addition $\oplus$ given as follows. For $\alpha, \beta \in \mathcal{J}$ let $\alpha \oplus \beta$ be the type of the space obtained by forming the orthogonal sum of a nondegenerate orthogonal space over $\mathbf{F}_q$ of type α and a nondegenerate orthogonal space over $\mathbf{F}_q$ of type β. This addition is well defined and makes $\mathcal{J}$ an abelian group. The identity element is $+$. If $q \equiv 1 \pmod 4$ then $\mathcal{J}$ is noncyclic. If $q \equiv 3 \pmod 4$ then $\mathcal{J}$ is cyclic, generated by $\diamondsuit$ and by $\triangle$.*

Definition 3.10 *Let n be a nonnegative integer and let q be an odd prime power. For $\alpha \in \mathcal{J}_n$, $GO_n^{\alpha}(q)$ is the group of isometries of $(V(n,q), f)$, where f is a symmetric form of decomposition type α on V.*

We have seen that for any n-dimensional orthogonal space (V, f) over $\mathbf{F}_q$, $GO(V, f) \cong GO_n^{\alpha}(q)$ for some $\alpha \in \mathcal{J}_n$. The following result is also well-known (see [2], p.89).

Lemma 3.11 *Let n be an odd integer and let q be an odd prime power. Then $GO_n^{\diamondsuit}(q) \cong GO_n^{\triangle}(q)$.*

Thus, when $dim(V)$ is odd, we will often write $GO(V)$ for $GO(V, f)$ if f is a nondegenerate symmetric form on V.

3.1.4 The Coxeter tori

Before stating the main theorem of this chapter, we must recall the existence of certain subgroups of the classical groups which we have defined above in order to specify some induced characters.

Definition 3.12 *Fix a linear space V of odd dimension n over $\mathbf{F}_q$, with q odd. Fix a basis $B = \{e_1, \ldots, e_n\}$ for V. Define $f_n^*(B)$ to be the element of $GL(V)$ such that $e_i f_n^*(B) = e_{i+1}$ for $1 \leq i < n$ and $e_n f_n^*(B) = e_1$. Now define $f_n(B) = f_n^*(B)Z \in PGL(V)$ and $F_n(B) = \langle f_n(B) \rangle \leq PGL(V)$.*

Proposition 3.13 *Let n be odd and let q be an odd prime power. Let B be the standard basis for $V = V(n,q)$ and set $f = f_n^*(B)$. We may choose a nondegenerate symmetric form s on V so that $f \in \Omega(V,s)$. If q is a square, we may choose a nondegenerate hermitian form h on V so that $f \in SU(V,h)$.*

Proof: The matrix P of f is a permutation matrix corresponding to an n-cycle in S_n, and since n is odd we have $f \in SL(V)$. Let both h and s be defined by the identity matrix. Note that $P^{(q)} = P$ and $P^{-1} = {}^tP$. It follows that $f \in SU(V,h) \cap SO(V,s)$. It is known that $\Omega(V,s)$ has index two in $SO(V,s)$ (see [28], p. 29). Since $|f| = n$ is odd, $f \in \Omega(V,s)$. □

Proposition 3.14 *Let Φ_m be the m^{th} cyclotomic polynomial, let d be an odd prime and let q be an odd prime power. Then for $1 \leq i < d$ we have*

$$gcd(\Phi_i(q), \Phi_d(q)) = \begin{cases} d & \text{if } i = 1 \text{ and } d | q-1 \\ 1 & \text{otherwise} \end{cases}$$

Furthermore, if $d|q-1$ then d^2 does not divide $\Phi_d(q)$.

Proof: See page 112 of [18]. □

Definition 3.15 *Let V be a linear space over any field $\mathbf{F}$. A subgroup H of $GL(V)$ is called reducible if and only if H fixes some nontrivial proper subspace of V. Also, $H \leq PGL(V)$ is called reducible if and only if H^* is reducible.*

Lemma 3.16 *Let V be a linear space of odd prime dimension d over $\mathbf{F}_q$ with q odd. $GL(V)$ contains a conjugacy class $\mathcal{C}_d$ of cyclic subgroups, called Coxeter tori, with the following properties.*

(1) If $C^* \in \mathcal{C}_d$ then $|C^*| = q^d - 1$ and $Z \le C^*$.

(2) A cyclic subgroup $H \le GL(V)$ is irreducible if and only if H is contained in some element of $\mathcal{C}_d$ and H is not contained in Z.

(3) If $H \le C^*$ for some $C^* \in \mathcal{C}_d$ and $H \not\le Z$, then $C_{GL(V)}(H) = C^*$.

(4) For each $C^* \in \mathcal{C}_d$ there exists a basis B of V such that the normalizer N^* of C^* in $GL(V)$ is the semidirect product of C^* by $F_d^*(B)$. In particular, there is a generator f of $F_d^*(B)$ such that for each $c \in C^*$, we have $c^f = c^q$.

(5) If $C^* \in \mathcal{C}_d$ then $[C^* : C^* \cap SL(V)] = [GL(V) : SL(V)]$

Furthermore, if q is a square and h is a nondegenerate hermitian from on V then the following claims hold.

(6) For each $C^* \in \mathcal{C}_d$, $|C^* \cap GU(V, h)| = 1$ or $\sqrt{q}^d + 1$, and both orders occur. The groups of order $\sqrt{q}^d + 1$ contain $Z \cap GU(V, h)$ and act irreducibly on V.

(7) If $C^* \in \mathcal{C}_d$ with $|C^* \cap GU(V, h)| = \sqrt{q}^d + 1$, then

$$[C^* : C^* \cap SU(V)] = [GU(V) : SU(V, h)].$$

(8) If $C^* \in \mathcal{C}_d$ with $|C^* \cap GU(V, h)| = \sqrt{q}^d + 1$, then there exists a basis B of V such that the normalizer N^* of C^* in $GL(V)$ is the semidirect product of C^* by $F_d^*(B)$. In particular, there is a generator f of $F_d^*(B)$ such that for each $c \in C^* \cap GU(V, h)$, we have $c^f = c^q$.

Finally, if s is any nondegenerate symmetric form on V, then the following claim holds.

(9) For any $C^* \in \mathcal{C}_d$, $C^* \cap GO(V, s) = \langle -1 \rangle$.

Proof: We identify V with the $\mathbf{F}_q$-space $\mathbf{F}_{q^d}$. Let α generate $\mathbf{F}_{q^d}^*$. The map $a : \beta \mapsto \alpha\beta$ is a linear transformation of order $q^d - 1$ on $\mathbf{F}_{q^d}$. Note that $b = a^{\frac{q^d-1}{q-1}}$ generates $\mathbf{F}_q^*$, and thus $\langle b \rangle = Z$. Therefore, the conjugacy class of $\langle a \rangle$ satisfies (1).

Let $H = \langle h \rangle$ be cyclic of order n, and let $\phi : H \mapsto GL(V)$ be an irreducible representation, with $T = \phi(h)$. Then V is an irreducible module for the ring $R = \mathbf{F}_q[T]$. By Schur's Lemma (see [25], p. 4), R is a field. Since V is an irreducible R-module, $V \cong R$. Since $|V| = q^d$, $V \cong \mathbf{F}_{q^d}$ and T acts on V as multiplication by some nonzero element of $\mathbf{F}_{q^d}$. Thus H is contained in a conjugate of $\langle a \rangle$. Conversely, it is known (see [25], problem 9.20) that the degree of every faithful irreducible $\mathbf{F}_q$-representation of H is the smallest number m such that $n | q^m - 1$. If $H \leq \langle a \rangle$ then $n | q^d - 1$. By Proposition 3.14, if $n | q^m - 1$ with $m < d$ then $n | q - 1$. Since the only subgroup of $\langle a \rangle$ of order $q - 1$ is Z, either $H \leq Z$ or H is irreducible. Thus claim (2) holds.

Let $y \in \langle a \rangle \setminus Z$. Since $\langle y \rangle$ is irreducible, $K = C_{GL(V)}(y)$ is cyclic by Schur's Lemma. Since K is irreducible, $|K|$ divides $q^d - 1$ by the argument on the above paragraph, and it follows immediately that $K = \langle a \rangle$. This gives claim (3).

Let $\mathcal{G}$ be the Galois group of $\mathbf{F}_{q^d}$ over $\mathbf{F}_q$, so $\mathcal{G}$ is generated by the map $f : \beta \mapsto \beta^q$. Then we can consider f to be an element of $GL(V)$. Note that $|f| = d$ and $a^f = a^q$. By the normal basis theorem (see for example [41], Theorem 8.7.2), there exists an $\mathbf{F}_q$-basis B for $\mathbf{F}_{q^d}$ such that $f = f_d^*(B)$. By [28], Table 3.5.H, $\langle f, a \rangle$ is maximal in $GL(V)$, so $N_{GL(V)}(\langle a \rangle) = \langle f, a \rangle$ and claim (4) holds.

Now

$$det(a) = \prod_{\sigma \in \mathcal{G}} \alpha^\sigma = \prod_{i=0}^{d-1} \alpha^{q^i} = \alpha^{\frac{q^d-1}{q-1}},$$

so

$$[\langle a \rangle : \langle a \rangle \cap SL(V)] = q - 1 = [GL(V) : SL(V)],$$

and claim (5) holds.

Now assume q is a square. It is straightforward to verify that the form on $V = \mathbf{F}_{q^d}$ given by

$$(v, w) = \sum_{\sigma \in \mathcal{G}} (vw^{\sqrt{q}})^{\sigma}$$

is a nondegenerate hermitian form on V. By the equivalence of all such forms, we may assume that any given nondegenerate form h on V is the one described above. We write $\langle a \rangle_u$ for $\langle a \rangle \cap GU(V, h)$. It is easily seen that multiplication by $\beta \in \mathbf{F}_{q^d}$ preserves h if and only if $\beta^{\sqrt{q}^d+1} = 1$. Thus $|\langle a \rangle_u| = \sqrt{q}^d + 1$. Now let $K = \langle k \rangle$ be a nontrivial irreducible cyclic subgroup of $GU(V, h)$. By [24], Satz 4a, $|K|$ divides $\sqrt{q}^d + 1$, and it follows that K is conjugate in $GL(V)$ to some $J \leq \langle a \rangle_u$. By Lemma 3.4, H is conjugate in $GU(V, h)$ to J. Thus $G_{GU(V,h)}(K)$ is conjugate to $\langle a \rangle_u$ in $GU(V, h)$ and it follows from (3) that all elements of $\mathcal{C}_d$ which intersect $GU(V, h)$ nontrivially intersect it in a conjugate of $\langle a \rangle_u$. Claim (6) now follows immediately from the fact that $|Z \cap GU(V, h)| = \sqrt{q} + 1$.

Let c generate $\langle a \rangle_u$. Then we can take c to be multiplication by $\alpha^{\sqrt{q}-1}$. Thus

$$det(c) = \prod_{\sigma \in \mathcal{G}} (\alpha^{\sqrt{q}-1})^{\sigma} = \prod_{i=0}^{d-1} \alpha^{(\sqrt{q}-1)q^i} = \alpha^{\frac{q^d-1}{\sqrt{q}^d+1}}.$$

Thus

$$[\langle a \rangle_u : \langle a \rangle_u \cap SU(V, h)] = \sqrt{q} + 1 = [GU(V, h) : SU(V, h)],$$

and claim (7) holds.

To prove claim (8), it is sufficient to show that $f \in GU(V, h)$. This is obvious, since f acts on $\mathbf{F}_{q^d}$ like a generator of $\mathcal{G}$.

Finally, claim (9) follows from Satz 3a of [24] and claim (2), since for any nondegenerate symmetric form s on V, $Z \cap GO(V, s) = \langle -1_V \rangle$. $\square$

3.1.5 The main theorems

The groups studied in this chapter are those contained in the set defined below.

Definition 3.17 *Let q be an odd prime power, and let V be a linear space of dimension d over $\mathbf{F}_q$. If q is a square, let h be a fixed nondegenerate hermitian form on V. Also,* *let s be a fixed nondegenerate symmetric form on V.*

(1) $PC_L(V) := \{PGL(V), L(V)\}$.

(2) $PC_U(V) := \begin{cases} \{PGU(V,h), PSU(V,h)\} & q \text{ a square} \\ \emptyset & q \text{ a nonsquare} \end{cases}$

(3) $PC_O(V) := \{PSO(V,s), P\Omega(V,s)\}$.

(4) $PC(V) := PC_L(V) \cup PC_U(V) \cup PC_O(V)$.

Note that if $d = dim(V)$ is odd, there is no ambiguity in referring to the unitary and orthogonal groups without specifying a form. Also note that if d is odd then $PSO(V) \cong SO(V)$, so in what follows we will work with $SO(V)$ and $\Omega(V)$ whenever it is convenient to do so. Often a lemma will begin with a phrase such as "Let V be a linear space or a nondegenerate unitary or orthogonal space and let $G \in PC(V)$". This should be taken to imply that if V is a linear space then $G \in PC_L(V)$, and so on. We now give some further general definitions.

Definition 3.18 *Let V be a linear space or a nondegenerate unitary or orthogonal space. Define $G(V) := GL(V)$ if V is a linear space, $G(V) := GU(V)$ if V is a unitary space, and $G(V) := GO(V)$ if V is an orthogonal space.*

Definition 3.19 *Let V be a vector space of odd dimension n over $\mathbf{F}_q$. A Coxeter torus of $PGL(V)$ is a subgroup C such that $C^* \in \mathcal{C}_n$. If q is a square then a Coxeter torus of $PGU(V)$ is a subgroup C of $PGU(V)$ such that $|C^*| = \sqrt{q}^n + 1$ and C^* is contained in some $D^* \in \mathcal{C}_n$.*

For a vector space V of odd prime dimension d over a field of odd order, we fix once and for all embeddings of each $G \in PC(V)$ in $PGL(V)$. Obviously, this can be done, since if we take V to be $V(n,q)$ we can embed each G^* in $GL_n(q)$.

Definition 3.20 *Let V be a linear space of odd prime dimension d over a field of odd order. Let s be a nondegenerate symmetric form on V, and if q is a square let h be* *a nondegenerate hermitian form on V. F_d is a fixed subgroup of $PGL(V)$ such that $F_d = F_d(B)$ for some basis B of V and F_d is contained in all elements of $PC(V)$. f_d is a fixed generator of F_d.*

The existence of F_d is guaranteed by Proposition 3.13. Also, by Lemma 3.4, there exists some Coxeter torus of $PGU(V)$ which is normalized by F_d.

The main theorem of this chapter can be stated after defining the posets on which the elements of $PC(V)$ will act.

Definition 3.21 *Let V be a linear space or a nondegenerate unitary or orthogonal space such that V has odd prime dimension over a field of odd order. Let $G \in PC(V)$.*

(1) $\mathcal{C}_1(G) := \{stab_G(W) : 1 < W < V\}$.

(2) $\mathcal{I}_1(G) := \{H : H \leq M$ for some $M \in \mathcal{C}_1(G)\} \cup \{G\}$.

(3) $\mathcal{I}_1^*(G) := \mathcal{I}_1(G) \setminus \{1, G\}$

(4) $\Lambda_{\mathcal{I}_1(G),G}$ is the Lefschetz character for the action of G on $\mathcal{I}_1^*(G)$ by conjugation.

We now state the main theorem in three parts.

Theorem 3.22 *(Linear case) Let V be a linear space of odd prime dimension d over a field $\mathbf{F}_q$ of odd order. Let G be one of $L(V)$ or $PGL(V)$. Let D be a Coxeter torus of $PGL(V)$ which is normalized by F_d, and set $C = D \cap G$. Let N be the normalizer of C in G, so $N = F_dC$. Let θ be the character of N defined by $ker(\theta) = C$ and $\theta(f_d) = e^{2\pi i/d}$. Then $-\Lambda_{1,G}$ is the induced character θ^G.*

Theorem 3.23 *(Unitary case) Let V be a nondegenerate unitary space of odd prime dimension d over a field $\mathbf{F}_q$ of odd order. Let G be one of $PSU(V)$ or $PGU(V)$. Let D be a Coxeter torus of $PGU(V)$ which is normalized by F_d and set $C = D \cap G$. Let*

N be the normalizer of C in G, so $N = F_dC$. Let θ be the character of N defined by $ker(\theta) = C$ and $\theta(f_d) = e^{2\pi i/d}$. Then $-\Lambda_{1,G}$ is the induced character θ^G.

Theorem 3.24 *(Orthogonal case) Let V be a nondegenerate orthogonal space of odd prime dimension d over a field $\mathbf{F}_q$ of odd order.*

(A) Let $G = SO(V)$. Let θ be the linear character of F_d defined by $\theta(f_d) = e^{2\pi i/d}$. Then $-\Lambda_{1,G}$ is the induced character θ^G.

(B) Let $G = \Omega(V)$ and assume $q > 3$. Then there exist $Y_d \leq G$ with Y_d conjugate to F_d in $SO(V)$ and faithful linear characters $\theta_1 : F_d \to \mathbf{C}$ and $\theta_2 : Y_d \to \mathbf{C}$ such that $-\Lambda_{1,G} = \theta_1^G + \theta_2^G$.

The three cases of the main theorem will be proved by first showing that the claim of the theorem holds at the identity element and then examining the nonidentity elements of G. The techniques used in the two parts of the theorem are quite different. For the identity element, we use mostly combinatorial tools, while for the nonidentity elements the proofs use linear algebra and depend more on knowledge of the structure of the elements of $PC(V)$.

3.2 $\Lambda_{\mathcal{I}_1(G),G}(1)$

The purpose of this section is to begin our proof of the main theorem by determining $\Lambda_{\mathcal{I}_1(G),G}(1)$. In particular, we will prove the following lemma.

Main Lemma 3.25 *Let V be a linear space or a nondegenerate unitary or orthogonal space over $\mathbf{F}_q$ with q odd and $d = dim(V)$ an odd prime. Let $G \in PC(V)$. If $G = \Omega(V)$ assume that $q > 3$. Let $\Lambda_{\mathcal{I}_1(G),G}$ be the Lefschetz character for the action of G on $\mathcal{I}_1^*(G)$ by conjugation.*

(1) If V is a linear space then $-\Lambda_{\mathcal{I}_1(G),G}(1) = \frac{|GL(V)|}{d(q^d-1)}$.

(2) If V is a unitary space then $-\Lambda_{\mathcal{I}_1(G),G}(1) = \frac{|GU(V)|}{d(\sqrt{q}^d+1)}$.

(3) If V is an orthogonal space then $-\Lambda_{\mathcal{I}_1(G),G}(1) = \frac{|GO(V)|}{2d}$.

The proof will be carried out as follows. Using Corollary 2.16 and Lemma 2.17, we see that $-\Lambda_{\mathcal{I}_1(G),G}(1)$ is equal to an alternating sum involving sets of subspaces of V whose simultaneous stabilizer in G is nontrivial. We then introduce a different collection of sets of subspaces of V such that the corresponding alternating sum can be calculated in a straightforward fashion. Finally, we show that the two alternating sums last mentioned are equal. This last step requires that d be prime.

Definition 3.26 *Let V be a linear space or a nondegenerate unitary or orthogonal space of finite dimension over $\mathbf{F}_q$. Let $G \in PC(V)$.*

(1) $\Phi(G) := \{X \subseteq \mathcal{C}_1(G) : \bigcap_{M \in X} M \neq 1\}$.

(2) $\Phi'(G)$ is the collection of all sets $E = \{V_1, \ldots, V_k\}$ of nontrivial proper subspaces of V such that $\{stab_G(V_i) : i \in [k]\} \in \Phi(G)$.

(3) $\mathcal{S}$ is the lattice of subspaces of V ordered by containment, and $\mathcal{S}^* = \mathcal{S} \setminus \{0, V\}$.

Note that $\Phi(G)$ is simply the collection of sets of subspace stabilizers whose intersection is nontrivial. We will apply some of our preliminary results to express $\Lambda_{\mathcal{I}_1(G),G}(1)$ involving the elements of $\Phi'(G)$.

Lemma 3.27 *Let V be a linear space or a nondegenerate unitary or orthogonal space of finite dimension d over $\mathbf{F}_q$. Let $G \in PC(V)$. Then*

$$-\Lambda_{\mathcal{I}_1(G),G}(1) = \sum_{E \in \Phi'(G)} (-1)^{|E|}.$$

Proof: By Lemma 2.6 and Corollary 2.16,

$$-\Lambda_{\mathcal{I}_1(G),G}(1) = \sum_{E \in \Phi(G)} (-1)^{|E|}.$$

By Lemma 2.17,

$$\sum_{E \in \Phi(G)} (-1)^{|E|} = \sum_{E \in \Phi'(G)} (-1)^{|E|},$$

and we are done. □

3.2.1 A useful subsum

Now we introduce the alternative set of collections of subspaces of V promised earlier.

Definition 3.28 *Let V be a finite dimensional linear space or a finite dimensional nondegenerate unitary or orthogonal space. Let $E = \{V_1, \ldots, V_k\}$ be a collection of nontrivial proper subspaces of V.*

(1) We say that E is nonspanning if $\sum_{i=1}^{k} V_i \neq V$.

(2) $N(V)$ is the set of nonspanning collections of nontrivial proper subspaces of V.

(3) We say that E is decomposing if $\sum_{i=1}^{k} V_i = V$ and one of the two following conditions holds:

(a) V is a linear space and there exists a decomposition $V = \oplus_{j=1}^{r} W_j$ such that each V_i is contained in some W_j.

(b) V is an orthogonal or unitary space and there exists a decomposition $V = \perp_{j=1}^{r} W_j$ with each V_i contained in some W_j. Note that in this case each W_j is nondegenerate.

(4) $D(V)$ is the set of decomposing collections of nontrivial proper subspaces of V.

(5) $\Gamma(V) = N(V) \cup D(V)$.

Lemma 3.29 *Let V be a linear space or a nondegenerate unitary or orthogonal space over $\mathbf{F}_q$. If $dim(V) = n$ then*

$$\sum_{E \in N(V)} (-1)^{|E|} = -\mu_{\mathcal{S}}(0, V) = (-1)^{n-1} q^{\binom{n}{2}}.$$

Proof: The first equality follows immediately from the application of Lemma 2.6 to the dual of the lattice $\mathcal{S}$ and the collection of nontrivial proper subspaces of V. The second equality is well known and appears on page 127 of [45]. $\Box$

Lemma 3.30 *Let $V, E = \{V_1, \ldots, V_k\}$ be as in Definition 3.28. If $E \in D(V)$ then there exists a unique finest decomposition $V = \oplus_{j=1}^{r} W_j$ or $V = \perp_{j=1}^{r} W_j$ such that each V_i is contained in some W_j.*

Proof: Let $V = \oplus_{l=1}^{s} X_l$ and $V = \oplus_{m=1}^{t} Y_m$ be two decompositions such that each V_i is contained in some X_l and in some Y_m. Let $I = \{(l, m) : X_l \cap Y_m \neq 0\}$. Since $\sum_{i=1}^{k} V_i = V$ and each V_i is contained in $X_l \cap Y_m$ for some $(l, m) \in I$, we have $V = \oplus_{(l,m) \in I} X_l \cap Y_m$. Furthermore, if the original decompositions are orthogonal with respect to a nondegenerate hermitian or symmetric from, so is the resulting decomposition. The lemma follows immediately. $\Box$

Definition 3.31 *Let $V, E = \{V_1, \ldots, V_k\} \in D(V)$ be as in Definition 3.28.*

(1) If V is a linear space then $\mathcal{D}(V)$ is the collection of decompositions $V = \oplus_{j=1}^r W_j$. If V is a unitary or orthogonal space then $\mathcal{D}(V)$ is the collection of decompositions $V = \perp_{j=1}^r W_j$. $\mathcal{D}(V)'$ is the set of proper decompositions of V, that is, $\mathcal{D}(V)' = \mathcal{D}(V) \setminus \{V = V\}$.

(2) $\delta(E) \in \mathcal{D}(V)$ is the unique finest decomposition $V = \oplus_{j=1}^r W_j$ or $V = \perp_{j=1}^r W_j$ such that each V_i is contained in some W_j.

Lemma 3.32 *Let $\delta : V = \oplus_{j=1}^r W_j$ or $\delta : V = \perp_{j=1}^r W_j$ be any proper decomposition of V, so $r > 1$. Then*

$$\sum_{\delta(E)=\delta} (-1)^{|E|} = (-1)^r \prod_{j=1}^r \sum_{F \in \Gamma(W_j)} (-1)^{|F|}.$$

Proof: Fix $E = \{V_1, \ldots, V_k\} \in D(V)$ with $\delta(E) = \delta$. For each $j \in [r]$ set $E_j = \{V_i : V_i \leq W_j\}$. Then $E_j \notin \Gamma(W_j)$, since otherwise there is a finer decomposition of V such that each V_i is contained in some summand. Conversely, if for each $j \in [r]$ we choose a collection F_j of nontrivial proper subspaces of W_j such that $F_j \notin \Gamma(W_j)$ then $F = \cup_{j=1}^r F_j$ satisfies $\delta(F) = \delta$. Note that the F_j can be chosen independently. The lemma now follows from the fact that the sum $\sum(-1)^{|F|}$ taken over all collections of nontrivial proper subspaces of W_j is zero. $\square$

Definition 3.33 *(1) $P(n)$ is the set of partitions of n, and $P'(n) = P(n) \setminus \{n\}$.*

(2) For $n \in \mathbf{N}$, q an odd prime power and $\alpha \in \mathcal{J}_n$, $S(n, q, \alpha)$ is the set of pairs (i, γ) such that $i \in [n]$ and $\gamma \in \mathcal{J}_i$ (see Definition 3.7).

(3) For n, q, α as in (2), $P(n, q, \alpha)$ is the set of "typed partitions"

$$(n, \alpha) = \textstyle\sum_{(i,\gamma) \in S(n,q,\alpha)} \lambda_{i,\gamma}(i, \gamma),$$

and $P'(n,q,\alpha) = P(n,q,\alpha) \setminus \{(n,\alpha)\}$. *A typed partition is simply a formal linear combination* λ *with nonnegative integer coefficients* $\lambda_{i,\gamma}$ *such that* $n = \sum \lambda_{i,\gamma} i$ *and* $\alpha = \sum \lambda_{i,\gamma}\gamma$ *in the abelian group* $\mathcal{J}(q)$.

Definition 3.34 *Let* $\delta : V = \oplus_{j=1}^{r} W_j$ *or* $\delta : V = \perp_{j=1}^{r} W_j$ *be an element of* $\mathcal{D}(V)$, *with* $dim(V) = n$. *If* V *is a linear or unitary space then for* $i \in [n]$, *set* $\delta_i = |\{j : dim(W_j) = i\}|$. *If* V *is an orthogonal space then for* $i \in [n]$ *and* $\gamma \in \mathcal{J}_i$ *define* $\delta_{i,\gamma}$ *to be the number of* W_j *of dimension* i *and decomposition type* γ. *We define* $\lambda(\delta)$ *as follows.*

(1) If V *is a linear or unitary space,* $\lambda(\delta)$ *is the partition* $n = \sum_{i=1}^{n} \delta_i i \in P(n)$.

(2) If V *is an orthogonal space of decomposition type* α, $\lambda(\delta)$ *is the typed partition* $(n,\alpha) = \sum_{(i,\gamma)\in S(n,\alpha)} \delta_{i,\gamma}(i,\gamma)$.

Proposition 3.35 *Let* V *be a finite dimensional linear space or a finite dimensional nondegenerate unitary or orthogonal space over* $\mathbf{F}_q$. *Let* $G(V)$ *act on* $\mathcal{D}(V)$ *in the manner induced by the natural action of* $G(V)$ *on* V. *Then* $\delta, \tau \in \mathcal{D}(V)$ *are in the same orbit under this action if and only if* $\lambda(\delta) = \lambda(\tau)$. *Moreover, if* δ *and* τ *are in the same orbit then* $\sum_{\delta(E)=\delta}(-1)^{|E|} = \sum_{\delta(E)=\tau}(-1)^{|E|}$.

Proof: The first claim is obvious in the linear case and follows from Witt's Theorem in the other cases. The second claim is obvious. □

We are going to calculate $\sum_{E\in\Gamma(V)}(-1)^{|E|}$ by induction on $dim(V)$. The last proposition allows us to group decompositions in the same orbit when making this calculation.

Lemma 3.36 *Let* V *be a linear space or nondegenerate unitary or orthogonal space of dimension* n *over* $\mathbf{F}_q$, *with* q *odd. Set* $\phi(V) = \sum_{E\in\Gamma(V)}(-1)^{|E|}$.

(1) If V *is a linear space then* $\phi(V) = \frac{|GL_n(q)|}{n(q^n-1)}$.

(2) If V is a unitary space then $\phi(V) = (-1)^{n-1}\frac{|GU_n(\sqrt{q})|}{n(\sqrt{q}^n-(-1)^n)}$.

(3a) If V is an orthogonal space with n odd then $\phi(V) = (-1)^{n-1}\frac{|GO_n(q)|}{2n}$.

(3b) If V is an orthogonal space with n even, let U be an orthogonal space of dimension n over $\mathbf{F}_q$ of different decomposition type than that of V. Then $\phi(V) = (-1)^{n-1}\frac{|GO(U)|}{2n}$.

Proof: If $n = 1$ then $\Gamma(V) = \{\emptyset\}$, and the lemma follows immediately in this case from calculation of the orders of $GL(V), GU(V)$ and $GO(V)$. We now proceed by induction on n, assuming $n > 1$.

We handle the linear and unitary cases first. For $j \in [n]$, set $G(j,q) = GL_j(q)$ in the linear case and $G(j,q) = GU_j(\sqrt{q})$ in the unitary case. Fix $\lambda : n = \sum_{j=1}^n \lambda_j j \in P'(n)$. If $\delta \in \mathcal{D}(V)$ with $\lambda(\delta) = \lambda$ then the stabilizer of δ in $G(n,q)$ is the direct product of wreath products $\prod_{j=1}^{n-1} S_{\lambda_j}[G(j,q)]$. For $\lambda : n = \sum_{j=1}^n \lambda_j j \in P(n)$ set $r(\lambda) = \sum_{j=1}^n \lambda_j$. Set $\varepsilon = 1$ and $u = q$ in the linear case and $\varepsilon = -1$ and $u = \sqrt{q}$ in the unitary case. Using Lemmas 3.29 and 3.32 and Proposition 3.35, it now follows from the inductive hypothesis that

$$\phi(V) = (-1)^{n-1}q^{\binom{n}{2}} + \sum_{\lambda\in P'(n)} \frac{(-1)^{r(\lambda)}|G(n,q)|}{\prod_{j=1}^{n-1}\lambda_j!|G(j,q)|^{\lambda_j}} \prod_{j=1}^{n-1} \varepsilon^{\lambda_j(j-1)} \frac{|G(j,q)|^{\lambda_j}}{(j(u^j-\varepsilon^j))^{\lambda_j}}.$$

Now note that in the linear case,

$$q^{\binom{n}{2}} = \frac{|G(n,q)|}{\prod_{j=1}^n(q^j-1)},$$

while in the unitary case,

$$q^{\binom{n}{2}} = \frac{|G(n,q)|\sqrt{q}^{\binom{n}{2}}}{\prod_{j=1}^n(\sqrt{q}^j-(-1)^j)}.$$

We now divide both sides of the given identity for $\phi(V)$ by $|G(n,q)|$. In the linear case, we see that the claim of the lemma is equivalent to the identity

$$\frac{1}{n(q^n-1)} = \frac{(-1)^{n-1}}{\prod_{i=1}^n(q^i-1)} + \sum_{\lambda\in P'(n)} (-1)^{r(\lambda)} \prod_{j=1}^{n-1} \frac{1}{\lambda_j! j^{\lambda_j}(q^j-1)^{\lambda_j}},$$

which can be rewritten as

$$\frac{1}{\prod_{i=1}^{n}(1-q^i)} = \sum_{\lambda\in P(n)}\prod_{j=1}^{n}\frac{1}{\lambda_j! j^{\lambda_j}(1-q^j)^{\lambda_j}}$$

In the unitary case, the claim of the lemma is equivalent to the identity

$$\frac{(-1)^{n-1}}{n(\sqrt{q}^n-(-1)^n)} = \frac{(-1)^{n-1}\sqrt{q}^{\binom{n}{2}}}{\prod_{i=1}^{n}(\sqrt{q}^i-(-1)^i)} + \sum_{\lambda\in P'(n)}\prod_{j=1}^{n-1}\frac{(-1)^n}{\lambda_j! j^{\lambda_j}(\sqrt{q}^j-(-1)^j)^{\lambda_j}}.$$

For $\lambda : n = \sum_{j=1}^{n}\lambda_j j \in P(n)$ let $e(\lambda) = \sum_{j \text{ even}}\lambda_j$. Then the above identity can be rewritten as

$$\frac{(-\sqrt{q})^{\binom{n}{2}}}{\prod_{i=1}^{n}(1-(-\sqrt{q})^i)} = \sum_{\lambda\in P(n)}(-1)^{e(\lambda)}\prod_{j=1}^{n}\frac{1}{\lambda_j! j^{\lambda_j}(1-(-\sqrt{q})^j)^{\lambda_j}}.$$

For $\sigma \in S_n$ with σ_i i-cycles in its decomposition into disjoint cycles, define $\lambda(\sigma) = \sum_{i=1}^{n}\sigma_i i \in P(n)$. The centralizer of σ in S_n is a direct product of wreath products $S_{\sigma_i}[S_i]$, and therefore has order $\prod_{i=1}^{n}\sigma_i! i!^{\sigma_i}$. Note that if $\lambda(\sigma)=\lambda$ then $sgn(\sigma)=e(\lambda)$. Set $t=q$ in the linear case and $t=-\sqrt{q}$ in the unitary case. The lemma is now equivalent to

$$\frac{1}{\prod_{i=1}^{n}(1-t^i)} = \frac{1}{|S_n|}\sum_{\sigma\in S_n}\prod_{j=1}^{n}\frac{1}{(1-t^j)^{\sigma_j}}$$

in the linear case, and

$$\frac{t^{\binom{n}{2}}}{\prod_{j=1}^{n}(1-t^j)} = \frac{1}{|S_n|}\sum_{\sigma\in S_n} sgn(\sigma)\prod_{j=1}^{n}\frac{1}{(1-t^j)^{\sigma_j}}$$

in the unitary case. Both of these identities hold in the power series ring $\mathbf{C}[[t]]$. Indeed, they are both examples of Polya's enumeration theorem. In the linear case, the left side of our identity is the generating function for partitions into n or $n-1$ parts, while in the unitary case, it is the generating function for partitions into n or $n-1$ distinct parts.

The proof in the orthogonal case uses the same strategy as those in the linear and unitary cases, but the details are more complicated. Define $\beta : \mathcal{J}\to\mathcal{J}$ by

$$+\mapsto -, -\mapsto +, \diamond\mapsto\diamond, \triangle\mapsto\triangle,$$

and for $\lambda : (n,\alpha) = \sum_{i,\gamma}\lambda_{i,\gamma}(i,\gamma)\in P(n,q,\alpha)$, set $r(\lambda)=\sum_{i,\gamma}\lambda_{i,\gamma}$. As in the previous cases, we can deduce from the inductive hypothesis that if V is of dimension n over $\mathbf{F}_q$

and has decomposition type α then

$$\phi(V) = (-1)^{n-1} q^{\binom{n}{2}} + (-1)^n \sum_{\lambda \in P'(n,q,\alpha)} \frac{|GO_n^\alpha(q)|}{\prod_{i,\gamma} \lambda_{i,\gamma}! |GO_i^\gamma(q)|^{\lambda_{i,\gamma}}} \prod_{i,\gamma} \left(\frac{|GO_i^{\beta(\gamma)}(q)|}{2i} \right)^{\lambda_{i,\gamma}}.$$

For any $n \in \mathbf{N}$, let $[n]_e$ be the set of even elements of $[n]$, and for any even $i \in \mathbf{N}$ define

$$f(i,q) = \frac{q^{i/2} - 1}{q^{i/2} + 1}.$$

Then

$$\frac{|GO_i^{\beta(\gamma)}(q)|}{|GO_i^\gamma(q)|} = \begin{cases} \frac{q^{i/2}+1}{q^{i/2}-1} & \gamma = + \\ \frac{q^{i/2}-1}{q^{i/2}+1} & \gamma = - \\ 1 & \gamma \in \{\diamond, \triangle\} \end{cases}$$

and it follows that

$$\phi(V) = (-1)^{n-1} q^{\binom{n}{2}} + (-1)^n |GO_n^\alpha(q)| \sum_{\lambda \in P'(n,q,\alpha)} \frac{1}{\prod_{i,\gamma} \lambda_{i,\gamma}! (2i)^{\lambda_{i,\gamma}}} \prod_{i \in [n]_e} f(i,q)^{\lambda_{i,+} - \lambda_{i,-}}.$$

If $n = 2k$ and $\alpha = +$ then $\binom{n}{2} = k^2 + k(k-1)$ and

$$q^{\binom{n}{2}} = \frac{q^{k^2} |GO_n^\alpha(q)|}{(q^k - 1) 2 \prod_{j=1}^{k-1} (q^{2j} - 1)} = |GO_n^\alpha(q)| \frac{q^{k^2}(q^k+1)}{2 \prod_{i \in [n]_e} (q^i - 1)}.$$

Similarly, if $n = 2k$ and $\alpha = -$ then

$$q^{\binom{n}{2}} = |GO_n^\alpha(q)| \frac{q^{k^2}(q^k - 1)}{2 \prod_{i \in [n]_e} (q^i - 1)},$$

and if $n = 2k+1$ then

$$q^{\binom{n}{2}} = |GO_n^\alpha(q)| \frac{q^{k(k+1)}}{2 \prod_{i \in [n]_e} (q^i - 1)}$$

independent of α. Now set

$$\rho(n,\alpha,q) = \begin{cases} q^{k^2}(q^k+1) & n = 2k, \alpha = + \\ q^{k^2}(q^k - 1) & n = 2k, \alpha = - \\ q^{k(k+1)} & n = 2k+1 \end{cases}$$

The lemma is equivalent to the following statement:

$$\frac{\rho(n,\alpha,q)}{2 \prod_{i \in [n]_e} (q^i - 1)} = \sum_{\lambda \in P(n,q,\alpha)} \frac{1}{\prod_{i,\gamma} \lambda_{i,\gamma}! (2i)^{\lambda_{i,\gamma}}} \prod_{i \in [n]_e} f(i,q)^{\lambda_{i,+} - \lambda_{i,-}}.$$

This equality follows immediately from the two claims below, which will be stated after defining the appropriate terms.

For $n \in \mathbf{N}$, set $P^*(n) = \bigcup_{\alpha \in \mathcal{J}_n} P(n, q, \alpha)$. Also, define $\varepsilon : \mathcal{J} \to \{1, -1\}$ by $+, \diamondsuit \mapsto 1$ and $-, \triangle \mapsto -1$. Set

$$\Upsilon(n, q) = \sum_{\lambda \in P^*(n)} \frac{1}{\prod_{i,\gamma} \lambda_{i,\gamma}!(2i)^{\lambda_{i,\gamma}}} \prod_{i \in [n]_e} f(i, q)^{\lambda_{i,+} - \lambda_{i,-}},$$

and

$$\Upsilon'(n, q) = \sum_{\lambda \in P^*(n)} \frac{\varepsilon(\alpha)}{\prod_{i,\gamma} \lambda_{i,\gamma}!(2i)^{\lambda_{i,\gamma}}} \prod_{i \in [n]_e} f(i, q)^{\lambda_{i,+} - \lambda_{i,-}}.$$

Claim 1 : If n is even then

$$\Upsilon(n, q) = \frac{\rho(n, +, q) + \rho(n, -, q)}{2 \prod_{i \in [n]_e} (q^i - 1)} = \frac{q^{k(k+1)}}{\prod_{i \in [n]_e} (q^i - 1)},$$

and if n is odd then

$$\Upsilon(n, q) = \frac{\rho(n, \diamondsuit, q) + \rho(n, \triangle, q)}{2 \prod_{i \in [n]_e} (q^i - 1)} = \frac{q^{k(k+1)}}{\prod_{i \in [n]_e} (q^i - 1)}.$$

Claim 2 : If n is even then

$$\Upsilon'(n, q) = \frac{\rho(n, +, q) - \rho(n, -, q)}{2 \prod_{i \in [n]_e} (q^i - 1)} = \frac{q^{k^2}}{\prod_{i \in [n]_e} (q^i - 1)},$$

and if n is odd then

$$\Upsilon'(n, q) = \frac{\rho(n, \diamondsuit, q) - \rho(n, \triangle, q)}{2 \prod_{i \in [n]_e} (q^i - 1)} = 0.$$

Note that the lemma follows from the claims through calculation of $\Upsilon(n, q) + \Upsilon'(n, q)$ and $\Upsilon(n, q) - \Upsilon'(n, q)$. Also note that the second equality of each claim follows immediately from the definition of ρ, so each claim will be proved by showing that the first term is equal to the third.

Proof of Claim 1: Let K be the wreath product $S_n[Z_2]$. We write an element of K as (σ, v), where $\sigma \in S_n$ and $v = (v_1, \ldots, v_n) \in Z_2^n$. Define a map $type : K \to P^*(n)$ as follows. Given $k = (\sigma, v) \in K$, write $\sigma = \tau_1 \ldots \tau_r$ as a product of disjoint cycles. For each $j \in [r]$, set $s(j) = supp(\tau_j)$. If $i \in [n]$ is even, define

$$k_{i,+} = |\{j \in [r] : |s(j)| = i \text{ and } \sum_{l \in s(j)} v_l \equiv 0\}|$$

and

$$k_{i,-} = |\{j \in [r] : |s(j)| = i \text{ and } \sum_{l \in s(j)} v_l \equiv 1\}|.$$

Similarly, if $i \in [n]$ is odd, define

$$k_{i,\triangle} = |\{j \in [r] : |s(j)| = i \text{ and } \sum_{l \in s(j)} v_l \equiv 0\}|$$

and

$$k_{i,\diamond} = |\{j \in [r] : |s(j)| = i \text{ and } \sum_{l \in s(j)} v_l \equiv 1\}|.$$

Now set

$$type(k) = \sum_{i,\gamma} k_{i,\gamma}(i,\gamma) \in P^*(n).$$

It is well known that $k_1, k_2 \in K$ are conjugate if and only if $type(k_1) = type(k_2)$ (see [8], p. 25). Moreover, it is straightforward to count the elements in each conjugacy class of K and see that

$$\Upsilon(n,q) = \frac{1}{|K|} \sum_{k \in K} \prod_{i \in [n]_e} f(i,q)^{k_{i,+} - k_{i,-}}.$$

For each $k = (\sigma, v) \in K$, set

$$Q(\sigma, v) = \prod_{i \in [n]_e} (\frac{1 - q^{i/2}}{1 + q^{i/2}})^{k_{i,+} - k_{i,-}}.$$

Let $M = \{(\sigma, v) \in K : \sigma \in A_n\}$. For $k = (\sigma, v) \in K$,

$$sgn(\sigma) = (-1)^{\sum_{i \in [n]_e} k_{i,+} + k_{i,-}}.$$

Thus

$$\begin{aligned} \Upsilon(n,q) &= \frac{1}{|K|} \sum_{(\sigma,v) \in K} sgn(\sigma) Q(\sigma, v) \\ &= \frac{1}{|M|} \sum_{(\sigma,v) \in M} Q(\sigma, v) - \frac{1}{|K|} \sum_{(\sigma,v) \in K} Q(\sigma, v). \end{aligned}$$

Fix $\sigma \in S_n$ and write $\sigma = \tau_1 \ldots \tau_r$ as a product of disjoint cycles. It is easy to see that

$$\sum_{v \in Z_2^n} Q(\sigma, v) = \prod_{j=1}^{r} \sum_{w \in Z_2^{supp(\tau_j)}} Q(\tau_j, w),$$

where $Q(\tau_j, w)$ is computed in the appropriate wreath product. Moreover, it is straightforward to calculate that if τ_j is an odd cycle of length i then

$$\sum_{w \in \mathbf{Z}_2^{supp(\tau_j)}} Q(\tau_j, w) = 2^i,$$

while if τ_j is an even cycle of length i then

$$\sum_{w \in \mathbf{Z}_2^{supp(\tau_j)}} Q(\tau_j, w) = 2^{i-1}\left(\frac{1+q^{i/2}}{1-q^{i/2}} + \frac{1-q^{i/2}}{1+q^{i/2}}\right) = 2^i \frac{1+q^i}{1-q^i}.$$

Let σ_i be the number of i-cycles in the decomposition of $\sigma \in S_n$ into disjoint cycles. We have shown that

$$\Upsilon(n, q) = \frac{1}{|A_n|} \sum_{\sigma \in A_n} \prod_{i \in [n]_e} \left(\frac{1+q^i}{1-q^i}\right)^{\sigma_i} - \frac{1}{|S_n|} \sum_{\sigma \in S_n} \prod_{i \in [n]_e} \left(\frac{1+q^i}{1-q^i}\right)^{\sigma_i}.$$

We will apply Polya's enumeration theorem (see [39]). Let $\Upsilon_n(t)$ be the power series obtained by replacing q by the indeterminate t in the right side of the above equation. Let $k = \lfloor \frac{n}{2} \rfloor$. Claim 1 will follow if we show that in $\mathbf{C}[[t]]$ we have

$$\Upsilon_n(t) = (-1)^k \frac{t^{k(k+1)}}{\prod_{i \in [n]_e} (1 - t^i)}.$$

Let R_n be the set of functions from $[n]$ to $\mathbf{N}_0$ and define $w : \mathbf{N}_0 \to \mathbf{C}[[t]]$ by $w(r) = (-1)^r t^{\lfloor \frac{r+1}{2} \rfloor}$, so

$$w(0) = 1, w(1) = -t, w(2) = t, w(3) = -t^2, w(4) = t^2, \ldots$$

If j is odd, then $\sum_{r \in \mathbf{N}_0} w(r)^j = 1$, and if j is even then

$$\sum_{r \in \mathbf{N}_0} w(r)^j = 1 + 2t^j + 2t^{2j} + \ldots = \frac{1+t^j}{1-t^j}.$$

Therefore,

$$\Upsilon_n(t) = \mathcal{P}_{A_n}(\sum_{r \in \mathbf{N}_0} w(r), \ldots, \sum_{r \in \mathbf{N}_0} w(r)^n) - \mathcal{P}_{S_n}(\sum_{r \in \mathbf{N}_0} w(r), \ldots, \sum_{r \in \mathbf{N}_0} w(r)^n)$$

and by Polya's theorem,

$$\Upsilon_n(t) = \sum_{f \in R_n / A_n} \prod_{i \in [n]} w(f(i)) - \sum_{f \in R_n / S_n} \prod_{i \in [n]} w(f(i)).$$

Let π_n be the set of all partitions of integers into n or $n-1$ distinct parts. For $\lambda \in \pi_n$, write $\lambda = (r_1, \ldots, r_s)$, where $s = n$ or $n-1$ and $r_i > r_{i+1}$ for all $i \in [s-1]$. Now $(R_n/A_n) \setminus (R_n/S_n)$ can be put in bijective correspondence with π_n so that

$$\Upsilon_n(t) = \sum_{\lambda \in \pi_n} \prod_{i \in [s]} w(r_i) = \sum_{m \in \mathbf{N}_0} c_m t^m,$$

where the c_m are to be determined.

For $\lambda = (r_1, \ldots, r_s) \in \pi_n$, let λ^* be the partition $\sum \mu_j j$ (returning to our previous notation for partitions), where $\mu_j = |\{i \in [s] : |w(r_i)| = t^j\}|$. For example, if $\lambda = (5,3,2,1)$ then $\lambda^* = (2 \times 1) + 2 + 3$. Also, set $s(\lambda) = (-1)^{\sum_{i \in [s]} r_i}$. For each partition μ, let $c_\mu = \sum_{\lambda^* = \mu} s(\lambda)$. Then we have

$$c_m = \sum_{\mu \in P(m)} c_\mu.$$

Fix $\mu \in P(m)$. If $\mu_j > 2$ for some $j \in [m]$ then there are no $\lambda \in \pi_n$ such that $\lambda^* = \mu$, so $c_\mu = 0$. If $\mu_j = 1$ for some j, then for each $\lambda = (r_1, \ldots, r_s) \in \pi_n$ such that $w(r_i) = t^j$ and $\lambda^* = \mu$, let ν be the partition obtained by replacing r_i with r_{i-1}. Then $\nu^* = \mu$ and $s(\lambda) + s(\nu) = 0$. It follows that $c_\mu = 0$. Therefore, we now assume that $\mu_j \in \{0, 2\}$ for all $j \in [m]$. If $\lambda \in \pi_n$ with $\lambda^* = \mu$, then there exist $r_1, \ldots, r_k$ such that $\lambda = (2r_1, 2r_1 - 1, 2r_2, 2r_2 - 1, \ldots, 2r_k, 2r_k - 1)$. Therefore, $s(\lambda) = (-1)^k$ and the $j \in [m]$ such that $\mu_j = 2$ are $r_1, \ldots, r_k$. It follows that $(-1)^k c_m$ is the number of partitions of $\frac{m}{2}$ into k distinct parts. Let $P_k(t)$ be the generating function for partitions into k distinct parts. It is well known (see for example [1]) and easy to show that

$$P_k(t) = \frac{t^{\binom{k+1}{2}}}{\prod_{j=1}^k (1 - t^j)}.$$

We now have

$$\Upsilon_n(t) = (-1)^k P_k(t^2) = (-1)^k \frac{t^{\binom{2k}{2}}}{\prod_{i=1}^k (1 - t^{2i})} = (-1)^k \frac{t^{k(k+1)}}{\prod_{i \in [n]_e} (1 - t^i)},$$

and the proof of Claim 1 is complete.

Proof of Claim 2: For $\nu \in P^*(n)$, define

$$c(\nu) = \frac{1}{\prod_{i,\gamma} \nu_{i,\gamma}! (2i)^{\nu_{i,\gamma}}},$$

and for $\nu \in P(n,q,\alpha)$ set

$$r(\nu) = \varepsilon(\alpha)c(\nu) \prod_{i\in[n]_e} f(i,q)^{\nu_{i,+}-\nu_{i,-}}.$$

For $\lambda \in P(n)$ define

$$T_\lambda = \left\{\nu \in \cup_{\alpha\in\mathcal{J}_n} P(n,q,\alpha) : \lambda_j = \textstyle\sum_{\gamma\in J_j} \nu_{j,\gamma} \text{ for all } j \in [n]\right\},$$

and set $R(\lambda) = \sum_{\nu\in T_\lambda} r(\nu)$. Then

$$\Upsilon'(n,q) = \sum_{\lambda\in P(n)} R(\lambda).$$

Our first step is to show that if $\lambda_i \neq 0$ for some odd $i \in [n]$ then $R(\lambda) = 0$. Assume that such an odd i exists. It is certainly sufficient to show that if we define a collection of elements $T \subseteq T_\lambda$ by fixing $\nu_{j,\gamma}$ for all $j \neq i$ and $\gamma \in \mathcal{J}_j$ and then letting $(\lambda_{i,\triangle}, \lambda_{i,\diamond})$ run over all pairs $(k, \lambda_i - k)$ then $\sum_{\nu\in T} r(\nu) = 0$. With this goal in mind, we define

$$\delta(k) = \begin{cases} 1 & \text{if } k\triangle + (\lambda_i - k)\diamond \in \{+,\triangle\} \\ -1 & \text{if } k\triangle + (\lambda_i - k)\diamond \in \{-,\diamond\} \end{cases}$$

for all $k \in [\lambda_i]$. It is easy to see that in order to show that $\sum_{\nu\in T} r(\nu) = 0$, it is sufficient to show that

$$\sum_{k=0}^{\lambda_i} \delta(k)\binom{\lambda_i}{k} = 0.$$

Now note that $k\triangle + (\lambda_i - k)\diamond = \lambda_i\diamond + k(-)$. Thus $\delta(k)$ alternates in sign as k increases by one, and the last sum given above is zero.

If n is odd, then for every $\lambda \in P(n)$ there exists some odd $i \in [n]$ with $\lambda_i \neq 0$. Thus $R(\lambda) = 0$ for all λ, and $\Upsilon'(n,q) = 0$ as claimed.

Now assume that n is even, and for $\alpha \in \{+,-\}$ define

$$P_e(n,q,\alpha) := \{\lambda \in P(n,q,\alpha) : \lambda_{i,\gamma} = 0 \text{ if } i \text{ is odd}\}.$$

It follows from the above result that

$$\Upsilon'(n,q) = \sum_{\alpha\in\{+,-\}} \sum_{\lambda\in P_e(n,q,\alpha)} \varepsilon(\alpha)c(\lambda) \prod_{i\in[n]_e} f(i,q)^{\lambda_{i,+}-\lambda_{i,-}}.$$

Note that if $\lambda \in P_e(n,q,\alpha)$ then

$$\varepsilon(\alpha) = (-1)^{\sum_{i\in[n]_e}\lambda_{i,-}}.$$

It follows that if we define K, M and $Q(\sigma,v)$ as in the proof of Claim 1 and set

$$K_e = \{(\sigma,v)\in K : \sigma \text{ has no odd cycles}\},$$

we get

$$\Upsilon'(n,q) = \frac{1}{|K|}\sum_{(\sigma,v)\in K_e}(-1)^{\sum v_j} sgn(\sigma)Q(\sigma,v).$$

As in the proof of Claim 1, we fix $\sigma = \tau_1\ldots\tau_r \in S_n$ with each τ_j a cycle of even length. For each i-cycle τ_j we calculate

$$\sum_{w\in \mathbf{Z}_2^{supp(\tau_j)}}(-1)^{\sum w_l}Q(\tau_j,w) = 2^{i-1}\left(\frac{1+q^{i/2}}{1-q^{i/2}} - \frac{1-q^{i/2}}{1+q^{i/2}}\right) = \frac{2^{i+1}q^{i/2}}{1-q^i}.$$

Set $S_n^e = \{\sigma\in S_n : \sigma \text{ has no odd cycles}\}$ and $A_n^e = A_n \cap S_n^e$. We have shown that

$$\Upsilon'(n,q) = \frac{1}{|A_n|}\sum_{\sigma\in A_n^e}\prod_i\left(\frac{2q^{i/2}}{1-q^i}\right)^{\sigma_i} - \frac{1}{|S_n|}\sum_{\sigma\in S_n^e}\prod_i\left(\frac{2q^{i/2}}{1-q^i}\right)^{\sigma_i},$$

where σ_i is the number of i-cycles in σ. Let $\Upsilon_n'(t^{1/2})$ be the power series in $t^{1/2}$ obtained by replacing q with t in the right side of the above equation. Set $k = \frac{n}{2}$. We will finish the proof of Claim 2 by showing that the identity

$$\Upsilon_n'(t^{1/2}) = (-1)^k\frac{t^{k^2}}{\prod_{i\in[n]_e}(1-t^i)}$$

holds in $\mathbf{C}[[t^{1/2}]]$.

Let Q_n be the set of functions from $[n]$ to $\mathbf{N}$, and define $w:\mathbf{N}\to\mathbf{C}\left[\left[t^{1/2}\right]\right]$ by

$$w(r) = \begin{cases} -t^{r/2} & r \text{ odd} \\ t^{\frac{r-1}{2}} & r \text{ even}\end{cases}$$

so for example $w(1) = -t^{1/2}$, $w(2) = t^{1/2}$, and $w(3) = -t^{3/2}$. If j is odd then $\sum_{r\in\mathbf{N}} w(r)^j = 0$, while if j is even then

$$\sum_{r\in\mathbf{N}} w(r)^j = \sum_{m\, odd} 2t^{mj/2} = \frac{2t^{j/2}}{1-t^j}.$$

Therefore,

$$\Upsilon_n'(t^{1/2}) = \mathcal{P}_{A_n}(\sum_{r\in\mathbf{N}} w(r),\ldots,\sum_{r\in\mathbf{N}} w(r)^n) - \mathcal{P}_{S_n}(\sum_{r\in\mathbf{N}} w(r),\ldots,\sum_{r\in\mathbf{N}} w(r)^n)$$

and by Polya's theorem,

$$\Upsilon_n'(t^{1/2}) = \sum_{f\in Q_n/A_n}\prod_{i\in[n]} w(f(i)) - \sum_{f\in Q_n/S_n}\prod_{i\in[n]} w(f(i)).$$

Let π_n' be the set of all partitions of integers into n distinct parts. As above, an element of π_n' will be written as $\lambda = (r_1,\ldots,r_n)$ with $r_i > r_{i+1}$. Then π_n' can be put into bijective correspondence with $(Q_n/A_n)\setminus(Q_n/S_n)$ so that

$$\Upsilon_n'(t^{1/2}) = \sum_{\lambda\in\pi_n'}\prod_{i=1}^{n} w(r_i) = \sum_{m\in\mathbf{N}} d_m t^m,$$

where the d_m are to be determined.

For $\lambda = (r_1,\ldots,r_s)\in\pi_n'$, let λ^+ be the partition $\sum \mu_j j$, where

$$\mu_j = |\left\{i\in[n] : |w(r_i)| = t^{j/2}\right\}|.$$

For example, if $\lambda = (5,3,2,1)$ then $\lambda^+ = (2\times 1)+3+5$. As before, set $s(\lambda) = (-1)^{\sum r_i}$. For each partition μ, let $d_\mu = \sum_{\lambda^+=\mu} s(\lambda)$. Then

$$d_m = \sum_{\mu\in P(2m)} d_\mu.$$

Note that if $d_\mu \neq 0$ then every element of $supp(\mu)$ is odd and $\sum\mu_j = n$. If $\mu_j > 2$ for some j, then there are no $\lambda\in\pi_n'$ with $\lambda^+ = \mu$, so $d_\mu = 0$. If $\mu_j = 1$ for some j, then for each $\lambda = (r_1,\ldots,r_n)\in\pi_n'$ with $\lambda^+ = \mu$ and $w(r_i) = t^{j/2}$ let ν be the partition obtained by replacing r_i with $r_i - 1$. Then $\nu^+ = \mu$ and $s(\lambda)+s(\nu) = 0$. It follows that $d_\mu = 0$. Now assume that $\mu_j\in\{0,2\}$ for all j. If $\lambda\in\pi_n'$ with $\lambda^+ = \mu$ then $\lambda = (j_1+1, j_1, j_2+1, j_2,\ldots,j_k+1,j_k)$, where $supp(\mu) = \{j_1,\ldots,j_k\}$. This gives $d_\mu = s(\lambda) = (-1)^k$, so $(-1)^k d_m$ is the number of partitions of m into k distinct odd parts. By associating each Young diagram with its conjugate, we see that this is equal to the number of partitions of m into parts of size at most k such that each size occurs at least once, k occurs an odd number of times, and each $l < k$ occurs an even number of times. This is in turn equal to the number of partitions of $m - \binom{k+1}{2} - \binom{k}{2} = m - k^2$ into parts of size at most k such that each part occurs an even number of times, which is equal to the number of partitions of $m - k^2$ into even parts of size at most n. The generating function that counts such partitions is

$$(-1)^k \frac{t^{k^2}}{\prod_{i \in [n]_e}(1-t^i)} = \Upsilon'_n(t^{1/2}).$$

The proof of Claim 2 is now complete, as is the proof of the lemma. □

3.2.2 Reduction to the subsum in prime dimension

Our goal is now to show that when $dim(V)$ is an odd prime we have $\Lambda_{\mathcal{I}_1(G),G}(1) = \sum_{E \in \Gamma(V)} (-1)^{|E|}$. We will show that when $dim(V)$ is prime we have $\sum_{E \in \Phi'(G)} (-1)^{|E|} = \sum_{E \in \Gamma(V)} (-1)^{|E|}$. We begin by determining the relationships between $\Gamma(V)$ and $\Phi'(G)$. We would like to show that $\Gamma(V) \subseteq \Phi'(G)$ and then show that $\sum_{E \in \Phi' \setminus \Gamma} (-1)^{|E|} = 0$. This method is essentially correct, although the first statement is false when V is an orthogonal space. We begin by stating an obvious proposition, which we will use many times without explicit reference.

Proposition 3.37 *Let V be a nondegenerate orthogonal or unitary space with form f, and let $V = \perp_{i=1}^k V_i$ be any decomposition. If $g \in GL(V)$ satisfies $g_{|V_i} \in G(V_i, f_{|V_i})$ for each i, then $g \in G(V, f)$.*

Lemma 3.38 *Let V be a linear space or a nondegenerate unitary or orthogonal space of odd dimension d over $\mathbf{F}_q$. Let $G \in PC(V)$, and assume $G \neq \Omega(V)$. Let $E = \{V_1, \ldots, V_k\} \in \Gamma(V)$. If one of the following cases holds, then $E \in \Phi'(G)$.*

(1) $E \in D(V)$.

(2) V is a linear space and $E \in N(V)$.

(3) V is a unitary or orthogonal space and there exists some nondegenerate $W < V$ such that $\sum_{i=1}^k V_i \leq W$.

Proof: In the given cases, there exist $W, X < V$ such that $V = W \oplus X$ or $V = W \perp X$ and each V_i is contained in W or X. Since d is odd, we may assume that $dim(W)$ is even and $dim(X)$ is odd. Define $g \in GL(V)$ by $g_{|W} = -1$ and $g_{|X} = 1$. Then g fixes each V_i and since $det(g) = 1$, $\overline{g} \in G$. □

Corollary 3.39 *Let V be a linear space of odd dimension over $\mathbf{F}_q$ and let $G \in PC_L(V)$. Then $\Gamma(V) \subseteq \Phi'(G)$.*

Lemma 3.40 *Let V be a unitary space of odd dimension over $\mathbf{F}_q$ and let $W < V$ be degenerate of codimension one. Let $G \in PC_U(V)$. If $E = \{V_1, \ldots, V_k\} \in N(V)$ with $\sum_{i=1}^{k} V_i \leq W$ then $E \in \Phi'(G)$.*

Proof: Let X be a complement to $rad(W)$ in W, so X is nondegenerate of codimension two in V. There is some unipotent $u \in GU(X^{\perp})$ such that $rad(W)$ is an eigenspace for u. Define $g \in SU(V)$ by $g_{|X} = 1$ and $g_{|X^{\perp}} = u$. Then $g_{|W} = 1$ and $\overline{g} \in G$. □

Corollary 3.41 *Let V be a unitary space of odd dimension over $\mathbf{F}_q$ and let $G \in PC_U(V)$. Then $\Gamma(V) \subseteq \Phi'(G)$.*

Proof: This follows immediately from Lemma 3.38(1) and (3) and Lemma 3.40. □

The orthogonal case is not quite as nice as the other cases, but is still tractable. We begin by recalling a criterion which determines whether an element of a special orthogonal group $SO(W)$ lies in $\Omega(W)$.

Lemma 3.42 *Let W be a nondegenerate orthogonal space of dimension at least two over a field $\mathbf{F}_q$ of odd order. For $w \in W$ such that $(w, w) \neq 0$ define $r_w \in GO(W)$ by $x \mapsto x - 2\frac{(w,x)}{(w,w)}w$. Each $g \in SO(W)$ can be written as a product $g = r_{w_1} \ldots r_{w_k}$ with k even. The homomorphism $\Theta : SO(W) \to \mathbf{F}_q^*/(\mathbf{F}_q^*)^2$ given by $\prod_{i=1}^{k} r_{w_i} \mapsto \prod_{i=1}^{k}(w_i, w_i)$ is well defined, and $ker(\Theta) = \Omega(W)$.*

Proof: This is well known. See [28], pages 29 and 30. □

Θ is called the spinor norm.

Lemma 3.43 *Let V be a nondegenerate orthogonal space over $\mathbf{F}_q$ with q odd and let $G \in PC_O(V)$. Let $W < V$ be degenerate with $codim(W) = 2$. If $E = \{V_1, \ldots, V_k\} \in N(V)$ with $\sum_{i=1}^{k} V_i \leq W$ then $E \in \Phi'(G)$.*

Proof: Let X be a complement to $R = rad(W)$ in W. If $dim(R) = 1$, then $dim(X^\perp) = 3$. In this case, $SO(X^\perp)$ acts transitively on the $q+1$ singular 1-spaces in $X^\perp$. Since $|SO(X^\perp)| = q(q^2-1)$, there exists some unipotent $u \in SO(X^\perp)$ such that R is an eigenspace for U. Note that $|u|$ is odd. By Lemma 3.42, $\left\{SO(X^\perp) : \Omega(X^\perp)\right\} = 2$, so $u \in \Omega(X^\perp)$. Now define $g \in SO(W)$ by $g_{|X} = 1$ and $g_{|X^\perp} = u$. Since $g_{|W} = 1$, $\overline{g} \in G$ fixes all the V_i. If $dim(R) = 2$, then $dim(X^\perp) = 4$. Since $X^\perp$ contains a totally singular subspace of dimension two, $\alpha(X^\perp) = +$. Let w_1, x_1, w_2, x_2 be a hyperbolic basis for $X^\perp$ such that w_1, w_2 is a basis for R. Define $h \in GL(X^\perp)$ by $w_1 h = w_1, x_1 h = x_1 + w_2, w_2 h = w_2, x_2 h = x_2 - w_1$. It is straightforward to show that $h \in SO(X^\perp)$, and since $|h|$ is the characteristic of $\mathbf{F}_q$, we have $h \in \Omega(X^\perp)$. Now define $g \in \Omega(V)$ by $g_{|X} = 1$ and $g_{|X^\perp} = h$. Then $\overline{g} \in G$ fixes all the V_i. □

Lemma 3.44 *Let V be a nondegenerate orthogonal space of odd dimension over $\mathbf{F}_q$ with q odd and let $G = \Omega(V)$. Let $W < V$ be nondegenerate with $codim(W) = 2$. If $E = \{V_1, \ldots, V_k\} \in N(V)$ with $\sum_{i=1}^{k} V_i \leq W$ then $E \in \Phi'(G)$.*

Proof: Note that $W^\perp$ is nondegenerate of dimension two. Let X_1, X_2 be 1-dimensional subspaces of $W^\perp$ such that $W^\perp = X_1 \perp X_2$. There are four elements $g \in GO(V)$ which act like 1 or -1 on X_1 and X_2 and satisfy $g_{|W} = -1$. One of these elements must lie in $\Omega(V)$. □

Lemma 3.45 *Let V be a nondegenerate orthogonal space of odd dimension over $\mathbf{F}_q$ with q odd and let $G = \Omega(V)$. Let W_1, W_2, W_3 be nondegenerate proper subspaces of V such that $V = W_1 \perp W_2 \perp W_3$. If $E = \{V_1, \ldots, V_k\} \in D(V)$ with each V_i contained in some W_j then $E \in \Phi'(G)$.*

Proof: Let H be the subgroup of $GO(V)$ containing all elements h such that $h_{|W_j} = 1$ or -1 for all $j \in [3]$. Then $|H| = 8$, so $H \cap \Omega(V) \neq 1$. Certainly any $1 \neq h \in H \cap \Omega(V)$ fixes all the V_i □

Corollary 3.46 *Let V be a nondegenerate orthogonal space of odd dimension over $\mathbf{F}_q$ with q odd and let $G \in PC_O(V)$. Let $E = \{V_1, \ldots, V_k\} \in \Gamma(V)$. If $E \notin \Phi'(G)$ then one of the following cases holds.*

(1) $E \in N(V)$ and $W = \sum_{i=1}^{k} V_i$ is degenerate of codimension one.

(2) $G = \Omega(V)$, $E \in N(V)$ and $W = \sum_{i=1}^{k} V_i$ is nondegenerate of codimension one.

(3) $G = \Omega(V)$, $E \in D(V)$ and for $0 < W < V$ such that each V_i is contained in W or $X = W^{\perp}$, there does not exist any orthogonal decomposition $W = W_1 \perp W_2$ or $X = X_1 \perp X_2$ such that each $V_i < W$ is contained in W_1 or W_2 or each $V_i < X$ is contained in either X_1 or X_2.

Proof: If $G = SO(V)$ then by Lemmas 3.38 and 3.43, (1) must hold. If $G = \Omega(V)$ then by Lemmas 3.43, 3.44 and 3.45, either (1),(2) or (3) holds or $E \in D(V)$ and there exists a decomposition $W = W_1 \perp W_2$ as in (3) such that each $V_i < W$ is contained in W_1 or W_2, but $W \in E$. In this case, we may define $1 \neq g \in \Omega(V)$ such that g acts as 1 or -1 on each of W_1, W_2 and X as in the proof of Lemma 3.45. In this case, $\overline{g}$ fixes W, so $E \in \Phi'(G)$. □

The following lemma is not necessary for our purposes, but completes the work begun with Lemmas 3.38 and 3.43.

Lemma 3.47 *Let V be a nondegenerate orthogonal space of odd dimension over $\mathbf{F}_q$ and let $W < V$ be degenerate of codimension one. Then there is no $1 \neq g \in SO(V)$ which stabilizes all subspaces of W.*

Proof: If such a g exists then $g_{|W} = 1$ or -1. Let X be a complement to $rad(W)$ in W, so X is nondegenerate of codimension two in V. Let w, x be a hyperbolic basis for $X^{\perp}$ with $w \in rad(W)$. Since $wg = \alpha w$ with $\alpha \in \{1, -1\}$, and $g_{|X^{\perp}} \in SO(X^{\perp})$, we must have $xg = \alpha x$. This gives $g = \alpha 1$, and since $dim(V)$ is odd, $\alpha = 1$. □

We will now calculate $\sum_{E\in\Gamma\setminus\Phi'}(-1)^{|E|}$ in the orthogonal case. We fix a nondegenerate orthogonal space V of odd dimension over $\mathbf{F}_q$ with q odd, and write Γ for $\Gamma(V)$.

Definition 3.48 *Let $W < V$ and let $G \in PC_O(V)$.*

(1) If codim$(W) = 1$,

$$\Gamma_W(G) := \left\{E = \{V_1, \dots, V_k\} \in \Gamma \setminus \Phi'(G) : \sum_{i=1}^{k} V_i = W\right\}.$$

(2) If W is nondegenerate,

$$\Gamma'_W(G) := \left\{E = \{V_i\} \in D(V) \setminus \Phi'(G) : V_i \le W \text{ or } W^\perp \text{ for all } V_i \in E\right\}.$$

Proposition 3.49 *Let $W, X < V$ be nondegenerate. If $\Gamma'_W(G) \cap \Gamma'_X(G) \neq \emptyset$ then $X \in \left\{W, W^\perp\right\}$.*

Proof: This follows immediately from Lemmas 3.30 and 3.45. $\square$

Lemma 3.50 *Let $W < V$ be degenerate of codimension one and let $G \in PC_O(V)$. If $q = 3$ assume $G = SO(V)$. Fix $E = \{V_1, \dots, V_k\} \in \Gamma_W(G)$. Let $R = rad(W)$. Then both $E \cup \{R\}$ and $E \setminus \{R\}$ are in $\Gamma_W(G)$.*

Proof: It is clear that $E \cup \{R\} \in \Gamma_W$, so we examine $E \setminus \{R\}$. If $R \notin E$ there is nothing to prove, so we assume that $V_k = R$. Assume for contradiction that $E \setminus V_k \notin \Gamma_W(G)$. If $X = \sum_{i=1}^{k-1} V_i < W$ then X is a complement to R in W. Let w, x be a hyperbolic basis for $X^\perp$ such that $w \in R$. If $q > 3$ then there is a square $\alpha \in \mathbf{F}_q^*$ with $\alpha \neq 1$. For $\gamma \in \mathbf{F}_q$ define $a_\gamma \in SO(X^\perp)$ by $wa_\gamma = \gamma w$ and $xa_\gamma = \gamma^{-1}x$. Let $\beta \in \mathbf{F}_q$ satisfy $\beta^2 = \alpha$. Then $a_\alpha = a_\beta^2$, so $a_\alpha \in \Omega(X^\perp)$. Define $g \in \Omega(V)$ by $g_{|X} = 1$ and $g_{|X^\perp} = a_\alpha$. Then $\overline{g} \in G$ fixes all the E_i, contradicting $E \notin \Phi'(G)$. If $q = 3$ then $G = SO(V)$ and we can define $g \in G$ by $g_{|X} = 1$ and $G_{|X^\perp} = -1$ so that g fixes all the V_i, again contradicting $E \notin \Phi'(G)$. If $\sum_{i=1}^{k-1} V_i = W$ then any element of G which fixes all V_i for $i \in [k-1]$ also fixes W, so g fixes R. This also contradicts $E \notin \Phi'(G)$. $\square$

Corollary 3.51 *Let $W < V$ be degenerate of codimension one and let $G \in PC_O(V)$. Then $\sum_{E\in\Gamma_W(G)}(-1)^{|E|} = 0$.*

Proof: Set $\Gamma_W^+(G) = \{E \in \Gamma_W(G) : rad(W) \in E\}$ and $\Gamma_W^-(G) = \Gamma_W(G) \setminus \Gamma_W^+(G)$. By Lemma 3.50, the map $\rho : \Gamma_W^+(G) \to \Gamma_W^-(G)$ defined by $E \mapsto E \setminus \{rad(W)\}$ is a bijection such that $(-1)^{|E|} + (-1)^{|\rho(E)|} = 0$. □

Lemma 3.52 *Let $W < V$ be nondegenerate of codimension one and let $G = \Omega(V)$. Then $\sum_{E \in \Gamma_W(G)} (-1)^{|E|} + \sum_{E \in \Gamma'_W(G)} (-1)^{|E|} = 0$.*

Proof: Let $E = \{V_1, \ldots, V_k\} \in \Gamma_W(G)$. Then $E \cup \left\{W^\perp\right\} \in D(V)$, so $E \cup \left\{W^\perp\right\} \in \Gamma'_W(G)$. Now let $F = \{X_1, \ldots, X_l\} \in \Gamma'_W(G)$. We may assume that $X_l = W^\perp$. Since $\sum_{i=1}^{l} X_i = V$, we have $\sum_{i=1}^{l-1} X_i = W$. If there is some $1 \neq g \in G$ which fixes X_i for all $i \in [l-1]$, then g fixes W and $W^\perp$, contradicting $F \in \Gamma'_W(G)$. Therefore, $F \setminus W^\perp \in \Gamma_W$. The bijection $\rho : \Gamma_W \to \Gamma'_W(G)$ given by $E \mapsto E \cup \left\{W^\perp\right\}$ satisfies $(-1)^{|E|} + (-1)^{|\rho(E)|} = 0$, and the lemma follows. □

Lemma 3.53 *Let $W < V$ be nondegenerate with $1 < dim(W) < d-1$. Assume $q > 3$ and let $G = \Omega(V)$. Then $\sum_{E \in \Gamma'_W(G)} (-1)^{|E|} = 0$.*

Proof: We may assume $dim(W)$ is odd. Let $E = \{V_1, \ldots, V_k\} \in \Gamma'_W(G)$. We may assume that there is some $l < k$ such that $W = \sum_{i=1}^{l} V_i$ and $W^\perp = \sum_{i=l+1}^{k} V_i$. Exactly one of the following conditions holds.

(a) $W \notin E$.

(b) $W \in E$ and $E \setminus \{W\} \in \Gamma'_W(G)$.

(c) $W \in E$ and $E \setminus \{W\} \notin \Gamma'_W(G)$.

The map $\rho : E \mapsto E \cup \{W\}$ determines a bijection between set of elements of $\Gamma'_W(G)$ satisfying condition (a) and the set of elements satisfying condition (b) such that $(-1)^{|E|} + (-1)^{|\rho(E)|} = 0$. We must account for those elements of $\Gamma'_W(G)$ satisfying condition (c). Let $E = \{V_1, \ldots, V_k\}$ be such an element. We may assume $W = V_l$. Let $X = \sum_{i=1}^{l-1} V_i$. If $X = W$ then $E \setminus \{W\} \in D(V)$, so $E \setminus \{W\} \in \Phi'(G)$. Now any $g \in G$

which fixes all the elements of $E \setminus \{W\}$ also fixes W, contradicting $E \notin \Phi'(G)$. If X is of codimension at least two in W then by Lemmas 3.43 and 3.44 there exists some $1 \neq h \in \Omega(W)$ which fixes V_i for all $i \in [l-1]$. Define $g \in G$ by $g_{|W} = h$ and $g_{|W^\perp} = 1$. Then g fixes all elements of E, again contradicting $E \notin \Phi'(G)$. If X is nondegenerate, then by Corollary 3.46 $E \notin \Gamma \setminus \Phi'(G)$. We have shown that if E satisfies condition (c) then X is degenerate of codimension 1 in W.

Now let X be any degenerate subspace of codimension one in W. Let $\Gamma'_W(G, X)$ be the set of all $E \in \Gamma'_W(G)$ such that E satisfies condition (c) and the sum of all elements of E which are proper subspaces of W is X. We will show that $\sum_{E \in \Gamma'_W(G,X)} (-1)^{|E|} = 0$, thereby completing this proof. Let $Y = W \cap X^\perp$. We first show that if $Y \in E$ then $E \setminus \{Y\} \in \Gamma'_W(G)$. Assume for contradiction that some $g \in G$ fixes all elements of $E \setminus \{Y\}$. We may assume that $V_{l-1} = Y$. Set $Z = \sum_{i=1}^{l-2} V_i$. If $Z = X$ then g fixes X and W, so g also fixes Y, a contradiction. Otherwise, Z is a complement to Y in X, so Z is nondegenerate. By Corollary 3.46, we have a contradiction to $E \in \Gamma \setminus \Phi'(G)$. Thus $E \setminus \{Y\} \in \Gamma'_W(G)$ as claimed. Now note that $E \setminus \{Y\}$ is actually in $\Gamma'_W(G, X)$. Indeed, if Z as defined above is a proper subspace of X, then every element of $E \setminus \{W\}$ is contained in one of Z, $Z^\perp \cap W$ or $W^\perp$, and we can apply Corollary 3.46 once more to get a contradiction. As above, we can use the bijection $E \mapsto E \cup \{Y\}$ to show that $\sum_{E \in \Gamma'_W(G,X)} (-1)^{|E|} = 0$. □

Corollary 3.54 *Let V be a nondegenerate orthogonal space of odd dimension over $\mathbf{F}_q$ with q odd. Let $G \in PC_O(V)$. Then*

$$\sum_{E \in \Gamma(V) \setminus \Phi'(G)} (-1)^{|E|} = 0.$$

Proof: This follows from Corollaries 3.46 and 3.51 and Lemmas 3.52 and 3.53. □

Our final task in this section is to show that if $dim(V)$ is prime and $G \in PC(V)$ then $\sum_{E \in \Phi'(G) \setminus \Gamma(V)} (-1)^{|E|} = 0$. Note that we have only required so far that $dim(V)$ be odd.

Definition 3.55 *Let V be a linear space or nondegenerate unitary or orthogonal space over $\mathbf{F}_q$. Let $G \in PC(V)$ and let $E \in \Phi'(G) \setminus \Gamma(V)$. A_E is the set of elements of E which are maximal in E with respect to the inclusion order on the lattice $\mathcal{S}$ of subspaces of V.*

Proposition 3.56 *Let V, G be as in Definition 3.55. Let $E \in \Phi'(G) \setminus \Gamma(V)$. Then A_E is an antichain in $\mathcal{S}^* = \mathcal{S} \setminus \{0, V\}$ and $A_E \in \Phi'(G) \setminus \Gamma(V)$.*

Proof: It is clear from its definition that A_E is an antichain. Any $g \in G$ which fixes all elements of E certainly fixes all elements of A_E, so $A_E \in \Phi'(G)$. If $A_E \in \Gamma(V)$ then either $A_E \in N(V)$, in which case $E \in N(V)$, or $A_E \in D(V)$, in which case $E \in D(V)$. In either case, $E \in \Gamma(V)$. □

Definition 3.57 *Let V, G be as in Definition 3.55. $\mathcal{A}$ is the set of antichains from $\mathcal{S}^*$ which lie in $\Phi'(G) \setminus \Gamma(V)$.*

Proposition 3.58 *Let V, G be as in Definition 3.55. Then*

$$\textstyle\sum_{E \in \Phi'(G) \setminus \Gamma(V)} (-1)^{|E|} = \sum_{A \in \mathcal{A}} \sum_{A_E = A} (-1)^{|E|}.$$

Proof: This is immediate from the definition of $\mathcal{A}$. □

Proposition 3.59 *Let V, G be as above. Let $A = \{X_1, \ldots, X_k\} \in \mathcal{A}$ and fix $E \in \Phi'(G) \setminus \Gamma(V)$ with $A_E = A$. Assume that there exist some $i \in [k]$ and $J \subseteq [k]$ such that $0 < X := X_i \cap \sum_{j \in J} X_j < X_i$. Then $E^+ := E \cup \{X\}$ and $E^- := E \setminus \{X\}$ are in $\Phi'(G) \setminus \Gamma(V)$, and $A_{E^+} = A_{E^-} = A$.*

Proof: It's clear that $A_{E^-} = A$, and since $X < X_i$, $A_{E^+} = A$. It follows immediately that E^+ and E^- are not in $\Gamma(V)$. Now since $E^- \subseteq E$, we certainly have $E^- \in \Phi'(G)$. Finally, any $1 \neq g \in G$ which fixes all elements of E also fixes X, so $E^+ \in \Phi'(G)$. □

Note that one of E^+, E^- is E and $(-1)^{|E^+|} + (-1)^{|E^-|} = 0$.

Corollary 3.60 *Let V, G be as above. Fix $A = \{X_1, \ldots, X_k\} \in \mathcal{A}$. If there exist some $i \in [k]$ and $J \subseteq [k]$ such that $0 < X := X_i \cap \sum_{j \in J} X_j < X_i$, then $\sum_{A_E = A} (-1)^{|E|} = 0$.*

Proof: By Proposition 3.59, the map $E \mapsto E^-$ gives a bijection

$$\rho : \{E : A_E = A, E = E^+\} \to \{E : A_E = A, E = E^-\}.$$

The corollary now follows immediately from the comment after the proposition. □

Proposition 3.61 *Let V be a nondegenerate unitary or orthogonal space over $\mathbf{F}_q$ with q odd. Let $G \in PC(V)$. Let $A = \{X_1, \ldots, X_k\} \in \mathcal{A}$ and fix $E \in \Phi'(G) \setminus \Gamma(V)$ with $A_E = A$. Assume that there exist some $i, j \in [k]$ such that $0 < Y := X_i \cap X_j^\perp < X_i$. Then $E^+ := E \cup \{Y\}$ and $E^- := E \setminus \{Y\}$ are in $\Phi'(G) \setminus \Gamma(V)$, and $A_{E^+} = A_{E^-} = A$.*

Proof: This is proved in exactly the same manner as Proposition 3.59, since any $1 \neq g \in G$ which fixes all elements of E certainly fixes $X_j^\perp$. □

Corollary 3.62 *Let V be a nondegenerate unitary or orthogonal space over $\mathbf{F}_q$ with q odd. Let $G \in PC(V)$. Fix $A = \{X_1, \ldots, X_k\} \in \mathcal{A}$. If there exist some $i, j \in [k]$ such that $0 < X := X_i \cap X_j^\perp < X_i$, then $\sum_{A_E = A} (-1)^{|E|} = 0$.*

Proof: We may repeat the proof of Corollary 3.60. □

We have shown that any $A \in \mathcal{A}$ which does not satisfy $\sum_{A_E = A} (-1)^{|E|} = 0$ satisfies the restrictive conditions that no i, j or J as given in Corollaries 3.60 and 3.62 can exist. We will now show that if $dim(V)$ is prime, there are no such A, by first showing that when d is prime, any such A is a collection of 1-spaces, and then deriving a contradiction to $A \in \mathcal{A}$.

Lemma 3.63 *Let V be a linear space of finite dimension n over $\mathbf{F}_q$. Let $A = \{X_1, \ldots, X_k\}$ be an antichain of nontrivial subspaces of V satisfying the following three conditions.*

(a) $\sum_{i=1}^k X_i = V$.

(b) There do not exist $W, X \leq V$ such that $V = W \oplus X$ and each X_i is contained in either W or X.

(c) For all $i \in [k]$ and $J \subseteq [k]$, $X_i \cap \sum_{j \in J} X_j = 0$ or X_i.

Then all the X_i have the same dimension.

Proof: If $n = 1$ the claim is trivially true, so we proceed by induction on n. Set $d_i = dim(X_i)$. We may assume that $k > 1$ and $d_1 \leq d_2 \leq \ldots \leq d_k$. We first show that $d_{k-1} = d_k$. By conditions (b) and (c), $X_k \leq \sum_{i=1}^{k-1} X_i$. By (c), we know that $X_k \cap X_1 = 0$ and that there must exist some $j \in [k-1]$ such that $X_k \leq \sum_{i=1}^{j} X_i$ and $X_k \cap \sum_{i=1}^{j-1} X_i = 0$. Now $X_j \not\leq \sum_{i=1}^{j-1} X_i$, so $X_j \cap \sum_{i=1}^{j-1} X_i = 0$. This gives

$$\begin{aligned} d_k + dim(\sum_{i=1}^{j-1} X_i) &= dim(X_k + \sum_{i=1}^{j-1} X_i) \leq dim(X_k + \sum_{i=1}^{j} X_i) \\ &= dim(\sum_{i=1}^{j} X_i) = d_j + dim(\sum_{i=1}^{j-1} X_i), \end{aligned}$$

so $d_k = d_j = d_{k-1}$.

Let $\overline{V} = V/X_k$, and for $W \leq V$ set $\overline{W} = (W + X_k)/X_k$. We will show that $\left\{\overline{X}_i : i \in [k-1]\right\}$ is an antichain of subspaces of $\overline{V}$ satisfying conditions (a)-(c). By inductive hypothesis, all the $\overline{X}_i$ have the same dimension. Now by (c), $dim(\overline{X}_i) = d_i$ and the proof will be complete.

Say $\overline{X}_i \cap \overline{X}_j \neq 0$ for some $i, j \in [k-1]$. This means that $x_i + X_k = x_j + X_k$ for some $x_i \in X_i$ and $x_j \in X_j$. Thus $x_i \in X_j + X_k$ and $x_j \in X_i + X_k$. Applying (c) to both of these inclusions gives $X_i + X_k = X_j + X_k$, so $\overline{X}_i = \overline{X}_j$. Therefore, the $\overline{X}_i$ form an antichain. Clearly this antichain satisfies condition (a). Say there exist $\overline{W}, \overline{X} \leq \overline{V}$ such that $\overline{V} = \overline{W} \oplus \overline{X}$ and each $\overline{X}_i$ is contained in $\overline{W}$ or $\overline{X}$. Let W, X be the respective preimages of $\overline{W}, \overline{X}$ in V. Let $I_W = \left\{i \in [k-1] : \overline{X}_i \leq \overline{W}\right\}$ and define

I_X similarly. Since the $\overline{X}_i$ satisfy (a), $\{X_i : i \in I_W\} \cup \{X_k\}$ is an antichain of subspaces of W satisfying (a) and (c), and a similar statement holds for the X_i contained in X. By the definition of $\overline{W}$ and $\overline{X}$, $W \cap X = X_k$. Say $\{X_i : i \in I_W\} \cup \{X_k\}$ does not satisfy (b), so there exist $Y, Z < W$ such that $W = Y \oplus Z$ and each of the X_i contained in W is contained in either Y or Z. We may assume that $X_k \leq Y$. But then $V = (X + Y) \oplus Z$ and each X_i is contained in either $X + Y$ or Z, contradicting the fact that our original antichain satisfies (b). Therefore, $\{X_i : i \in I_W\} \cup \{X_k\}$ must also satisfy (b) and all of these spaces have the same dimension by inductive hypothesis. A similar argument may be applied to X. This means that either $d_i = d_k$ for all $i \in [k]$, in which case there is nothing left to prove, or the $\overline{X}_i$ satisfy (b). Finally, say for some $i \in [k-1]$ and $J \subseteq [k-1]$ we have $\overline{X}_i \cap \sum_{j \in J} \overline{X}_j \neq 0$. Then we must also have $X_i \cap (X_k + \sum_{j \in J} X_j) \neq 0$, so by (c), $X_i \leq X_k + \sum_{j \in J} X_j$. Therefore, $\overline{X}_i \subseteq \sum_{j \in J} \overline{X}_j$, and the $\overline{X}_i$ satisfy (c). $\square$

Note that this lemma can be generalized. That is, if L is a finite modular lattice and $\{x_i\}$ is a collection of elements of L satisfying the general analogues of (a)-(c) above, then all of the x_i have the same rank.

Lemma 3.64 *Let V be a nondegenerate unitary or orthogonal space of finite dimension n over $\mathbf{F}_q$. Let $A = \{X_1, \ldots, X_k\}$ be an antichain of nontrivial subspaces of V satisfying the following three conditions.*

(a) $\sum_{i=1}^{k} X_i = V$.

(d) There do not exist $W, X \leq V$ such that $V = W \perp X$ and each X_i is contained in either W or X.

(e) For all $i, j \in [k]$, $X_i \cap X_j^{\perp} = 0$ or X_i.

Then all then X_i have the same dimension.

Proof: Let $d_i = dim(X_i)$. We may assume that $d_1 \leq d_2 \leq \ldots \leq d_k$. Assume for contradiction that $d_m < d_{m+1}$ for some $m \in [k]$. We may assume that we have chosen the smallest such m. Now if $1 \leq i \leq m$ and $m < j \leq k$ then $d_i < d_j$, so $dim(X_i^\perp) + dim(X_j) > n$. Thus $X_j \cap X_i^\perp \neq 0$, so by (e) we have $X_j \leq X_i^\perp$. Now by (a) we have $V = (\sum_{i=1}^m X_i) \perp (\sum_{i=m+1}^k X_i)$, contradicting (b). □

Corollary 3.65 *Let V be a linear space or a nondegenerate unitary or orthogonal space over $\mathbf{F}_q$. Let $G \in PC(V)$ and let $A = \{X_1, \ldots, X_k\}$ be an antichain from $\Phi'(G) \setminus \Gamma(V)$. If $d = dim(V)$ is an odd prime, then $\sum_{A_E = A} (-1)^{|E|} = 0$.*

Proof: Assume for contradiction that $\sum_{A_E = A} (-1)^{|E|} \neq 0$. Corollaries 3.60 and 3.62 show that if V is a linear space then A satisfies conditions (a),(b) and (c) of Lemma 3.63, and if V is a unitary or orthogonal space then A satisfies conditions (a),(d) and (e) of Lemma 3.64 along with condition (c) of Lemma 3.63. Let $J \leq [k]$ be minimal with respect to the condition that $\sum_{j \in J} X_j = V$. Then by condition (c), $V = \oplus_{j \in J} X_j$. Since $dim(V)$ is prime and all the X_i have the same dimension, we have $dim(X_i) = 1$ for all $i \in [k]$. Now since $A \in \Phi'(G)$ there exists some nonscalar $g \in G(V)$ such that each X_i is contained in an eigenspace for g. Therefore, g is diagonalizable, and V decomposes into the direct sum of the eigenspaces $V_\alpha = \{v \in V : vg = \alpha v\}$ for g which are nontrivial, as α ranges over $\mathbf{F}_q$. Each X_i is contained in some V_α. In the linear case, since g has more than one eigenvalue, condition (b) is violated, giving the desired contradiction. In the unitary or orthogonal case, let a be the automorphism of $\mathbf{F}_q$ which determines the form f, so $|a| = 2$ in the unitary case and $a = 1$ in the orthogonal case. Note that if $\alpha a(\gamma) \neq 1$ then $V_\alpha \leq V_\gamma^\perp$. Now fix α such that $V_\alpha \neq 0$ and set $\beta = a(\alpha)^{-1}$. By condition (d) we must have $V = V_\alpha + V_\beta$. If $V_\beta = 0$ or $\beta = \alpha$ we are done. Assume for contradiction that neither of these cases holds. Then by the definition of β, V_α and V_β must both be totally singular. However, since d is odd, one of these two subspaces has dimension greater than $\frac{d}{2}$. This contradicts the fact that V is nondegenerate. □

Corollary 3.66 *Let V be a linear space or a nondegenerate unitary or orthogonal space over $\mathbf{F}_q$. Let $G \in PC(V)$. If d is an odd prime then $\Lambda_{\mathcal{I}_1(G),G}(1) = \sum_{E \in \Gamma(V)} (-1)^{|E|}$.*

Proof: This follows from Lemma 3.27, Corollaries 3.39,3.41 and 3.54, Proposition 3.58 and Corollary 3.65. □

Now Lemma 3.36 and Corollary 3.66 prove Main Lemma 3.25.

3.3 $\Lambda_{\mathcal{I}_1(G),G}(g)$ for $g \neq 1$

In this section, we will determine $\Lambda_{\mathcal{I}_1(G),G}(g)$ for the nonidentity elements of $G \in PC(V)$. We continue with the notation of Section 3.1.5, with $d = dim(V)$ an odd prime. Recall that by Corollary 2.16 we have $\Lambda_{\mathcal{I}_1(G),G}(g) = \mu_{\mathcal{I}_1^g}(1, G)$, where $\mathcal{I}_1^g$ is the set of all $H \in \mathcal{I}_1(G)$ such that g normalizes H. Our first step is to replace $\mathcal{I}_1(G)$ with a sublattice that is easier to work with.

Definition 3.67 *Let $G \in PC(V)$.*

(1) $\dot{\mathcal{I}}_1(G) := \{H \in \mathcal{I}_1(G) : H = \cap_{M\in D} M$ for some $D \subseteq \mathcal{C}_1(G)\}$.

(2) For $H \in \mathcal{I}_1(G)$, $\mathcal{M}_H := \{M \in \mathcal{C}_1(G) : H \leq M\}$.

(3) For $H \in \mathcal{I}_1(G)$, $\mathcal{V}_H := \{W \leq V : M = stab_G(W)$ for some $M \in \mathcal{M}_H\}$.

We will sometimes drop the symbol G from $\mathcal{I}_1(G)$, $\dot{\mathcal{I}}_1(G)$ and $\mathcal{C}_1(G)$ in what follows.

Proposition 3.68 *Let $g \in G \in PC(V)$. Then $\Lambda_{\mathcal{I}_1(G),G}(g) = \mu_{\dot{\mathcal{I}}_1^g}(1, G)$.*

Proof: The map $H \mapsto \bigcap_{M\in\mathcal{M}_H} M$ is a G-equivariant closure on $\mathcal{I}_1$ whose image is $\dot{\mathcal{I}}_1$. By [40] (1.3), this map induces a G-equivariant homotopy of the associated order complexes, so the Lefschetz characters for the actions of G on $\mathcal{I}_1^*$ and $(\dot{\mathcal{I}}_1)^* = \dot{\mathcal{I}}_1 \setminus \{1, G\}$ are the same (see [51], Theorem 2.4). The proposition now follows from Corollary 2.16. $\square$

The next lemma is crucial, and is another step in which the proof of the main theorem of this section depends heavily on the fact that we are working in prime dimension.

Lemma 3.69 *Let $g \in G \in PC(V)$ and $1 < K \in \dot{\mathcal{I}}_1(G)^g$. Then one of the following holds:*

(a) There exists some $M \in \mathcal{M}_K$ such that $g \in M$.

(b) There exists a frame $X_1, X_2, \ldots, X_d$ of 1-spaces, each fixed by K, such that $V = \oplus_{i=1}^d X_i$ and g cyclically permutes the X_i (that is, $X_i g = X_{i+1}$ for $1 \le i \le d-1$ and $X_d g = X_1$). Furthermore, if V is a unitary or orthogonal space, then $V = \perp_{i=1}^d X_i$.

Proof: Assume that (a) does not hold, so that no $M \in \mathcal{M}_K$ contains g. Note that K is an intersection of subspace stabilizers and g acts on $\mathcal{V}_K$. It follows that g^* normalizes K^*. By definition, $K^*\langle g^* \rangle$ acts irreducibly on V. By Clifford's Theorem (see [25], p. 79), there exists a decomposition $V = \oplus_{i=1}^r X_i$, where each X_i is a homogeneous $\mathbf{F}_q[K^*]$-module and $\langle g^* \rangle$ permutes the X_i transitively. If $r > 1$ then since d is prime we have $dim(X_i) = 1$ for all $i \in [r]$. If $r = 1$ then since K^* is reducible but homogeneous, $V = X_1$ is the sum of isomorphic 1-dimensional K^*-modules, which contradicts $K \neq 1$.

Now assume that V is a unitary or orthogonal space, and let $1 \neq k \in K$. Fix $0 \neq x_i \in X_i$ for each $i \in [d]$. Then for each i there exists some $\alpha_i \in \mathbf{F}_q$ such that $x_i k^* = \alpha_i x_i$. Define $a \in Aut(\mathbf{F}_q)$ by $a(\alpha) = \alpha^{\sqrt{q}}$ in the unitary case and $a(\alpha) = \alpha$ in the orthogonal case. Assume for contradiction that $(x_i, x_j) \neq 0$ for some $i \neq j$. Then $\alpha_i a(\alpha_j) = 1$. By the transitivity of g on the X_i, $\alpha_{i+k} a(\alpha_{j+k}) = 1$ for all k, with addition mod d. Since d is an odd prime, we must have $\alpha_i = \alpha_j$ for all i, j, contradicting $k \neq 1$. Thus the X_i are mutually orthogonal and $V = \perp_{i=1}^d X_i$. □

Given the above result, we make the following definitions.

Definition 3.70 *Let $g \in G \in PC(n,q)$.*

(1) A g-frame with respect to G is a set of 1-spaces $F = \{X_1, \ldots, X_d\}$ with the following properties.

(a) $X_i g = X_{i+1}$ for $1 \le i < d$ and $X_d g = X_1$.

(b) $\bigcap_{i=1}^d stab_G(X_i) \neq 1$.

(c) $V = \oplus_{i=1}^d X_i$ in the linear case.

(d) $V = \perp_{i=1}^{d} X_i$ *in the orthogonal and unitary cases.*

(2) $\mathcal{F}(G,g)$ *is the set of* g*-frames with respect to* G.

(3) For $F = \{X_1, \ldots, X_d\} \in \mathcal{F}(G,g)$, $T_F := \bigcap_{i=1}^{d} stab_G(X_i)$.

(4) $\mathcal{C}_1(G,g) := \{M \in \mathcal{C}_1(G) : g \in M\}$.

Corollary 3.71 *Let* $g \in G \in PC(V)$ *and let* K *be a coatom in* $\dot{\mathcal{I}}_1^g$. *Then either* $K \in \mathcal{C}_1(G,g)$ *or* $K = T_F$ *for some* $F \in \mathcal{F}(G,g)$.

Proof: This follows immediately from Lemma 3.69. □

Note that we have not yet proved that each T_F is a coatom in $\dot{\mathcal{I}}_1^g$. The next two lemmas will show that T_F is both a coatom and an atom.

Lemma 3.72 *Let* $g \in G \in PC(V)$. *Let* $M \in \mathcal{C}_1(G,g)$ *and let* $F = \{X_1, \ldots, X_d\} \in \mathcal{F}(G,g)$. *Then* $T_F \cap M = 1$.

Proof: Let $K = T_F \cap M$. Fix $0 \neq x_i \in X_i$. Note that K^* is diagonal with respect to the basis $x_1, \ldots x_d$. Let $W < V$ with $M = stab_G(W)$. Note that both g^* and K^* fix W. Assume for contradiction that $K \neq 1$. For any function $a : K^* \to \mathbf{F}_q^*$, set $V_a = \{v \in V : vk^* = a(k^*)v \text{ for all } k^* \in K^*\}$. Then V is a direct sum of some of the nontrivial V_a. Also, since each V_a is a common eigenspace for all $k^* \in K^*$, each nonzero V_a is a sum of some of the X_i. Since g normalizes K and permutes the X_i transitively, g permutes the nonzero V_a transitively. Thus all the nonzero V_a have the same dimension, and since V is the direct sum of the nonzero V_a, that dimension is one or d. Thus if K^* contains a nonscalar matrix, the nonzero V_a are the X_i. Now since K fixes W, W is a sum of some of the X_i. However, g permutes the X_i transitively and fixes W, which forces $W = V$, giving the desired contradiction. □

Lemma 3.73 *Let* $g \in G \in PC(V)$. *If* $F = \{X_1, \ldots, X_d\}$, $F' = \{Y_1, \ldots, Y_d\}$ *are distinct elements of* $\mathcal{F}(G,g)$ *then* $T_F \cap T_{F'} = 1$.

Proof: Let $K = T_F \cap T_{F'}$. Fix $0 \neq x_i \in X_i$. Then K^* is diagonal with respect to the basis $x_1, \ldots, x_d$. As in the proof of Lemma 3.72, we have a decomposition of V into subspaces V_a, such that each nonzero V_a is a sum of some X_i. Again, all the V_a have the same dimension, and if K^* contains a nonscalar element then each nonzero V_a is some X_i. Now each Y_j is a common eigenspace for all $k^* \in K^*$, so each Y_j is contained in some V_a. However, if each V_a is some X_i, we then have $F = F'$. □

Corollary 3.74 *Let $g \in G \in PC(V)$ and let $F = \{X_1, \ldots, X_d\} \in \mathcal{F}(G, g)$. Then T_F is both an atom and a coatom in $\dot{\mathcal{I}}_1^g$.*

Proof: This follows from Lemmas 3.71, 3.72 and 3.73. □

Corollary 3.75 *Let $1 \neq g \in G \in PC(V)$. Then*

$$\Lambda_{\mathcal{I}_1(G),G}(g) = \mu_{\dot{\mathcal{I}}_1^g}(1, G) = \begin{cases} |\mathcal{F}(G,g)| & \mathcal{C}_1(G,g) \neq \emptyset \\ |\mathcal{F}(G,g)| - 1 & \mathcal{C}_1(G,g) = \emptyset \end{cases}$$

Proof: If $\mathcal{C}_1(G, g) = \emptyset$ then by Corollaries 3.71 and 3.74 we have $\dot{\mathcal{I}}_1^g = \{1, G\} \cup \{T_F : F \in \mathcal{F}(G, g)\}$ and it follows immediately that $\mu_{\dot{\mathcal{I}}_1^g}(1, G) = |\mathcal{F}(G, g)| - 1$. Now assume that $\mathcal{C}_1(G, g) \neq \emptyset$. Let $J = \cap_{M \in \mathcal{C}_1(G,g)} M$, so that $g \in J$, and set $\mathcal{W}_J = \left\{1 < T \in \dot{\mathcal{I}}_1^g : T \cap J = 1\right\}$. By Theorem 2.5,

$$\mu_{\dot{\mathcal{I}}_1^g}(1, G) = -\textstyle\sum_{T \in \mathcal{W}_J} \mu_{\dot{\mathcal{I}}_1^g}(T, G).$$

By Corollaries 3.71 and 3.74, $\mathcal{W}_J = \{T_F : F \in \mathcal{F}(G, g)\}$ and $\mu_{\dot{\mathcal{I}}_1^g}(T_F, G) = -1$ for all $T_F \in \mathcal{W}_J$. The proof is now complete. □

Thus to calculate $\Lambda_{\mathcal{I}_1(G),G}(g)$ for all nonidentity $g \in G \in PC(V)$, we need to determine which g satisfy $\mathcal{C}_1(G, g) \neq \emptyset$ and count $\mathcal{F}(G, g)$ for all nonidentity $g \in G$. In order to do this, we will have to consider various cases depending on d, q and G, as given below. We continue under the assumption that we have fixed a vector space V of odd prime dimension d over a field $\mathbf{F}_q$ of odd order.

Case (L1): $d \not| q-1$ and $G = L(V) = PGL(V)$.

Case (L2): $d|q-1$ and $G = PGL(V)$.

Case (L3): $d|q-1$ and $G = L(V)$.

Case (U1): $d \not| \sqrt{q}+1$ and $G = PSU(V) = PGU(V)$.

Case (U2): $d|\sqrt{q}+1$ and $G = PGU(V)$.

Case (U3): $d|\sqrt{q}+1$ and $G = PSU(V)$.

Case (O1): $G = PSO(V) = SO(V)$.

Case (O2): $G = P\Omega(V) = \Omega(V)$.

Recall that in the statement of the main theorems we fixed C to be the intersection of $G \in PC(V)$ with some fixed Coxeter torus of $PGL(V)$, so that in cases (O1) and (O2) we have $C = 1$. In cases (L1)-(L3) and (U1)-(U3), we further defined N to be the extension of C by F_d. In these cases, C^* contains the center of G^* and $C^*F_d^*$ is the normalizer of C^* in G^*, so CF_d is the normalizer of C in G.

We have essentially already solved the problem of determining $|\mathcal{C}_1(G,g)|$.

Lemma 3.76 *Let $g \in G \in PC(V)$. Then $\mathcal{C}_1(G,g) = \emptyset$ if and only if some G-conjugate of g is contained in C.*

Proof: Note that $\mathcal{C}_1(G,g) = \emptyset$ if and only if $\langle g^* \rangle$ is irreducible. It follows immediately from Lemma 3.16(2) that $\mathcal{C}_1(G,g) = \emptyset$ if and only if g is contained in a Coxeter torus of $PGL(V)$. It now follows from Lemma 3.16(5),(6) and Lemma 3.4 that in cases (U1)-(U3) that $\mathcal{C}_1(G,g) = \emptyset$ if and only if g is contained in a Coxeter torus of $PGU(V)$, and that all such Coxeter tori are conjugate. It only remains to show that in cases (L3) and (U3) the intersections of Coxeter tori of $PGL(V)$ and $PGU(V)$ with $L(V)$ and $PSU(V)$ form one conjugacy class in the smaller groups. This follows from the fact that in case (L3) we have $[PGL(V) : DF_d] = [L(V) : CF_d]$ and in case (U3) we have $[PGU(V) : DF_d] = [PSU(V) : CF_d]$. □

We now try to count $\mathcal{F}(G, g)$.

Lemma 3.77 *If q is a square and $d | \sqrt{q}+1$ then there exists a transversal $\mathcal{T}$ to $(\mathbf{F}_q^*)^d$ in $\mathbf{F}_q^*$ such that $t^{\sqrt{q}+1} = 1$ for all $t \in \mathcal{T}$.*

Proof: Assume that q is a square and let A be the unique subgroup of $\mathbf{F}_q^*$ having order $\sqrt{q}+1$. Since $d|\sqrt{q}+1$ and d is odd, $gcd(d, \sqrt{q}-1) = 1$ and $\left[A : A^d\right] = d$. We can now take $\mathcal{T}$ to be a transversal to A^d in A. □

Definition 3.78 *(1) $\mathcal{T}$ is a fixed transversal to $(\mathbf{F}_q^*)^d$ in $\mathbf{F}_q^*$ containing 1, so $\mathcal{T} = \{t_1 = 1\}$ in case (L1) and $\mathcal{T} = \{t_1 = 1, t_2, \ldots, t_d\}$ in cases (L2) and (L3). Moreover, if q is a square, then $\mathcal{T}$ is a transversal to A^d in A, where A is the unique subgroup of $\mathbf{F}_q^*$ of order $\sqrt{q}+1$.*

(2) For $g \in PGL(V)$, g^* is a fixed preimage of g in $GL(V)$ such that $det(g^*) \in \mathcal{T}$.

(3) Let $\{e_1, \ldots, e_d\}$ be a basis for V such that $F_d = F_d(B)$. Then for $t_i \in \mathcal{T}$, p_i is the element of $GL(V)$ such that $e_j p_i = e_{j+1}$ for $1 \le j \le d-1$ and $e_d p_i = t_i e_1$, and $g_i = \overline{p_i}$.

Lemma 3.77 allows us to assume that if q is a square then $g_i \in PGU(V)$ for all $t_i \in \mathcal{T}$. Note that $det(p_i) = t_i$, so $p_i = g_i^*$, and that except in cases (L2) and (U2), the only g_i which is contained in G is $g_1 = f_d$. Furthermore, the minimal polynomial of p_i is $t^d - t_i$.

Lemma 3.79 *(1) Let $g \in PGL(V)$. $\mathcal{F}(G, g) \neq \emptyset$ if and only if g^* is conjugate to some p_i in $GL(V)$.*

(2) Let $g \in PGL(V)$ with $|g| = d$ and $det(g^*) \neq 1$. Then g^* is conjugate in $GL(V)$ to some p_i with $i > 1$ if and only if some $PGL(V)$-conjugate of g is contained in the Coxeter torus C of $PGL(V)$.

Proof: (1) It is clear that each p_i permutes some frame. Now say $F = \{X_1, \ldots, X_d\} \in \mathcal{F}(G, g)$. For $1 \leq i \leq d$ we may choose some $0 \neq x_i \in X_i$ such that for $1 \leq i \leq d-1$, $x_i g^* = x_{i+1}$. Now $x_{i+1} g^* = \alpha x_1$ for some $\alpha \in \mathbf{F}_q$, and since $det(g^*) = \alpha$, $\alpha \in \mathcal{T}$.

(2) By Lemma 3.16, g is conjugate in $PGL(V)$ to an element of C if and only if g^* is irreducible. This condition holds if and only if and only if the minimal polynomial $f(t)$ of g is equal to the characteristic polynomial $c(t)$ of g, and $f(t)$ is irreducible. Since $f(t)|t^d - \alpha$ for some $\alpha \in \mathbf{F}_q$ and $c(t)$ has degree d, the two conditions of the previous sentence hold if and only if $f(t) = t^d - \alpha$ with $\alpha \in \mathbf{F}_q$ not a d^{th} power. Now by the definition of g^* and the fact that $det(g^*) \neq 1$, the condition of the previous sentence holds if and only if $\alpha = t_i$ for some $i > 1$. This last condition holds if and only if g^* is conjugate to some p_i with $i > 1$. □

Corollary 3.80 *Let $g \in G \in PC(V)$ with $\mathcal{F}(G, g) \neq \emptyset$. In cases (L1)-(L3) and (U1)-(U3), some G-conjugate of g is contained in N.*

Proof: In cases (L1) and (L2), the claim follows immediately from Lemma 3.79, and cases (U1) and (U2) it follows from Lemma 3.79 and Lemma 3.4. In case (L3), we must show that g is conjugate to f_d in $L(V)$. We know that g is conjugate to f_d in $PGL(V)$, and f_d centralizes an element y of order d in the Coxeter torus D of $PGL(V)$. By Lemma 3.79(2), $y \notin L(V)$. It follows that all $PGL(V)$-conjugates of f_d are already conjugate to f_d in $L(V)$. Case (U3) is handled similarly. □

Main Lemma 3.81 *Let $g \in G \in PC(V)$ and assume that one of the cases (L1)-(L3) or (U1)-(U3) holds. If no G-conjugate of g is contained in N, then $\Lambda_{\mathcal{I}_1(G),G}(g) = 0$.*

Proof: Since no conjugate of g is contained in C, $\mathcal{C}_1(G, g) \neq \emptyset$ by Lemma 3.76 and $\Lambda_{\mathcal{I}_1(G),G}(g) = |\mathcal{F}(G, g)|$ by Corollary 3.75. Now $\mathcal{F}(G, g) = \emptyset$ by Corollary 3.80. □

Lemma 3.82 *Let $g \in G = SO(V)$ or $\Omega(V)$ with $\mathcal{F}(G,g) \neq \emptyset$. Then g is conjugate to f_d^* in $SO(V)$.*

Proof: Recall that $F_d^* = F_d^*(B)$ for the basis $B = e_1, \ldots, e_n$. Let $F = \{X_1, \ldots, X_d\} \in \mathcal{F}(G,g)$, and choose $0 \neq x_i \in X_i$ such that $x_i g = x_{i+1}$ for $1 \leq i < d$. Since $det(g) = 1$, $x_d g = x_1$, so g is certainly conjugate to f_d^* in $GL(V)$. Now since $\langle g \rangle$ is transitive on the X_i, all of the X_i have the same isometry type. By Lemma 3.9, the isometry type of V uniquely determines the isometry type of X_1. In particular, X_1 is isometric to $\langle e_1 \rangle$, so the change of basis $x_i \mapsto e_i$ is an isometry and g is conjugate to f_d^* in $GO(V)$. Now the centralizer of g in $GO(V)$ contains -1, which is not contained in $SO(V)$, so every $GO(V)$-conjugate of f_d^* is already conjugate to f_d^* in $SO(V)$. □

Main Lemma 3.83 *If $g \in G = PSO(V)$ or $P\Omega(V)$ and $\Lambda_{\mathcal{I}_1(G),G}(g) \neq 0$ then some $PSO(V)$-conjugate of g is contained in F_d.*

Proof: This follows from Lemma 3.76, Corollary 3.75 and Lemma 3.82. □

Lemma 3.84 *Let $G \in PC(V)$ but assume that $G \neq \Omega(V)$. If $g_i \in G$ then $C_G(g_i)$ acts transitively on $\mathcal{F}(G, g_i)$.*

Proof: Let $g = g_i$ and fix $F = \{X_1, \ldots, X_d\} \in \mathcal{F}(G,g)$. We will show that there is some $h \in C_G(g)$ which maps F to $F' := \{\langle e_1 \rangle, \ldots, \langle e_d \rangle\}$. Fix $0 \neq x_i \in X_i$ such that $x_i g^* = x_{i+1}$ for $1 \leq i < d$. Since $det(g^*) = t_i$, $x_d g^* = t_i x_1$, so the matrices of g^* with respect to the bases $x_1, \ldots, x_d$ and $e_1, \ldots, e_d$ are the same, and the transformation given by $x_i \mapsto e_i$ centralizes g^*. In the unitary and orthogonal cases, we know that all the X_i have the same isometry type by the transitivity of $\langle g \rangle$. Furthermore, the argument given in the proof of Lemma 3.69 shows that the x_i are mutually orthogonal, so $V = \perp_{i=1}^d X_i$. Now since the isometry type of all the X_i is uniquely determined by the isometry type of V, we may assume that the x_i have been chosen so that the map $x_i \mapsto e_i$ is an isometry. We have shown so far that $C_P(g_i)$ is transitive on $\mathcal{F}(G,g)$, where P is any one of $PGL(V), PGU(V)$ or $PGO(V) \cong SO(V)$. It remains to show that the P-orbit of F does not split into smaller orbits in cases (L3) and (U3), where

$g_i = g_1$. In these cases, the stabilizer of F' contains g_i for all $i > 1$, and it follows immediately that the P-orbit does not split. □

We can now count $\mathcal{F}(G, g_i)$ by determining $|C_G(g_i) \cap stab_G(F)|$ for $F \in \mathcal{F}(G, g_i)$. We first show that we may actually assume that G is one of $PGL(V)$, $PGU(V)$ or $PSO(V)$.

Lemma 3.85 *(1)* $\mathcal{F}(PGL(V), f_d) = \mathcal{F}(L(V), f_d)$.

(2) $\mathcal{F}(PGU(V), f_d) = \mathcal{F}(PSU(V), f_d)$.

(3) $\mathcal{F}(PSO(V), f_d) = \mathcal{F}(P\Omega(V), f_d)$.

Proof: If this is false, there exists some f_d-frame F for one of the larger groups whose stabilizer in the corresponding smaller group is trivial. By transitivity, we may assume that $F = \{\langle e_1\rangle, \ldots, \langle e_d\rangle\}$. We may assume in the linear case that $d|q-1$ and in the unitary case that $d|\sqrt{q}+1$, for otherwise there is nothing to prove in these cases. Note that the smaller group is normal in the larger group in each case, and has index d in the linear and unitary cases and index two in the orthogonal cases. This means that if the lemma is false, the stabilizer of F in the larger group has order d in the linear unitary cases and two in the orthogonal case. Of course this is not true. Indeed, let $M = stab_G(F)$, where G is one of the larger groups. Then M^* is the product of the diagonal matrices which lie in G^* by the permutation matrices which lie in G^*, and it is easily seen that M cannot be cyclic. □

Lemma 3.86 *Let $G \in PC(V)$ with $g_i \in G$ and let $F = \{X_1, \ldots, X_d\} \in \mathcal{F}(G, g_i)$.*

(1) In case (L1), $|C_{PGL(V)}(g_1) \cap stab_{PGL(V)}(F)| = d$.

(2) In cases (L2),(L3), $|C_{PGL(V)}(g_i) \cap stab_{PGL(V)}(F)| = d^2$ for all g_i.

(3) In case (U1), $|C_{PGU(V)}(g_1) \cap stab_{PGU(V)}(F)| = d$.

(4) In cases (U2),(U3), $|C_{PGU(V)}(g_i) \cap stab_{PGU(V)}(F)| = d^2$ *for all* g_i.

(5) In cases (O1),(O2), $|C_{SO(V)}(p_1) \cap stab_{SO(V)}(F)| = d$.

Proof: We may assume that $F = \{\langle e_1\rangle, \ldots, \langle e_d\rangle\}$. Let $M = stab_H(F)$, where H is one of $PGL(V)$, $PGU(V)$ or $SO(V)$. In the linear case, M^* is the monomial subgroup of H, that is, with respect to the basis B, M^* is the split extension of the group of diagonal matrices by the group of permutation matrices. Thus M is the split extension of a group $X \cong Z_{q-1}^{d-1}$ by a group $S \cong S_d$. Let $\tilde{M} = M/X$, and let $K = C_M(g_i)$. Since $\tilde{g}_i$ corresponds to a d-cycle in S_d, $|\tilde{K}| = d$ and $|K| = d|C_X(g_i)|$. Let $z \in X$. Then $z \in C_X(g_i)$ if and only if $(z^*)^{p_i} = \alpha z^*$ for some $\alpha \in \mathbf{F}_q$. Write $z^* = diag(z_1, \ldots, z_d)$. Then $(z^*)^{p_i} = diag(z_d, z_1, \ldots, z_{d-1})$, so $(z^*)^{p_i} = \alpha z^*$ if and only if $z_d = \alpha z_1, z_1 = \alpha z_2, \ldots, z_{d-1} = \alpha z_d$. Thus we must have $\alpha^d = 1$, and each such α gives a different $z \in C_X(g_i)$. The claim in the linear case now follows. The other two cases are similar. In the unitary case, M is a split extension of a group $X \cong Z_{\sqrt{q}+1}^{d-1}$ by a group $S \cong S_d$, and the same analysis gives the desired result. In the orthogonal case, M is the split extension of the group $X \cong Z_2^{d-1}$ of the diagonal matrices in $SO(V)$ by the group $S \cong S_d$ of positive and negative permutation matrices in $SO(V)$. In this case, $C_X(p_1) = 1$. □

Main Lemma 3.87 *For* $g_i \in G \in PC(V)$*, we have the following results.*

(1) In case (L1), $\Lambda_{\mathcal{I}_1(G),G}(g_1) = \frac{|C_{PGL(V)}(g_1)|}{d}$.

(2) In case (L2), $\Lambda_{\mathcal{I}_1(G),G}(g_1) = \frac{|C_{PGL(V)}(g_1)|}{d^2}$,

and for $i > 1$, $\Lambda_{\mathcal{I}_1(G),G}(g_i) = \frac{|C_{PGL(V)}(g_i)|}{d^2} - 1$.

(3) In case (L3), $\Lambda_{\mathcal{I}_1(G),G}(g_1) = \frac{|C_{PGL(V)}(g_1)|}{d^2}$.

(4) In case (U1), $\Lambda_{\mathcal{I}_1(G),G}(g_1) = \frac{|C_{PGU(V)}(g_1)|}{d}$.

(5) In case (U2), $\Lambda_{\mathcal{I}_1(G),G}(g_1) = \frac{|C_{PGU(V)}(g_1)|}{d^2}$,

and for $i > 1$, $\Lambda_{\mathcal{I}_1(G),G}(g_i) = \frac{|C_{PGU(V)}(g_i)|}{d^2} - 1$.

(6) In case (U3), $\Lambda_{\mathcal{I}_1(G),G}(g_1) = \frac{|C_{PGU(V)}(g_1)|}{d}$.

(7) In cases (O1) and (O2), $\Lambda_{\mathcal{I}_1(G),G}(p_1) = \frac{|C_{SO(V)}(p_1)|}{d}$.

Proof: This follows from Corollary 3.75 and Lemmas 3.76, 3.79. 3.84, 3.85 and 3.86. □

The only elements of $G \in PC(V)$ left to examine are those which are contained in a Coxeter torus and do not have order 1 or d. This case is easy.

Main Lemma 3.88 *Let* $G \in PC(V)$ *be one of* $L(V), PGL(V), PSU(V)$ *or* $PGU(V)$. *Let* $g \in G$ *be conjugate to some element of* C. *If* $g^d \neq 1$ *then* $\Lambda_{\mathcal{I}_1(G),G}(g) = -1$.

Proof: This follows immediately from Corollary 3.75 and Lemma 3.76, since $\mathcal{C}_1(G,g) = \mathcal{F}(G,g) = \emptyset$. □

3.4 The end of the proof of the main theorems

The proof of the main theorem of this chapter is essentially complete. If only remains to confirm that the induced characters described in the main theorem are actually equal to the characters $\Lambda_{\mathcal{I}_1(G),G}$ that we have calculated. We first state a formula which follows easily from direct calculation and appears on page 64 of [25].

Proposition 3.89 *Let* H *be a subgroup of* K *and let* ϕ *be a character of* h. *For* $h \in H$, *let* $h_1, \ldots, h_r$ *be a set of representatives for the* H*-conjugacy classes which are contained in the* K*-conjugacy class of* h. *Then*

$$\phi^K(h) = |C_K(h)| \sum_{i=1}^{r} \frac{\phi(h_i)}{|C_H(h_i)|}.$$

Now we state some facts about the structure of N and the way in which N sits in G in the linear and unitary cases.

Lemma 3.90 *Let G, N, C be as in Theorem 3.22. Let $1 \neq y \in C$. Then*

$$C_G(y) = \begin{cases} N & \text{if } d|q-1 \text{ and } |y| = d \\ C & \text{otherwise} \end{cases}$$

Proof: By Lemma 3.16(3), $C_{G^*}(y^*) = C^*$. Thus if $g \in G \setminus C$ centralizes y, then $(y^*)^{g^*} = y^*z$ for some $1 \neq z \in Z$. We temporarily assume that y^* has prime order s. Then we must have $|z| = s = |y|$, and since $gcd(|C|, |Z|) = 1$ or d by Lemma 3.14, $|y^*| = d$ and $d|q-1$. It now follows that d is the only prime divisor of $|y|$, and since $d^2 \not| |C|$, we have $|y| = d$. The Lemma now follows. □

Lemma 3.91 *Let G, N, C be as in Theorem 3.23. Let $1 \neq y \in C$. Then*

$$C_G(y) = \begin{cases} N & \text{if } d|\sqrt{q}+1 \text{ and } |y| = d \\ C & \text{otherwise} \end{cases}$$

Proof: This follows immediately from the above Lemma. □

Lemma 3.92 *Let G, N, C be as in Theorem 3.22 or Theorem 3.23. In cases (L1), (L3), (U1) and (U3), $N \setminus C$ consists of $(d-1)|C|$ G-conjugates of $g_1 = f_d$. In cases (L2) and (U2), C contains one conjugate of g_i for each $i > 1$, and $N \setminus C$ contains $\frac{d-1}{d}|C|$ conjugates of g_i for each $i \in [d]$.*

Proof: Recall that the action of $g_1 = f_d$ on C is given by $c^{g_1} = c^q$ for all $c \in C$. It follows that in the first four cases, $C_C(g_1) = 1$. This means that F_d is a Frobenius complement in N, and the claim follows immediately from Lemma 3.79(1). In cases (L2) and (U2), since d divides $|C|$, C contains a subgroup H of order d. By Lemma 3.79(2), H is generated by a conjugate of g_i for some $i > 1$. Now the nontrivial powers of p_i have $d-1$ distinct determinants, so C contains a conjugate of each g_i with

$i > 1$. By Lemma 3.14, $C \setminus H$ does not contain any d-elements. Now let $D = \langle g_1 \rangle \times H$. Since $D \in Syl_d(N)$, every d-element of N is a conjugate of some element of D. By Lemma 3.79(1), every nontrivial power of g_1 is conjugate to g_1 in G, so every nontrivial d-element of N is conjugate in G to an element of the form kg_i, with k conjugate to g_1 in G and $kg_i = g_i k$. It remains to show that such an element is conjugate to g_i in G. Since k centralizes g_i, k acts on the set of g_i-frames. We know from Lemmas 3.90 and 3.91 that $C_G(g_i) = \langle k, g_i \rangle$, and it follows from Lemma 3.86 that $|\mathcal{F}(G, g_i)| = 1$. Thus kg_i stabilizes the same frame as g_i, and since $det(g_i^*) = det((kg_i)^*)$, g_i and kg_i are conjugate in G. □

It is now easy to show that $-\Lambda_{\mathcal{I}_1(G),G}$ is indeed the given induced character in all of our cases. We will examine each case, temporarily excluding case (O2). In each of the remaining cases, it follows immediately from Lemma 3.16 and Main Lemma 3.25 that the degrees are correct, so we examine nonidentity elements.

Lemma 3.93 *Let G, N, C, θ be as in Theorem 3.22 or Theorem 3.23. Let $c \in C$ with $c^d \neq 1$. Then $\theta^G(c) = 1$.*

Proof: By Lemmas 3.90 and 3.91, c is contained in a unique Coxeter torus of $PGL(V)$, so any G-conjugate of c in N is already conjugate to c in N. The Lemma now follows from Proposition 3.89. □

Lemma 3.94 *Let G, N, C, θ be as in Theorem 3.22 or Theorem 3.23. In cases (L1), (L3), (U1) and (U3) we have $\theta^G(g_1) = -\frac{|C_G(g_1)|}{d}$.*

Proof: Note that by Lemma 3.92, for each primitive d^{th} root of unity r there exists a unique N-conjugacy class of G-conjugates g of g_1 satisfying $\theta(g) = r$. By Lemma 3.92, $|C_N(g)| = d$ for each such g. The Lemma now follows immediately from Proposition 3.89. □

Lemma 3.95 *Let G, N, C, θ be as in Theorem 3.22 or Theorem 3.23. In cases (L2) and (U2) we have $\theta^G(g_1) = -\frac{|C_G(g_1)|}{d^2}$.*

Proof: In this case, $|C_N(g_1)| = d^2$ by Lemma 3.90, and we argue as in the proof of the previous lemma. □

Lemma 3.96 *Let G, N, C, θ be as in Theorem 3.22 or Theorem 3.23. In cases (L2) and (U2) we have $\theta^G(g_i) = 1 - \frac{|C_G(g_1)|}{d^2}$ for all $i > 1$.*

Proof: Here we apply Lemma 3.92 to see that there is one conjugate of g_i in N satisfying $\theta(g) = 1$, and that for each primitive d^{th} root of unity r there is one N-conjugacy class of G-conjugates of g_i whose representative satisfies $\theta(g) = r$. Now we apply Proposition 3.89. □

Lemma 3.97 *Let $G = SO(V)$ and let θ be as in Theorem 3.24. Then $\theta^G(f_d^*) = -\frac{|C_G(f_d^*)|}{d}$.*

Proof: This follows immediately from Proposition 3.89. □

By the previous five lemmas and Main Lemmas 3.25, 3.81, 3.83, 3.87 and 3.88 the proof of the main theorem is complete except in case (O2), that is, the case where $G = \Omega(V)$. Note that we have shown in Main Lemmas 3.81, 3.83 and 3.87 that $\Lambda_{\mathcal{I}_1(\Omega(V)),\Omega(V)} = (\Lambda_{\mathcal{I}_1(SO(V)),SO(V)})_{\Omega(V)}$. The theorem in case (O2) now follows from Mackey's Lemma, which appears on page 74 of [25] and is stated below.

Theorem 3.98 (Mackey) *Let H, K be subgroups of G and let T be a set of $H-K$ double coset representatives in G. Let ϕ be a character of H. Then $(\phi^G)_K = \sum_{t \in T} (\phi^t_{H^t \cap K})^K$.*

The proof of the main theorem is now complete.

Chapter 4

The Möbius numbers of orthogonal groups in odd characteristic and prime dimension

In this chapter, we will find a formula for $\mu(1,G)$ when $G = SO_d(q)$ or $\Omega_d(q)$ with q odd and d an odd prime satisfying certain conditions which will be described later. This will be done by computing $\sum_{H\in\mathcal{I}}\mu(1,H)$ for a large ideal in the subgroup lattice of G. The results of the previous chapter in the orthogonal case determine the sum of the Möbius numbers of the reducible subgroups of G, so we must describe in some useful manner the irreducible subgroups of G. We will use Aschbacher's classification of the maximal subgroups of G, as described in [3] and [28]. We retain the notation used in the previous chapter. In particular, $\mathcal{I}_1(G)$ is the set of reducible subgroups of G.

Definition 4.1 *Let V be a nondegenerate orthogonal space of odd prime dimension d over a field $\mathbf{F}_q$ of order $q = p^a$, with p an odd prime. Let f be the given symmetric form on V.*

(1) An isometric decomposition of V is a collection $\{V_1,\ldots,V_d\}$ of 1-spaces from V such that $V = \perp_{i=1}^{d} V_i$ and all the V_i have the same isometry type. $\mathcal{E}$ is the set of isometric decompositions of V.

(2) If $E = \{V_1,\ldots,V_d\} \in \mathcal{E}$, then M_E is the stabilizer of E in $GO(V)$.

(3) For $G = SO(V)$ or $\Omega(V)$, $\mathcal{C}_2(G) := \{M_E \cap G : E \in \mathcal{E}\}$.

(4) $\mathcal{SF}$ is the set of subfields of $\mathbf{F}_q$ and $\mathcal{MSF}$ is the set of maximal subfields of $\mathbf{F}_q$. If $\mathbf{F}_* \in \mathcal{SF}$ then $O(\mathbf{F}_*)$ is the set of additive subgroups W of V which are d-dimensional

$\mathbf{F}_*$-subspaces of V such that the $\mathbf{F}_q$-span of W is V and $f_{|W}$ is a nondegenerate symmetric bilinear form on W which takes values in $\alpha\mathbf{F}_*$ for some $\alpha \in \mathbf{F}_q^*$.

(5) For $\mathbf{F}_* \in \mathcal{SF}$ and $W \in O(\mathbf{F}_*)$, $M_*(W)$ is the stabilizer of W in $GO(V)$.

(6) For $G = SO(V)$ or $\Omega(V)$,

$$\mathcal{C}_5(G) := \{M_*(W) \cap G : \mathbf{F}_* \in \mathcal{MSF}, W \in O(\mathbf{F}_*)\}.$$

(7) For $G = SO(V)$ or $\Omega(V)$ and $i \in \{2, 5\}$, $\mathcal{I}_i(G)$ is the ideal in the subgroup lattice of G generated by $\mathcal{C}_i(G)$.

(8) For $G = SO(V)$ or $\Omega(V)$, $\mathcal{C}(G) = \mathcal{I}_1(G) \cup \mathcal{I}_2(G) \cup \mathcal{I}_5(G)$, and $\mathcal{S}(G)$ is the set of proper subgroups of G which do not contain $\Omega(V)$ and are not contained in $\mathcal{C}(G)$.

The following lemma is Aschbacher's theorem applied to orthogonal groups in odd prime dimension over fields of odd order, and can be read off directly from Table 3.5.D of [28]. Note that if $H \in \mathcal{S}(G)$ as defined above, the embedding of H in G is an imprimitive irreducible representation of H which is not realizable over any subfield of $\mathbf{F}_q$.

Lemma 4.2 (Aschbacher,Kleidman-Liebeck) *Let V be an orthogonal space of odd prime dimension over a field $\mathbf{F}_q$ of odd order. Let G be one of $GO(V)$, $SO(V)$ or $\Omega(V)$. If $H \in \mathcal{S}(G)$, then there is some nonabelian simple group $S \lhd H$ such that $C_H(S) = 1$, that is, we may regard H as a subgroup of $Aut(S)$ which contains $Inn(S) \cong S$. Furthermore, H acts absolutely irreducibly on V, that is, the representation determined by the embedding of H in G is irreducible over any extension field of $\mathbf{F}_q$. Finally, the representation determined by the embedding of H in G cannot be realized over any proper subfield of $\mathbf{F}_q$.*

Our goal is to compute $\sum_{H \in \mathcal{C}(G)} \mu(1, H)$. The achievement of this goal is in some sense the best possible result in our attempt to compute $\mu(1, G)$, since it is not currently possible to determine the members of $\mathcal{S}(GO(V))$ for an arbitrary nondegenerate orthogonal space V. We begin by restating Lemma 3.25(3).

Lemma 4.3 *Let $\mathbf{F}_q$ be a finite field of odd order with $q > 3$ and let V be a vector space of odd prime dimension d over $\mathbf{F}_q$. If $G = SO(V)$ or $\Omega(V)$, then*

$$\sum_{H \in \mathcal{I}_1(G)} \mu(1, H) = \frac{|SO(V)|}{d}.$$

We first examine subgroups contained in $\mathcal{I}_2(G) \setminus \mathcal{I}_1(G)$.

Lemma 4.4 *Let V be a nondegenerate orthogonal space of prime dimension d over a field $\mathbf{F}_q$ of odd order. Let $E = \{V_1, \ldots, V_d\}$ be an isometric decomposition of V.*

(1) M_E is isomorphic to the wreath product $S_d\,[Z_2]$.

(2) $M_E \cap SO(V)$ is a semidirect product whose kernel T is elementary abelian of order 2^{d-1}, with a complement isomorphic to S_d acting on T as it acts on a complement to the unique trivial submodule of its natural permutation module over $\mathbf{F}_2$. This complement is orthogonal to the trivial module with respect to the symmetric form with respect to which S_d permutes an orthonormal basis.

(3) If $q \equiv 1, 7 \bmod 8$, then $M_E \cap SO(V) \leq \Omega(V)$. Otherwise, $M_E \cap \Omega(V)$ is a semidirect product with kernel T and complement isomorphic to A_d acting as in (2) above.

Proof: Fix $0 \neq v_i \in V_i$ such that $(v_i, v_i) = (v_j, v_j)$ for all $i, j \in [d]$. M_E permutes the V_i, and any element of $GO(V)$ which permutes the V_i is contained in M_E. The kernel T of the action of M_E on the V_i consists of elements of $GO(V)$ fixing all the V_i. All of these elements are diagonal with respect to the basis $v_1, \ldots, v_d$ of V. Since $V = \perp_{i=1}^{d} V_i$, the V_i are certainly nondegenerate. It follows that with respect to the given basis, T consists of all matrices of the form $diag(\alpha_1, \ldots, \alpha_d)$ with $\alpha \in \{1, -1\}$ for all i. Thus T is elementary abelian of order 2^d and $|M_E| = d!2^d$. The elements of $GL(V)$ which permute the v_i certainly lie in $GO(V)$ and stabilize E. They clearly form a complement to T in M_E, call it P. For $i \in [d]$, let $g_i \in M_E$ be the reflection r_{v_i}. Then the g_i form an $\mathbf{F}_2$-basis for T, which is clearly permuted by the conjugation action of P

in the same manner that P permutes the V_i. This proves (1). Now with respect to the given basis, $T \cap SO(V) = \left\{diag(\alpha_1, \ldots, \alpha_d) \in M_E : \prod_{i=1}^{d} \alpha_i = 1\right\}$ forms a P-invariant complement in T to the 1-space generated by -1, which is orthogonal with respect to the obvious symmetric form. Let $\phi : P \to S_d$ be the isomorphism induced by the action of P on the V_i. Set $Q = \{g : g \in P, \phi(g) \in A_d\} \cup \{-g : g \in P, \phi(g) \notin A_d\}$. Then $Q \leq M_E \cap SO(V)$ acts on T in the same way as P. Claim (2) follows immediately. Every element of $T \cap SO(V)$ is a product of evenly many of the g_i, and since (v_i, v_i) is independent of i, $T \cap SO(V) \leq ker\Theta = \Omega(V)$. The set of permutation matrices in Q is isomorphic to A_d and therefore contains no normal subgroup of index two. Thus this subgroup lies in $M_E \cap \Omega(V)$, and it remains to determine whether the set of negative permutation matrices in Q lies in $\Omega(V)$. It suffices to consider the element $g = r_{v_1 - v_2} \prod_{i=1}^{d} r_{v_i}$, which is a negative permutation matrix acting like a transposition on the V_i. Now $(v_1 - v_2, v_1 - v_2) \prod_{i=1}^{d} (v_i, v_i) = 2(v_1, v_1)^{d+1}$, which is a square in $\mathbf{F}_q$ if and only if $2 \in \mathbf{F}_q^2$. Since $2 \in \mathbf{F}_q^2$ if and only if $q \equiv 1, 7 \bmod 8$ (see [15], p.40), we have (3). $\square$

Lemma 4.5 *Let V be a nondegenerate orthogonal space of odd prime dimension d over a field $\mathbf{F}_q$ of odd order. Let $E = \{V_1, \ldots, V_d\}$ be an isometric decomposition of V. Set $M = M_E \cap SO(V)$ and $L = M_E \cap \Omega(V)$. Let T be the kernel of the action of M on the V_i. Then all complements to T in M are conjugate in M and all complements to T in L are conjugate in L.*

Proof: Fix a basis $v_1, \ldots, v_d$ for V such that $0 \neq v_i \in V_i$ and $(v_i, v_i) = (v_j, v_j)$ for all $i, j \in [d]$. Let Q be the subgroup of M consisting of the elements which are permutation matrices with respect to this basis, so $Q \cong A_d$. Let R be the set of elements of M which are negative permutation matrices with respect to this basis, and set $P = Q \cup R \leq M$, so $P \cong S_d$ is a complement to T in M. Note that if $L < M$ then $L = QT$. It is known that $H^1(Q, T) = 0$, that is, all complements to T in QT are conjugate to Q in QT (see [2], p.74). This settles the claim for L when $L < M$. Now let C be a complement to T in PT. C contains a normal subgroup C' of index two, with $C' \cong A_d$. Since C' contains no normal subgroup of index two, $C' \leq L$. Thus C' is conjugate to Q in L.

Now since $C_T(Q) = 1$, $N_{PT}(Q) = P$. It follows immediately that $C = N_{PT}(C')$ and C is conjugate to P in PT. $\square$

Lemma 4.6 *Let V be a nondegenerate orthogonal space of prime dimension d over a field $\mathbf{F}_q$ of odd order. Let $E = \{V_1, \ldots, V_d\}$ be an isometric decomposition of V. Set $M = M_E \cap SO(V)$. Let T be the kernel of the action of M on the V_i and let P be a complement to T in M. Let $D \leq P$ be a Sylow d-subgroup of M. Then $N_M(D) \leq P$.*

Proof: Let $\overline{M} = M/T$. Let $N = N_M(D)$. We may assume that D is generated by a permutation matrix of order d. It follows that $C_T(D) = 1$, so $N \cap T = 1$. Thus $N \cong \overline{N}$. Since d does not divide $|T|$, $\overline{N} = N_{\overline{M}}(\overline{D})$, so $N_P(D) \cong \overline{N}$ and we are done. $\square$

With the above information on the structure of $M = M_E \cap SO(V)$ in hand, we can calculate the sum of the Möbius numbers of the irreducible subgroups of M if d satisfies the condition given in the definition below.

Definition 4.7 *An odd prime d is called solvable if every transitive proper subgroup of A_d is solvable.*

Note that if d is a solvable odd prime then a transitive subgroup of S_d which does not contain A_d contains a normal d-subgroup.

Lemma 4.8 *Let V be a nondegenerate orthogonal space of dimension d over a field $\mathbf{F}_q$ of odd order, with d a solvable odd prime. Let $E = \{V_1, \ldots, V_d\}$ be an isometric decomposition of V, and set $M = M_E \cap SO(V)$. Let T be the kernel of the action of M on the V_i. Let $H \leq M$. Then H acts irreducibly on V if and only if d divides $|H|$ and $H \cap T \neq 1$.*

Proof: Set $\overline{M} = M/T \cong S_d$, and fix $H \leq M$. If d does not divide $|H|$, then H is not transitive on the V_i and the orbits of H span H-invariant proper subspaces of V. If d divides $|H|$ and $H \cap T = 1$, then $H \cong \overline{H}$, so H is isomorphic to a transitive subgroup of S_d. Since d is a solvable prime, either $H \leq N_M(D)$ for some $D \in Syl_d(M)$ or H is isomorphic to one of A_d or S_d. By Lemmas 4.5 and 4.6, H is contained in some complement to T in M. By Lemma 4.6, we may assume that H consists of positive and negative permutation matrices with respect to the basis $v_1, \ldots, v_d$ with $v_i \in V_i$. Now the 1-space spanned by $\sum_{i=1}^{d} v_i$ is H-invariant, so H is reducible.

Now assume that d divides $|H|$ and $H \cap T \neq 1$. Let $D \in Syl_d(H)$ and set $K = D(H \cap T)$. We will show that K acts irreducibly on V. Since $C_T(D) = 1$, K is a Frobenius group with complement D and kernel $N = H \cap T$. Since $gcd(|N|, q) = 1$, every irreducible $\mathbf{F}_q$-representation of K either has degree at least d or satisfies $N \leq ker(\phi)$ (see [25], Theorem 15.16). Let $1 \neq n \in N$, so $n = diag(\alpha_1, \ldots, \alpha_d)$ with respect to the basis $v_1, \ldots, v_d$ with each $\alpha_i = 1$ or -1. Let W be the span of the V_i such that $\alpha_i = 1$. If X is a K-invariant subspace of V on which n acts trivially, then $X \leq W$. However, it is clear that D does not preserve any nontrivial subspace of W. Thus V must be an irreducible K-module. □

After finishing our examination of orthogonal groups whose dimension is a solvable prime, we will see that the "only if" part of Lemma 4.8 can be false when d is an odd prime which is not solvable.

Lemma 4.9 *Let V be a nondegenerate orthogonal space of odd prime dimension d over a field $\mathbf{F}_q$ of odd order. Let $E = \{V_1, \ldots, V_d\}$ be an isometric decomposition of V. Set $M = M_E \cap SO(V)$. Let T be the kernel of the action of M on the V_i, and let $D \in Syl_d(M)$. Then D is contained in a unique complement to T in M.*

Proof: This follows immediately from Lemmas 4.5 and 4.6, and the fact that a complement to T in M is self normalizing. Let P be a complement to T containing D. There are $[M : P]$ complements to T, each of which contains $[P : N_P(D)] = [P : N_M(D)]$ conjugates of D. Since $|Syl_d(M)| = [M : N_M(D)]$, the claim is correct. □

Corollary 4.10 *Let V be a nondegenerate orthogonal space of dimension d over a field $\mathbf{F}_q$ of odd order, with d a solvable odd prime. Let $E = \{V_1, \ldots, V_d\}$ be an isometric decomposition of V. Set $M = M_E \cap SO(V)$ and $L = M_E \cap \Omega(V)$. Let $\mathcal{I}(M)$ be the set* *of subgroups of M which act irreducibly on V and define $\mathcal{I}(L)$ similarly. Then*

$$\sum_{H\in\mathcal{I}(M)} \mu(1,H) = -2^{d-1}(d-1)!,$$

and if $L < M$ then

$$\sum_{H\in\mathcal{I}(L)} \mu(1,H) = -2^{d-1}((d-1)! - \frac{d!}{2}).$$

Proof: Let T be the kernel of the action of M on the V_i, and let P and Q be complements to T in M and L, respectively. Set $\mathcal{D}(M) = \{H \leq M : d \mid |H|\}$ and $\mathcal{T}(M) = \{H \in \mathcal{D}(M) : H \cap T = 1\}$. Define $\mathcal{D}(L)$ and $\mathcal{T}(L)$ similarly. By Lemma 4.8,

$$\sum_{H\in\mathcal{I}(M)} \mu(1,H) = \sum_{H\in\mathcal{D}(M)} \mu(1,H) - \sum_{H\in\mathcal{T}(M)} \mu(1,H),$$

and a similar formula holds for L.

We define closures on the subgroup lattices of M and L, both of which will be denoted by $H \mapsto \tilde{H}$, by $\tilde{H} = HT$. Note that d divides $|\tilde{H}|$ if and only if d divides $|H|$. Since $\tilde{1} = T$, it follows immediately from Theorem 2.3 that

$$\sum_{H\in\mathcal{D}(M)} \mu(1,H) = \sum_{H\in\mathcal{D}(L)} \mu(1,H) = 0.$$

It remains to evaluate $\sum_{H\in\mathcal{T}(M)} \mu(1,H)$ and $\sum_{H\in\mathcal{T}(L)} \mu(1,H)$. By Lemmas 4.9 and 4.5, each element of $\mathcal{T}(M)$ is contained in a unique conjugate of P, and there are $[M:P] = 2^{d-1}$ conjugates of P in M. A subgroup of P lies in $\mathcal{T}(M)$ if and only if it is transitive on the V_i, that is, if and only if it is transitive in the natural representation of S_d. Let $\mathcal{T}_d$ be the set of transitive subgroups of S_d. Define a closure on the lattice of subgroups of S_d by mapping H to the largest subgroup of S_d with the same orbits as H. Note that 1 is closed, the lattice of closed subgroups is isomorphic to the lattice Π_d of partitions of $[d]$, and $H \mapsto S_d$ if and only if H is transitive. Thus by Theorem 2.3 and our argument so far we have

$$\sum_{H\in\mathcal{I}(M)} \mu(1,H) = -\sum_{H\in\mathcal{T}(M)} \mu(1,H) = -2^{d-1}\mu_{\Pi_d}(\hat{0},\hat{1}).$$

The first claim of the corollary now follows from Lemma 2.7. When $L < M$, we apply the argument of the previous paragraph to the lattice of subgroups of $Q \cong A_d$. The lattice of closed subgroups with respect to the orbit closure is isomorphic to the lattice obtained by removing from Π_d all of its atoms, that is, the partitions of $[d]$ into one 2-set and $d-2$ 1-sets. Let $\mathcal{A}$ be the set of atoms from Π_d and let Π_d^* be the lattice obtained by removing all of the elements of $\mathcal{A}$ from Π_d. It follows easily from Lemma 2.7 that

$$\mu_{\Pi_d^*}(\hat{0},\hat{1}) = \sum_{a\in\mathcal{A}} \mu_{\Pi_d}(a,\hat{1}) + \mu_{\Pi_d}(\hat{0},\hat{1}) = -\binom{d}{2}(d-2)! + (d-1)!,$$

and the second claim follows. □

Lemma 4.11 *Let V be a nondegenerate orthogonal space of dimension d over a field $\mathbf{F}_q$ of odd order, with d a solvable odd prime. Let $E = \{V_1, \ldots, V_d\}$ and $F = \{W_1, \ldots, W_d\}$ be distinct isometric decompositions of V. Set $K = M_E \cap SO(V)$ and $M = M_F \cap SO(V)$. Then $K \cap M$ acts reducibly on V.*

Proof: Assume the contrary, and set $H = K \cap M$. By Lemma 4.8 there exists $h \in H$ with $|h| = d$, and h cyclically permutes both the V_i and the W_j. Let T_E and T_F be the respective kernels for the actions of K on the V_i and M on the W_j. Set $H_E = H \cap T_E$ and $H_F = H \cap T_F$. Since d is a solvable prime, either H/H_E embeds in $Aut(Z_d)$ or H/H_E is isomorphic to one of A_d or S_d. It follows that $H_E = \mathbf{O}_2(H)$. By the same argument, $H_F = \mathbf{O}_2(H)$, so $H_E = H_F$. By Lemma 4.8, $H_E \neq 1$, so $T_E \cap T_F \neq 1$. In the language of the previous chapter, both E and F are h-frames with respect to $SO(V)$. However, by Lemma 3.73 we now have $T_E \cap T_F = 1$, giving a contradiction. □

Corollary 4.12 *Let V be a nondegenerate orthogonal space of dimension d over a field $\mathbf{F}_q$ of odd order, with d a solvable odd prime.*

(1) If $G = SO(V)$, then

$$\sum_{H\in\mathcal{I}_2(G)\setminus\mathcal{I}_1(G)} \mu(1,H) = -\frac{|G|}{d}.$$

(2) If $G = \Omega(V)$, then

$$\sum_{H \in \mathcal{I}_2(G) \setminus \mathcal{I}_1(G)} \mu(1,H) = \begin{cases} -2\frac{|G|}{d} & q \equiv 1,7 \bmod 8 \\ |G| - 2\frac{|G|}{d} & q \equiv 3,5 \bmod 8 \end{cases}$$

Proof: Let E be an isometric decomposition of V. Set $M = M_E \cap SO(V)$ and $L = M_E \cap \Omega(V)$. By Witt's Theorem, $GO(V)$ acts transitively on the set of isometric decompositions of V, and by Lemma 4.4(2), $SO(V)$ also acts transitively on this set. Thus there are $[SO(V) : M]$ isometric decompositions of V. The corollary now follows immediately from Lemmas 4.4 and 4.11 and Corollary 4.10, as we can determine the given sums by calculating the sums of the Möbius numbers of the irreducible subgroups of M and L and multiplying by $[SO(V) : M]$. □

Now we examine the elements of $\mathcal{I}_5(G) \setminus (\mathcal{I}_1(G) \cup \mathcal{I}_2(G))$.

Lemma 4.13 *Let V be a nondegenerate orthogonal space of odd dimension d over $\mathbf{F}_q$, where $q = p^a$ with p an odd prime. Let $\mathbf{F}_*$ be a subfield of $\mathbf{F}_q$ of order p^b, where b is a proper divisor of a and let $W \in O(\mathbf{F}_*)$. Then there is an embedding $\phi : GO(W) \hookrightarrow GO(V)$ such that*

(1) $Im\phi = M_*(W)$.

(2) $\phi^{-1}(SO(V)) = SO(W)$.

(3) If $\frac{a}{b}$ is even, then $\phi^{-1}(\Omega(V)) = SO(W)$, while if $\frac{a}{b}$ is odd, then $\phi^{-1}(\Omega(V)) = \Omega(W)$.

Proof: We may assume that $V = W \otimes_{\mathbf{F}_*} \mathbf{F}_q$ and identify W with the subspace $\{w \otimes 1 : w \in W\}$ (see [23], Corollary 5.13). Now define ϕ by $\phi(g)(w \otimes \alpha) = (wg \otimes \alpha)$. It is clear that $Im\phi \leq M_*(W)$, that $Im\phi$ induces every element of $GO(W)$ on W and that $Ker\phi = 1$. If two elements $g, h \in M_*(W)$ act the same on W, then gh^{-1} acts trivially on W. Since an $\mathbf{F}_*$-basis for W is an $\mathbf{F}_q$-basis for V, gh^{-1} acts trivially on V, so $g = h$. Thus $Im\phi = M_*(W)$. Since $\phi(g)$ acts on V as $g \otimes 1$, it follows easily from the definitions of determinant and tensor product that $Im\phi \cap SO(V) = \phi(SO(W))$. Note that either $\Omega(W)$ is simple or $d = p^b = 3$, in which case $SO(W) \cong S_4$ (see [2], p.253). In either case, $\Omega(W)$ is the only subgroup of index two in $SO(W)$. It follows that $\phi(\Omega(W)) \leq \Omega(V)$. It remains to determine when $\phi(SO(W)) \leq \Omega(V)$. Let $w \in W$ be nonsingular. Since an $\mathbf{F}_*$-basis for W is an $\mathbf{F}_q$-basis for V, $\phi(r_{w|W}) = r_{w|V}$, where r_w is the reflection in the hyperplane orthogonal to w. Thus the spinor norms $\Theta_{SO(W)}(g)$ and $\Theta_{SO(V)}(\phi(g))$ are equal for all $g \in SO(W)$. Since $[SO(W) : \Omega(W)] = 2$, there exists some $g \in SO(W)$ such that $\Theta_{SO(W)}(g) \neq \mathbf{F}_*^2$. It follows that $\phi(SO(W)) \leq \Omega(V)$ if and only if $\mathbf{F}_* \subseteq \mathbf{F}_q^2$. This last condition is equivalent to the condition that $\frac{a}{b}$ is even. □

Corollary 4.14 *Let V be a nondegenerate orthogonal space of odd prime dimension d over $\mathbf{F}_q$, where $q = p^a$ with p an odd prime. Let $G = SO(V)$ or $\Omega(V)$. Let $\mathbf{F}_*$ be a subfield of $\mathbf{F}_q$ with $|\mathbf{F}_*| > 3$ and let $W \in O(\mathbf{F}_*)$. Then $M_*(W) \cap \Omega(V) \in \mathcal{I}_5(G) \setminus (\mathcal{I}_1(G) \cup \mathcal{I}_2(G))$.*

Proof: Let $\phi : GO(W) \hookrightarrow GO(V)$ be as in Lemma 4.13, and let $H = Im\phi \cap \Omega(V)$. By Lemma 2.10.6 of [28], $\phi(\Omega(W))$ acts absolutely irreducibly on V. It follows immediately from Lemma 4.13(3) that $H \notin \mathcal{I}_1(G)$. Next assume for contradiction that $H \in \mathcal{I}_2(G)$. Since $|\mathbf{F}_*| > 3$, $\Omega(W)$ is simple and $[H : \phi(\Omega(W))] = 1$ or 2. It follows from Lemma 4.4 that H embeds in S_d. However, it also follows from Lemma 4.4 that S_d embeds in H as a reducible subgroup of $GO(W)$, a contradiction. Finally, it is clear that $H \in \mathcal{I}_5(G)$, since if $\mathbf{E}_*$ is a maximal subfield of $\mathbf{F}_q$ containing $\mathbf{F}_*$ then there are embeddings $W \hookrightarrow W \otimes_{\mathbf{F}_*} \mathbf{E}_* \hookrightarrow W \otimes_{\mathbf{F}_*} \mathbf{F}_q$ which determine an embedding of H in an element of $O(\mathbf{E}_*)$ which is contained in $\mathcal{C}_5(G)$. □

Proposition 4.15 *Let V be a nondegenerate orthogonal space of odd prime dimension d over $\mathbf{F}_q$, where $q = p^a$ with p an odd prime. Let $G = SO(V)$ or $\Omega(V)$. Let $\mathbf{F}_*$ be a subfield of $\mathbf{F}_q$ and let $W \in O(\mathbf{F}_*)$. Let $H = M_*(W) \cap G$ and let $K \leq H$. If $K \in \mathcal{I}_1(H) \cup \mathcal{I}_2(H)$ with respect to the natural action of H on W, then $K \in \mathcal{I}_1(G) \cup \mathcal{I}_2(G)$.*

Proof: If $K \in \mathcal{I}_1(H)$ then the embedding of K in H is a reducible $\mathbf{F}_*$-representation of K, which remains reducible over the extension field $\mathbf{F}_q$, so $K \in \mathcal{I}_1(G)$. If $K \in \mathcal{I}_2(H)$ then there is some isometric decomposition $E = \{W_1, \ldots, W_d\}$ of $V_*(B)$ such that K permutes the W_i. Let V_i be the $\mathbf{F}_q$-span of W_i. Then $F = \{V_1, \ldots, V_d\}$ is an isometric decomposition of V, and K permutes the V_i, so $K \in \mathcal{I}_2(G)$. □

We are now in a position to describe the elements of $\mathcal{I}_5(G) \setminus (\mathcal{I}_1(G) \cup \mathcal{I}_2(G))$ in a manner which will allow us to determine our desired formula for $\mu(1, G)$ by induction on q.

Lemma 4.16 *Let V be a nondegenerate orthogonal space of odd prime dimension d over a field $\mathbf{F}_q$ of odd order, and let $1 \neq g \in SO(V)$. Then $C_{SO(V)}(g)$ acts reducibly on V.*

Proof: Let $p = |g|$. Since $C_{SO(V)}(g)$ centralizes any power of g, we may assume that p is prime. If $p|q$, then $\{v \in V : vg = v\}$ is a nontrivial proper subspace of V which is stabilized by $C_{GL(V)}(g)$. If $p = 2$, then there is some decomposition $V = W \oplus X$ such that $g_W = 1$ and $g_X = -1$, and $C_{GL(V)}(g)$ stabilizes both W and X. Since d is odd, $-1_V \notin SO(V)$, so both W and X are nontrivial. Finally, assume that p is odd and does not divide q, and assume for contradiction that $C_{SO(V)}(g)$ is irreducible. By (8-1)(6) and (7) of [18], V is orthogonally homogeneous as a $\langle g \rangle$-module. That is, there exists a decomposition $V = \perp_{i=1}^{s} V_i$ such that all the V_i are g-invariant and equivalent as $\langle g \rangle$-modules. Furthermore, there is no decomposition $V_i = W \perp X$ with W, X g-invariant. Since d is prime, either $s = d$ and each V_i is a 1-space, or $s = 1$ and $V_1 = V$. In the first case, each V_i is nondegenerate, so $g_{V_i} = 1$ or -1. Then $p = 2$, giving the desired contradiction. In the second case, by (8-1)(4) of [18], $C_{GO(V)}(g)$ is isomorphic to a subgroup of $GL_1(q^n)$ for some n. In particular, $C_{GO(V)}(g)$ is cyclic. Now by Lemma 3.16, no cyclic subgroup of $SO(V)$ acts irreducibly on V, again giving a contradiction. □

Definition 4.17 *Let V be a nondegenerate orthogonal space of odd prime dimension d over $\mathbf{F}_q$, where $q = p^a$ with p an odd prime. Let $G = SO(V)$ or $\Omega(V)$. $\mathcal{I}_5^*(G)$ is the set* *of all subgroups of G of the form $\phi(SO(W))$ or $\phi(\Omega(W))$, where $W \in O(\mathbf{F}_*)$ for some subfield $\mathbf{F}_*$ of $\mathbf{F}_q$, and $\phi : GO(W) \hookrightarrow GO(V)$ is as in Lemma 4.13.*

Lemma 4.18 *Let V be a nondegenerate orthogonal space of odd prime dimension d over $\mathbf{F}_q$, where $q = p^a$ with p an odd prime. Let $G = SO(V)$ or $\Omega(V)$. Let $K \in \mathcal{I}_5(G) \setminus (\mathcal{I}_1(G) \cup \mathcal{I}_2(G))$. Then either $K \in \mathcal{I}_5^*(G)$ or there exists a unique $H \in \mathcal{I}_5^*(G)$ such that $K \in \mathcal{S}(H)$ with respect to the natural action of H on its associated space $W \in O(\mathbf{F}_*)$.*

Proof: Let $\mathbf{F}_*$ be the smallest subfield of $\mathbf{F}_q$ such that $Tr(k) \in \mathbf{F}_*$ for all $k \in K$. Then by [25], Theorem 9.14, there exists a K-invariant additive subgroup $W \leq V$ which is a d-dimensional $\mathbf{F}_*$-subspace of V and whose $\mathbf{F}_q$ span is V, on which K acts absolutely irreducibly and primitively by Proposition 4.15. Furthermore, $\mathbf{F}_*$ is the smallest subfield of $\mathbf{F}_q$ with this property. By [3], (8.1)(1), $W \in O(\mathbf{F}_*)$. Thus if $K \notin \mathcal{I}_5^*(G)$ then every $H \in \mathcal{I}_5^*(G)$ which is minimal with respect to containing K is of the form $\phi(SO(W))$ or $\phi(\Omega(W))$ for some $W \in O(\mathbf{F}_*)$, where ϕ is as in Lemma 4.13. It is now sufficient to show that if $W, X \in O(\mathbf{F}_*)$ then either $M_*(W) = M_*(X)$ or $M_*(W) \cap M_*(X)$ is not irreducible.

First we prove that $M_*(W)$ and $M_*(X)$ are conjugate by an element of $SO(V)$ for all $W, X \in O(\mathbf{F}_*)$. Since an $\mathbf{F}_*$-basis for W is an $\mathbf{F}_q$-basis for V and X has the same property, W and X are similar $\mathbf{F}_*$-spaces. Let $w_1, w_2, \ldots, w_d$ and $x_1, x_2, \ldots, x_d$ be orthogonal bases for W and X, respectively, such that there is some $\alpha \in \mathbf{F}_q$ with $(x_i, x_i) = \alpha(w_j, w_j)$ for all i, j. Define $g \in GL(V)$ by $x_i g = w_i$. Then g is a similarity from V to itself, so there exists some $\beta \in \mathbf{F}_q$ such that $\beta g \in GO(V)$. Now either βg or $-\beta g$ is in $SO(V)$, and both conjugate $M_*(W)$ to $M_*(X)$. We now assume that $\beta g \in SO(V)$. Let σ be the automorphism of $\mathbf{F}_q$ whose centralizer in $\mathbf{F}_q$ is $\mathbf{F}_*$, and also denote by σ the automorphism of $GO(V)$ induced by the semilinear transformation $1 \otimes \sigma$ on $V = W \otimes \mathbf{F}_q$. Thus centralizer of σ in $GO(V)$ is $M_*(W)$. We will work in the semidirect product $\langle \sigma \rangle GO(V)$. In this group, $C_{GO(V)}(\sigma^{\beta g}) = M_*(X)$. Thus, $M_*(W) \cap M_*(X) \leq C_{GO(V)}([\sigma, \beta g])$. Since $[\sigma, \beta g] \in SO(V)$, it follows from Lemma 4.16

that $M_*(W) \cap M_*(X)$ is reducible unless $\beta g \in M_*(W)$, in which case $M_*(W) = M_*(X)$. $\square$

Theorem 4.19 *Fix an odd prime $p > 3$ and a solvable prime d. Let a be any natural number. Let V be a nondegenerate orthogonal space of dimension d over a field of order p^a. Set*

$$\omega(a) := \frac{\mu(1, \Omega(V)) + \sum_{H \in \mathcal{S}(\Omega(V))} \mu(1, H)}{|\Omega(V)|}$$

and

$$\sigma(a) := \frac{\mu(1, SO(V)) + \sum_{H \in \mathcal{S}(SO(V))} \mu(1, H)}{|\Omega(V)|}.$$

Then

$$\omega(a) = \begin{cases} -1 & p \equiv 3, 5 \bmod 8 \text{ and } a = 1 \\ 0 & \text{otherwise} \end{cases}$$

Furthermore, $\sigma(a) = -\omega(a)$.

Proof: For $G = \Omega(V)$ or $SO(V)$, define

$$f_G(a) = \frac{\sum_{H \in \mathcal{I}_1(G) \cup \mathcal{I}_2(G)} \mu(1, H)}{|\Omega(V)|}.$$

By Lemma 4.3 and Corollary 4.12, we have

$$f_G(a) = \begin{cases} 1 & \text{if } p \equiv 3, 5 \bmod 8, G = \Omega(V) \text{ and } a \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$$

Let $D(a)$ be the set of proper divisors of a and set $D_e(a) := \{b \in D(a) : 2 \mid \frac{a}{b}\}$ and $D_o(a) = D(a) \setminus D_e(a)$. For $b \in D(a)$, set $n(b) := \frac{|SO_d(p^a)|}{|SO_d(p^b)|} = \frac{|\Omega_d(p^a)|}{|\Omega_d(p^b)|}$. We saw in the proof of Lemma 4.18 that $SO(V)$ acts transitively by conjugation on any set consisting of all elements of $\mathcal{I}_5^*(G)$ of a given isomorphism type. It now follows from Lemma 4.13 that for each $b \in D(a)$, $\mathcal{I}_5^*(SO(V))$ consists of $n(b)$ subgroups isomorphic to $SO_d(p^b)$ and the same number of subgroups isomorphic to $\Omega_d(p^b)$. Also, for each $b \in D_e(a)$, $\mathcal{I}_5^*(\Omega(V))$ contains $n(b)$ subgroups isomorphic to $SO_d(p^b)$ and $n(b)$ subgroups isomorphic to $\Omega_d(p^b)$, while for $b \in D_o(a)$, $\mathcal{I}_5^*(\Omega(V))$ contains $n(b)$ subgroups isomorphic to $\Omega_d(p^b)$. It now follows from Lemma 4.2 and Lemma 4.18 that

$$-\omega(a) = f_{\Omega(V)}(a) + \sum_{b \in D_e(a)} (\omega(b) + \sigma(b)) + \sum_{b \in D_o(a)} \omega(b)),$$

and

$$-(\sigma(a)+\omega(a)) = f_{SO(V)}(a) + \sum_{b\in D(a)} (\omega(b)+\sigma(b)).$$

The theorem will now follow easily by induction on a. First assume that $p \equiv 1, 7 \bmod 8$. Then $f_G(a) = 0$ for all G and a. It follows immediately that $\omega(1) = \sigma(1) = 0$, and that induction on a gives $\omega(a) = \sigma(a) = 0$ for all a. Now assume that $p \equiv 3, 5 \bmod 8$. Then $f_{\Omega(V)}(a) = 1$ if a is odd and 0 if a is even, while $f_{SO(V)}(a) = 0$ for all a. Therefore, $\omega(1) = -1$ and $\sigma(1) = 1$. By induction on a, for $a > 1$ we have $\omega(a) = -(1+\omega(1)) = 0$ and $\sigma(a)+\omega(a) = -(\sigma(1)+\omega(1)) = 0$. □

We now give the promised discussion of the case where d is a nonsolvable prime. Let V be a nondegenerate orthogonal space of dimension d over $\mathbf{F}_q$ with q odd. Let E be an isometric decomposition of V and let $M = stab_{SO(V)}(E)$. With respect to the appropriate basis B for V, M consists of monomial matrices with entries from $\{1, -1\}$. Now for any group S, an embedding of S in M is determined by a subgroup H of S such that $[S : H] = d$ and $core_S(H) = 1$, along with a homomorphism $\phi : H \to Z_2$. In particular, the embedding of S in M is the representation induced from ϕ. Now if H has no subgroup of index two, then ϕ is trivial and the embedding of S in M is equivalent to a permutation representation of S. In the notation used in Lemma 4.5, the image of our embedding is contained in a complement to T in M, and therefore, S acts reducibly on V. However, for many simple groups $S \ncong A_d$ which have a subgroup H of prime index d, H contains a normal subgroup of index two. For example, if $S = M_{11}$ and $H = M_{10}$, then H has a subgroup of index two isomorphic to A_6. More typically, $S \cong L_n(q)$ with $d = \frac{q^n-1}{q-1}$ and H is the stabilizer of a 1-space in the natural action. Then H is a split extension of an elementary abelian group of order q^{n-1} by a group isomorphic to $GL_{n-1}(q)$, and if q is odd, H certainly has a subgroup of index two, since $GL_{n-1}(q)$ has such a subgroup. Now if H has a subgroup of index two, we can consider the representation of S induced from the nontrivial representation $\phi : H \to Z_2$ to be a complex representation of S. If ϕ^S is irreducible over $\mathbf{C}$, then it is also irreducible over any finite field whose characteristic does not divide S. Thus if we can find an irreducible complex representation ϕ^S of the type described above, we will have found infinitely many examples for which M contains irreducible groups which intersect T trivially. It turns out that the example $S = M_{11}$, $H = M_{10}$ given above provides such an irreducible representation. If we let ϕ^S be the complex representation described above, then it follows from Mackey's lemma that either ϕ^S is irreducible or it is the sum of two irreducible characters (see [25], problem 5.24). The only irreducible characters of M_{11} of degree less than 11 are the trivial character and some characters of degree ten (see [25], p. 291). However, by Frobenius reciprocity, the trivial representation is not a constituent of ϕ^S. Thus ϕ^S is irreducible. Note that the calculations made above in determining $\omega(a)$ and $\sigma(a)$ are valid for a nonsolvable prime, except that they ignore the groups described in this paragraph. Thus, one can give a formula for $\mu(1, SO(V))$ or $\mu(1, \Omega(V))$ when d is a nonsolvable odd prime, in which the "error term" involves not only the elements of $\mathcal{S}$ but also the groups described here.

We close this chapter by noting that the results above allow us to give a formula for $\mu(1, G)$ when $\Omega(V) \leq G \leq GO(V)$ and $dim(V)$, $\mathbf{F}_q$ are as in Theorem 4.19.

Proposition 4.20 *Let V be a nondegenerate orthogonal space of odd dimension d over a field $\mathbf{F}_q$ of odd order. Let Z be the subgroup of $GO(V)$ generated by -1_V. Let $X = \{-g : g \in SO(V)\}$, and define $TO(V) := \Omega(V) \cup X$. Then*

(1) If $\Omega(V) < G < GO(V)$ then G is one of $SO(V), TO(V)$ or $\Omega(V) \times Z$.

(2) $TO(V) \cong SO(V)$, so $\mu(1, TO(V)) = \mu(1, SO(V))$.

(3) $\mu(1, \Omega(V) \times Z) = -\mu(1, \Omega(V))$.

(4) $\mu(1, GO(V)) = -2\mu(1, SO(V))$.

Proof: It is easily seen that $TO(V)$ is a subgroup of $GO(V)$ which is distinct from $SO(V)$ and $\Omega(V) \times Z$. Since $\Omega(V)$ is a normal subgroup of index four in $GO(V)$, there are at most three proper subgroups of $GO(V)$ containing $\Omega(V)$, and (1) follows. The map from $SO(V)$ to $TO(V)$ which sends g to $-g$ if $g \notin \Omega(V)$ and is the identity on $\Omega(V)$ is an isomorphism, and (2) follows. Since $\Omega(V)$ is either simple or isomorphic to A_4, it contains no subgroup of index two, so the only complement to Z in $\Omega(V) \times Z$ is $\Omega(V)$. Any complement to Z in $GO(V)$ is of index two and does not contain Z, so the complements to Z in $GO(V)$ are $SO(V)$ and $TO(V)$. Now (3) and (4) follow immediately from Theorem 2.4. $\square$

Chapter 5

The Möbius numbers of some two dimensional linear groups

In this section we will determine $\mu(1, G)$ for certain groups G satisfying $L_2(q) \leq G \leq Aut(L_2(q))$, where q is an odd prime power. The values of $\mu(1, L_2(p))$ for p prime were given in [20]. The values of $\mu(1, L_2(q))$ when q is odd were given without proof, and with an error in the case $q = p^2$, $p \equiv 2, 3 \bmod 5$, in [16]. Many of the results in this chapter will be used in the determination of $\mu(1, S_n)$ for certain n. We begin with the groups $L_2(q)$ and $PGL_2(q)$, where $q > 3$ is odd.

Theorem 5.1 *Fix a prime $p > 3$. For a positive integer a, define*

$$\lambda(a) := \frac{\mu(1, L_2(p^a))}{|L_2(p^a)|}$$

and

$$\rho(a) := \frac{\mu(1, PGL_2(p^a))}{|L_2(p^a)|}.$$

Then

$$\rho(a) = \begin{cases} 1 & a = 1,\ p \equiv 3, 5 \pmod 8 \\ 0 & \textit{otherwise} \end{cases}$$

and

$$\lambda(1) = \begin{cases} 2 & q \equiv 1, 4 \pmod 5 \quad q \equiv 1, 7 \pmod 8 \\ 1 & q \equiv 1, 4 \pmod 5 \quad q \equiv 3, 5 \pmod 8 \\ 0 & q \equiv 2, 3 \pmod 5 \quad q \equiv 1, 7 \pmod 8 \\ -1 & q \equiv 0, 2, 3 \pmod 5 \quad q \equiv 3, 5 \pmod 8 \end{cases}$$

$$\lambda(2) = \begin{cases} 0 & p \equiv 0, 1, 4 \pmod 5 \\ 2 & p \equiv 2, 3 \pmod 5 \end{cases}$$

$$\lambda(a) = 0 \textit{ if } a > 2.$$

Proof: We will use Theorem 4.19, preserving the definitions of $\omega(a)$ and $\sigma(a)$ used therein. It is well known that for an odd prime power q, $PGL_2(q) \cong SO_3(q)$ and $L_2(q) \cong \Omega_3(q)$ (see for example [28], pp. 43-44). Since 3 is a solvable prime, we can determine $\mu(1, G)$ for $G = \Omega_3(q)$ or $SO_3(q)$ if we can calculate $\sum_{H \in \mathcal{S}(G)} \mu(1, H)$. To determine the members of $\mathcal{S}(G)$, we use the list of subgroups of $L_2(q)$ that appears in [14], (260). Note that in any case, if $H \in \mathcal{S}(G)$ then $S = soc(H)$ is a simple subgroup of $L_2(q)$. According to [14] (260), any simple subgroup of $L_2(q)$ which is not a subfield subgroup is isomorphic to A_5. Since $Aut(A_5) \cong S_5$, we can determine $\mathcal{S}(G)$ in all cases by determining all three dimensional absolutely irreducible representations of A_5 and S_5 in characteristic $p > 3$.

First note that if $p = 5$ then $A_5 \cong \Omega_3(5)$. According to [27], A_5 has a unique irreducible 3-dimensional character in characteristic five, so any subgroup of $G = \Omega_3(5^a)$ isomorphic to A_5 is contained in $\mathcal{I}_5(G)$. Thus $\mathcal{S}(\Omega_3(5^a)) = \mathcal{S}(SO_3(5^a)) = \emptyset$ for all a, so $\lambda(a) = \omega(a)$ and $\rho(a) = \sigma(a)$. Our theorem in the case $p = 5$ now follows from Theorem 4.19.

Now if $p > 5$, the irreducible characters of A_5 and S_5 in characteristic p are their irreducible complex characters, with the appropriate interpretation of the complex character values as elements of an algebraic closure of $\mathbf{F}_p$ (see [25], Chapter 15). According to [10], A_5 has two irreducible 3-dimensional complex characters, and S_5 has none. It follows immediately that if $G = SO(p^a)$ with $p > 5$ then $\mathcal{S}(G) = \emptyset$ and $\mu(1, G) = \sigma(a)$. The claim of our theorem for $G = PGL_2(p^a)$ again follows from Theorem 4.19.

We now return to the results in [14] (260) to finish our proof in the case $G = \Omega_3(p^a) = L_2(p^a)$. It is stated there that G contains two conjugacy classes of $\frac{|G|}{60}$ subgroups isomorphic to A_5 if and only if $p^a \equiv 1, 4 \bmod 5$. Thus if $p \equiv 1, 4 \bmod 5$ and $a = 1$ or if $p \equiv 2, 3 \bmod 5$ and $a = 2$, then $\mathcal{S}(G)$ contains $\frac{|G|}{30}$ subgroups isomorphic to A_5. In all other cases, $\mathcal{S}(G) = \emptyset$. Applying our theorem in the case $p = 5$ to $A_5 \cong L_2(5)$, we get

$\mu(1, A_5) = -60$, and the remaining cases of our theorem again follow from Theorem 4.19. $\square$

We can also use our results on 3-dimensional orthogonal groups, with some adjustments, to calculate $\mu(1, G)$ when $G = L_2(3^a)$ or $PGL_2(3^a)$.

Theorem 5.2 *For a positive integer a, define*

$$\lambda(a) := \frac{\mu(1, L_2(3^a))}{|L_2(3^a)|}$$

and

$$\rho(a) := \frac{\mu(1, PGL_2(3^a))}{|L_2(3^a)|}.$$

Then

$$\rho(a) = \begin{cases} -\mu(a) & a \text{ odd} \\ 0 & a \text{ even} \end{cases}$$

and

$$\lambda(a) = \begin{cases} \frac{1}{3} & a = 1 \\ 2 & a = 2 \\ \mu(a) & a > 1 \text{ odd} \\ 0 & a > 2 \text{ even.} \end{cases}$$

Proof: We first consider the case $a = 1$. It is well known that $L_2(3) \cong A_4$ and $PGL_2(3) \cong S_4$ (the natural action on 1-spaces embeds these groups in S_4 and the claim follows immediately when their orders are calculated). It is straightforward to calculate that $\mu(1, A_4) = 4$ and $\mu(1, S_4) = -12$.

For $a > 1$, we consider $\Omega_3(3^a) \cong L_2(3^a)$ and $SO_3(3^a) \cong PGL_2(3^a)$. Let G be either of these groups and let $\mathcal{I}_i(G)$ for $i = 1, 2, 5$ as in Definition 4.1. Since $a > 1$, the results in Main Lemma 3.25(3) apply, so

$$\sum_{H \in \mathcal{I}_1(G)} \mu(1, H) = \frac{|SO_3(3^a)|}{3}.$$

The results of Corollary 4.12 certainly apply, so

$$\sum_{H \in \mathcal{I}_2(G) \setminus \mathcal{I}_1(G)} \mu(1, H) = \begin{cases} |G| - \frac{|SO_3(3^a)|}{3} & G = \Omega_3(3^a), a \text{ odd} \\ -\frac{|SO_3(3^a)|}{3} & \text{otherwise.} \end{cases}$$

We now need to adjust the definition of $\mathcal{I}_5^*(G)$ which was given in Definition 4.17. In particular, we must exclude subgroups isomorphic to $\Omega_3(3)$ and $SO_3(3)$ from $\mathcal{I}_5^*(G)$, since we will see in what follows that these groups lie in $\mathcal{I}_2(G)$. First of all, note that an element of $\mathcal{C}_2(SO_3(3^a))$ is an irreducible subgroup isomorphic to S_4, and that the character associated with this embedding takes nonzero values on some elements of S_4 which are not contained in A_4, namely, the transpositions. The degrees of the complex irreducible characters of S_4 are $1, 1, 2, 3, 3$. Since S_4 contains four conjugacy classes of 3-regular elements, it has four irreducible characters in characteristic three (see [25], Chapter 15). We know that at least one of these has degree three, and since this character χ takes nonzero values on the transpositions, the tensor product of χ with the alternating character is another irreducible 3-dimensional character in characteristic three. Thus, the degrees of the irreducible characters of S_4 in characteristic three are $1, 1, 3, 3$. Now since the two 3-dimensional characters are obtained from each other by taking the tensor product with the alternating character, only one of them can be the character of an embedding of S_4 in $SO_3(3^a)$. Thus, the subfield subgroups isomorphic to S_4 are members of $\mathcal{I}_2(PGL_3(3^a))$. A similar but easier argument can be applied to A_4, since that group has a unique irreducible 3-dimensional character in characteristic three. If we let $\mathcal{I}_5^*(G)$ be the set of almost simple subfield subgroups of G, then as in Lemma 4.18, every subgroup of G which is not contained in $\mathcal{I}_1(G) \cup \mathcal{I}_2(G)$ is either contained in $\mathcal{I}_5^*(G)$ or is an element of $\mathcal{S}(H)$ for some $H \in \mathcal{I}_5^*(G)$.

Using [14], (260) and the arguments given in the proof of Theorem 5.1, we see that any subgroup of the second type described in the previous sentence is one of $\frac{|\Omega_3(3^a)|}{30}$ subgroups isomorphic to A_5 and exists in $SO_3(3^a)$ if and only if a is even. Let $D''(a)$ be the set of nontrivial proper divisors of a. Then for each $b \in D''(a)$, $\mathcal{I}_5^*(SO_3(3^a))$ contains one conjugacy class of $\frac{|SO_3(3^a)|}{|SO_3(3^b)|}$ subgroups isomorphic to $SO_3(3^b)$ and one class of the same number of subgroups isomorphic to $\Omega_3(3^b)$. By Lemma 4.13, the subgroups isomorphic to $SO_3(3^b)$ are contained in $\Omega_3(3^a)$ if and only if $\frac{a}{b}$ is even.

Let $D_1(a)$ be the set of divisors of a besides one and set

$$D^e(a) = \left\{ b \in D_1(a) : \frac{a}{b} \text{ is even} \right\}.$$

By the above arguments, we have

$$\lambda(a) = \begin{cases} -(-2 + \sum_{b \in D^e(a)} \rho(b) + \sum_{b \in D''(a)} \lambda(b)) & a \text{ even} \\ -(1 + \sum_{b \in D''(a)} \lambda(b)) & a \text{ odd} \end{cases}$$

and

$$\rho(a) = \begin{cases} -(-2 + \sum_{b \in D''(a)} \rho(b) + \sum_{b \in D_1(a)} \lambda(b)) & a \text{ even} \\ -(\sum_{b \in D''(a)} \rho(b) + \sum_{b \in D_1(a)} \lambda(b)) & a \text{ odd.} \end{cases}$$

The theorem now follows by multiplicative induction on a. If a is an odd prime then $\lambda(a) = -1$ and $\rho(a) = 1$ by inspection. Now by inductive hypothesis, when a is odd and composite, $\lambda(a) = -(\mu(1) + \sum_{b \in D''(a)} \mu(b)) = \mu(a)$, and $\rho(a) = -\lambda(a)$ since $\lambda(b) = -\rho(b)$ for all $b \in D''(a)$. Also, $\lambda(2) = 2$ and $\rho(2) = 0$ by inspection. If $a > 2$ is even, then by inductive hypothesis we have $\rho(a) = \lambda(a) = -(-2 + \lambda(2)) = 0$. □

The remainder of this section will be devoted to finding the Möbius numbers of certain extensions of two dimensional linear groups by field automorphisms of order two. These results will be used in the determination of the Möbius numbers of certain symmetric groups.

Lemma 5.3 *Let p be prime with $p \equiv 1, 4 \bmod 5$. Let $L = L_2(p^2)$ and let f be the automorphism of L induced by the automorphism $f^* : \alpha \mapsto \alpha^p$ of $\mathbf{F}_{p^2}$. Let $\mathcal{L}$ be the lattice of subgroups of L and let $\mathcal{L}^f$ be the lattice of subgroups of L which are normalized by f. Let $\mathbf{P}$ be the natural projective space for L. Let f' be the involution on the 1-spaces in $\mathbf{P}$ determined by f^*. If M is a coatom of $\mathcal{L}^f$ then one of the following holds.*

(1) M is the stabilizer in L of a 1-space from $\mathbf{P}$ which is also stabilized by f'.

(2) M is the stabilizer in L of a set of two 1-spaces from $\mathbf{P}$ *which is stabilized by* f'.

(3) $M = C_L(f)$.

(4) $M \cong PGL_2(p)$ *and* $M \neq C_L(f)$.

(5) $M \cong S_4$ *and* $M \not\leq C_L(f)$.

(6) $M \cong A_5$ *and* $M \not\leq C_L(f)$.

Furthermore, any element of $\mathcal{L}^f$ *which is not contained in one of the subgroups described in (1), (2) and (3) above is a subgroup of index at most two in one of the subgroups described in (4), (5) and (6).*

Proof: First note that f certainly normalizes the groups described in (1), (2) and (3). Let $H \in \mathcal{L}^f$. First suppose H is reducible, so H stabilizes some 1-space X from $\mathbf{P}$. Then since f' acts on the set F_H of 1-spaces stabilized by H, H also stabilizes $X^{f'}$. If $X^{f'} = X$ then H is contained in a subgroup described in (1), while if $X^{f'} \neq X$ then H is contained in a subgroup described in (2).

Next assume that $H \in \mathcal{L}^f$ is irreducible but imprimitive, so H stabilizes a set $S = \{X, Y\}$ of 1-spaces from $\mathbf{P}$. Now if H fixes only S, then f normalizes $stab_L(S)$, which contains H, so assume that H stabilizes more than one 2-set. Since $p^2 \equiv 1 \bmod 4$, the stabilizer M of $\{X, Y\}$ in L is dihedral of order $p^2 - 1$ and is the centralizer of an involution in L. Furthermore, the stabilizer in L of any 2-set from $\mathbf{P}$ is conjugate to M in L and intersects L in a group of order $1, 2$ or 4, the groups of order four being noncyclic (see [14], Chapter XII). Note that since $p^2 \equiv 1 \bmod 4$, every involution in L fixes a 1-space from $\mathbf{P}$. Since H is irreducible and H fixes more than one 2-set we have $|H| = 4$ and H centralizes exactly three involutions. Thus H fixes exactly three 2-sets, and f' permutes these three sets. Now f' must fix one of these 2-sets, and f normalizes the stabilizer of this set, which contains H. Now by [14], (260), any subgroup of L which is neither reducible nor imprimitive either is of index at most two in a subgroup isomorphic to one of S_4, $PGL_2(p)$ or A_5, or contains a normal cyclic irreducible subgroup. If H contains a normal cyclic irreducible subgroup K, then by [14], (260) H is cyclic or dihedral and there is a unique Coxeter torus $C \leq L$ such that $K \leq C$. Thus it remains to show that f does not normalize any Coxeter torus of L. Let $\overline{L} = L_2(\overline{\mathbf{F}}_p)$, where $\overline{\mathbf{F}}_p$ is the algebraic closure of $\mathbf{F}_p$. Then we may assume that f is an automorphism of $\overline{L}$ and that L is a subgroup of index two in $C_{\overline{L}}(f^2)$ (see [43],I,2.1). It is straightforward to show that if C is a Coxeter torus of L which is normalized by f then C is contained in a unique maximal torus $\overline{T}$ of $\overline{L}$. Thus f normalizes $\overline{T}$, and $\overline{T}$ intersects $C_{\overline{L}}(f)$ in a cyclic group of order $p+1$ or $p-1$ (see for example [9], p.21). Now by [14], (260), C is a self-centralizing subgroup of L of order $\frac{p^2+1}{2}$. Since $\overline{T} \cap C_{\overline{L}}(f) \leq C_L(C)$, one of $p+1$ or $p-1$ divides p^2+1, which is impossible since $p \neq 3$. Thus we have a contradiction to the fact that $\overline{T}$ centralizes C. □

Theorem 5.4 *Let p be prime with $p \equiv 1, 4 \bmod 5$. Let $L = L_2(p^2)$ and let f be the automorphism of L induced by the automorphism $f^* : \alpha \mapsto \alpha^p$ of $\mathbf{F}_{p^2}$. Let G be the semidirect product $\langle f \rangle L$. Then $\mu(1, G) = 0$.*

Proof: Let $\overline{L}$ be as above, and let $K = C_{\overline{L}}(f^2)$, so $K \cong PGL_2(p^2)$ and $[K : L] = 2$. Let c generate a complement to L in G. Then $c = fx$ for some $x \in L$ with $x^f = x^{-1}$. By Lang's Theorem (see [43],I,2.2), there is some $y \in \overline{L}$ such that $x = y^f y^{-1}$, so $c = yfy^{-1}$. Now $y^f = xy$, so

$$y^{(f^2)} = (xy)^f = x^{-1} y^f = yy^{-f} y^f = y,$$

and so $y \in K$. Thus every complement to L in G is conjugate to f in $\langle f \rangle K$, which normalizes G. Let X be the number of K-conjugates of f in G. Then by Theorem 2.4,

$$\mu(1, G) = -X \mu(\langle f \rangle, G).$$

Let μ_f be the Möbius function on the lattice $\mathcal{L}^f$ of subgroups of G normalized by f. The map $H \mapsto H \cap L$ is an isomorphism of the interval $[\langle f \rangle, G]$ in the subgroup lattice of G with $\mathcal{L}^f$. Thus it is sufficient to show that $\mu_f(1, L) = 0$.

Let $\mathcal{M}$ be the set of coatoms in $\mathcal{L}^f$ described in (1), (2) and (3) of Lemma 5.3, and let $\mathcal{I}$ be the ideal in $\mathcal{L}^f$ generated by $\mathcal{M}$. Let $\mathcal{R}$ be the collection of subsets S of $\mathcal{M}$ satisfying $\bigcap_{M \in S} M \neq 1$. By Theorem 2.6 we have

$$\sum_{H \in \mathcal{I}} \mu_f(1, H) = \sum_{S \in \mathcal{R}} (-1)^{|S|}.$$

Let $P = C_L(f)$. We will show that this alternating sum is zero by showing that if $S \in \mathcal{R}$ with $P \notin S$ then $S \cup \{P\} \in \mathcal{R}$.

Define f' and $\mathbf{P}$ as in Lemma 5.3. Let W be a 1-space from $\mathbf{P}$. Then W is fixed by f' if and only if W contains the vector $[0\,1]$ or a vector $[1\,\alpha]$ with $\alpha \in \mathbf{F}_p$. Note that P acts 2-transitively on the set Γ of these 1-spaces. If $S \in \mathcal{R}$, then S contains at most two elements of the form $stab_L(W)$ with $W \in \Gamma$. On the other hand, if $S = \{stab_L(W_1), stab_L(W_2)\}$ contains exactly two of these elements, we may assume by 2-transitivity that $[1\,0] \in W_1$ and $[0\,1] \in W_2$. Let $L_i = stab_L(W_i)$. The preimage of $L_1 \cap L_2$ in $SL_2(p^2)$ consists of the diagonal matrices. Certainly $L_1 \cap L_2 \cap P \neq 1$, so $\{L_1, L_2, P\} \in \mathcal{R}$. Also, if $S \in \mathcal{R}$ consists of one subgroup of the form $stab_L(W)$ then $S \cup \{P\} \in \mathcal{R}$.

If $D \in \mathcal{L}^f$ is of the type described in (2) of Lemma 5.3, then D is dihedral of order $p^2 - 1$. Since $p^2 \equiv 1 \bmod 4$, $|Z(D)| = 2$. Since $Z(D)$ is characteristic in D, $Z(D) \in \mathcal{L}^f$ and $Z(D) \leq P$. Therefore, $\{D, P\} \in \mathcal{R}$. We saw in the proof of Lemma 5.3 that the intersection of D with any of its conjugates has order one, two or four. Thus if $S \in \mathcal{R}$ contains D and one of its conjugates, $H = \bigcap_{M \in S} M$ has order two or four. Certainly $H \cap P \neq 1$ in this case.

It remains to examine those $S \in \mathcal{R}$ which contain D and either one or two groups described in (1). Let S be such a collection and set $H = \bigcap_{M \in S} M$. If $|H|$ is even then any automorphism of H of order two has a fixed point, so $H \cap P \neq 1$. Now assume for contradiction that $|H|$ is odd. Since $H \leq D$ and H is not dihedral, H is cyclic. Since $H \neq 1$, H fixes at most two 1-spaces from $\mathbf{P}$. However, the intersection of D with the stabilizers of these two 1-spaces has index two in D, and since $|D|$ is divisible by four, $|K|$ is even. This gives the desired contradiction.

All possibilities for $S \in \mathcal{R}$ with $P \notin S$ have been considered, so we have shown that

$$\sum_{S \in \mathcal{R}} (-1)^{|S|} = 0.$$

It remains to consider the subgroups of index one or two in elements of $\mathcal{L}^f$ described in (4), (5) and (6) of Lemma 5.3. Let $H \in \mathcal{L}^f$ with $H \cong PGL_2(p)$ and $H \neq P$. Then the subgroup J of index two in H isomorphic to $L_2(p)$ is characteristic in H and thus also contained in $\mathcal{L}^f$. Conversely, for any $J \in \mathcal{L}^f$ isomorphic to $L_2(p)$, $N_L(J) \cong PGL_2(p)$ is a subgroup described in (4). Let $J < H$ be a pair as described above. By [14], (260), H is conjugate to P in K, so $N_G(H) \cong N_G(P) \cong Z_2 \times PGL_2(p)$. Thus f must act on H as a nontrivial inner automorphism. Let t be an involution in H which acts like f on H, and let $\mathcal{H}$ be the lattice of subgroups of H in $\mathcal{L}^f$. Then t normalizes every element of $\mathcal{H}$. Note that J is simple and is therefore the only subgroup of index two in H. If $t \in J$ then for every $R < H$ with $R \in \mathcal{H}$, $\langle t, R\rangle$ is a proper subgroup of H contained in $\mathcal{H}$. Furthermore, if $R < J$ then $\langle t, R\rangle < J$. Thus every coatom of $\mathcal{H}$ contains $\langle t\rangle$, as does every coatom of the lattice of subgroups of J normalized by f. It now follows from Theorem 2.6 then $\mu_f(1, H) = \mu_f(1, J) = 0$. It $t \in H \setminus J$ then J is the unique complement to $\langle t\rangle$ in $\mathcal{H}$. By Theorem 2.4, $\mu_f(1, H) = -\mu_f(1, J)$. Thus the sum of $\mu_f(1, R)$ over all subgroups R of index one or two in groups described in (4) is zero.

A similar argument to the one in the previous paragraph shows that elements of $\mathcal{L}^f$ which are subgroups of index one or two in the groups described in (5) of Lemma 5.3 come in pairs $J < H$ with $J \cong A_4$ and $H \cong S_4$. All subgroups of L isomorphic to S_4 are conjugate in K. Since P contains a subgroup isomorphic to S_4, if $H \in \mathcal{L}^f$ with $H \cong S_4$ and $H \not\leq P$, then $\langle f\rangle H \cong Z_2 \times S_4$. Thus f acts on H as conjugation by an involution $t \in H$, and J is the unique subgroup of index two in H. As in the previous paragraph we have $\mu_f(1, H) + \mu_f(1, J) = 0$.

Finally, let $H \in \mathcal{L}^f$ with $H \cong A_5$ and $H \not\leq P$. Since $p \equiv 1, 4 \bmod 5$, P contains a subgroup isomorphic to A_5. We have shown in the proof of Theorem 5.1 that K contains no subgroup isomorphic to S_5. Thus the $\frac{|L|}{30}$ subgroups of L isomorphic to A_5 are all conjugate in K, so $\langle f \rangle H \cong Z_2 \times A_5$ and f acts on H as conjugation by some involution $t \in H$. Now arguing as we did for $H \cong L_2(p)$, we see that every coatom in the lattice of subgroups of H which are fixed by f contains t. It follows from Theorem 2.6 that $\mu_f(1, H) = 0$.

We have considered all proper subgroups of L contained in $\mathcal{L}^f$ and shown that the sum of $\mu_f(1, R)$ over all of these subgroups is zero, so the proof of the theorem is complete. $\square$

Chapter 6

The Möbius numbers of three dimensional linear and unitary groups in odd characteristic

In this chapter we will determine $\mu(1, G)$ when G is one of $L_3(q)$, $PGL_3(q)$, $U_3(q)$ or $PGU_3(q)$ with q odd. We will use some conventions that were defined previously. In particular, let V be a 3-dimensional vector space over $\mathbf{F}_q$ with q odd. If q is a square, let f be a nondegenerate hermitian form on V. We will have to examine the following six cases separately.

Case (L1): $3 \not| q-1$ and $G = L(V) = PGL(V)$.

Case (L2): $3|q-1$ and $G = PGL(V)$.

Case (L3): $3|q-1$ and $G = L(V)$.

Case (U1): $3 \not| \sqrt{q}+1$ and $G = U(V,f) = PGU(V,f)$.

Case (U2): $3|\sqrt{q}+1$ and $G = PGU(V,f)$.

Case (U3): $3|\sqrt{q}+1$ and $G = U(V,f)$.

From now on, we will assume in cases (U1)-(U3) that f has been fixed, and write $PGU(V)$ and $U(V)$ for $PGU(V,f)$ and $U(V,f)$, respectively.

Our first step is to describe the maximal subgroups of G, where G is described as above. We will use the notation from [3] and [28], although the results below are found in [34]. Recall that we have already defined $\mathcal{I}_1(G)$ to be the ideal of reducible subgroups of G, and that we have defined the conjugacy classes of Coxeter tori of $PGL(V)$ and $PGU(V)$ in Definition 3.19.

Definition 6.1 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ with q odd.*

(1) $\mathcal{F}$ is the set of frames from V, so an element of $\mathcal{F}$ is a set $F = \{X_1, X_2, X_3\}$ of 1-spaces from V with $V = \oplus_{i=1}^{3} X_i$.

(2) If $F = \{X_1, X_2, X_3\} \in \mathcal{F}$ then M_F is the stabilizer of F in $PGL(V)$.

(3) For $G = L(V)$ or $PGL(V)$, $\mathcal{C}_2(G) := \{M_F \cap G : F \in \mathcal{F}\}$.

(4) $\mathcal{CX}$ is the set of Coxeter tori of $PGL(V)$.

(5) For $G = L(V)$ or $PGL(V)$, $\mathcal{C}_3(G) := \{N_G(C) : C \in \mathcal{CX}\}$.

(6) $\mathcal{SF}$ is the set of proper subfields of $\mathbf{F}_q$ and $\mathcal{MSF}$ is the set of maximal subfields of $\mathbf{F}_q$. For $\mathbf{F}_* \in \mathcal{SF}$, $L(\mathbf{F}_*)$ is the set of additive subgroups of V which are 3-dimensional $\mathbf{F}_*$-subspaces of V and whose $\mathbf{F}_q$-span is V.

(7) For $G = L(V)$ or $PGL(V)$, $\mathcal{C}_5(G)$ is the set of all subgroups of the form $stab_G(V_*)$, where $V_* \in L(\mathbf{F}_*)$ and $\mathbf{F}_* \in \mathcal{MSF}$.

(8) $\mathcal{ES}$ is the set of subgroups of $GL(V)$ which are nonabelian of exponent three and order 27 and which act absolutely irreducibly on V. For $E \in \mathcal{ES}$, $\overline{E}$ is, as usual, the image of E in $PGL(V)$.

(9) For $G = L(V)$ or $PGL(V)$, $\mathcal{C}_6(G) := \left\{N_G(\overline{E}) : E \in \mathcal{ES}\right\}$.

(10) $\mathcal{SY}$ is the set of nondegenerate symmetric forms on V and if q is a square then $\mathcal{HE}$ is the set of nondegenerate hermitian forms on V.

(11) For $G = L(V)$ or $PGL(V)$, $\mathcal{C}_8(G) := \{stab_G(f) : f \in \mathcal{SY} \cup \mathcal{HE}\}$.

(12) I is the index set $\{1, 2, 3, 5, 6, 8\}$ and $J = I \setminus \{5, 8\}$.

(13) For $G = L(V)$ or $PGL(V)$ and $j \in I$, $\mathcal{I}_j(G)$ is the ideal in the subgroup lattice of G generated by the elements of $\mathcal{C}_j(G)$.

(14) For $G = L(V)$ or $PGL(V)$, $\mathcal{I}^*_{58}(G)$ is the set of all subgroups of G of the form $L(V_*)$, $PGL(V_*)$, $SO(V_*, f)$, $\Omega(V_*, f)$, $U(V_*, f)$ or $PGU(V_*, f)$, where $V_* \in L(\mathbf{F}_*)$ for some $\mathbf{F}_* \in \mathcal{SF}$ and f is a nondegenerate $\mathbf{F}_*$-symmetric or $\mathbf{F}_*$-hermitian form on V_*.

(15) For $G = L(V)$ or $PGL(V)$, $\mathcal{S}^*(G)$ is the set of subgroups of G which are not contained in $(\bigcup_{j \in J} \mathcal{I}_j(G)) \bigcup \mathcal{I}^*_{58}(G)$ and do not contain $L(V)$.

The lemma given below is essentially due to Mitchell.

Lemma 6.2 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ with $q = p^a$ odd. If $G = L(V)$ or $PGL(V)$ then $H \in \mathcal{S}^*(G)$ if and only if H is one of the groups described on the list below, and p and a satisfy the given conditions.*

(1) If a is even and $p \neq 7$ or if $p \equiv 1, 2, 4 \bmod 7$ then $\mathcal{S}^*(G)$ contains one $PGL(V)$-conjugacy class of $\frac{|PGL(V)|}{168}$ subgroups isomorphic to $L_2(7)$.

(2) If a is even and $p \neq 3, 5$, or if $p \equiv 1, 4 \bmod 15$ then $\mathcal{S}^*(G)$ contains one $PGL(V)$-conjugacy class of $\frac{|PGL(V)|}{360}$ subgroups isomorphic to A_6.

(3) If a is even and $p = 5$ then $\mathcal{S}^*(G)$ contains one $PGL(V)$-conjugacy class of $\frac{|PGL(V)|}{720}$ subgroups isomorphic to M_{10}, one $PGL(V)$-conjugacy class of $\frac{|PGL(V)|}{720}$ subgroups isomorphic to A_6 and one $PGL(V)$-conjugacy class of $\frac{|PGL(V)|}{2520}$ subgroups isomorphic to A_7.

(4) If a is even and $p \neq 5$ or if $p \equiv 1, 4 \bmod 5$ then $\mathcal{S}^*(G)$ contains one $PGL(V)$-conjugacy class of $\frac{|PGL(V)|}{60}$ subgroups isomorphic to A_5.

Proof: The orders of the elements of $\mathcal{S}^*(G)$, along with some of the isomorphism types, are given in [34], with the exception of the subgroups isomorphic to A_5. These subgroups are not explicitly listed therein because they are contained in the previously mentioned orthogonal subgroups (in the language of [34], these subgroups stabilize a conic). The remaining information is verified in [10] and [27]. □

Definition 6.3 *Let V be a 3-dimensional unitary space over $\mathbf{F}_{q^2}$, with Hermitian form f, where q is odd.*

(1) $\mathcal{UF}$ is the set of unitary frames from V, so an element of $\mathcal{UF}$ is a set $F = \{X_1, X_2, X_3\}$ of 1-spaces from V with $V = \perp_{i=1}^{3} V_i$.

(2) If $F \in \mathcal{UF}$ then M_F is the stabilizer of F in $PGU(V)$.

(3) For $G = U(V)$ or $PGU(V)$, $\mathcal{C}_2(G) := \{M_F \cap G : F \in \mathcal{UF}\}$.

(4) $\mathcal{UCX}$ is the set of Coxeter tori of $PGU(V)$.

(5) For $G = U(V)$ or $PGU(V)$, $\mathcal{C}_3(G) := \{N_G(C) : C \in \mathcal{UCX}\}$.

(6) $\mathcal{SF}$ and $\mathcal{MSF}$ are the sets of subfields and maximal subfields of $\mathbf{F}_{q^2}$, respectively, as defined above. If $\mathbf{F}_* \in \mathcal{SF}$ is of odd index in $\mathbf{F}_{q^2}$, $U(\mathbf{F}_*)$ is the set of all $W \in L(\mathbf{F}_*)$ such that $f_{|W}$ is a nondegenerate $\mathbf{F}_*$-hermitian form. If $\mathbf{F}_*$ is of even index in $\mathbf{F}_{q^2}$ then

$U(\mathbf{F}_*)$ is the set of all $W \in L(\mathbf{F}_*)$ such that $f_{|W}$ is a nondegenerate $\mathbf{F}_*$-symmetric form.

(7) For $G = U(V)$ or $PGU(V)$, $\mathcal{C}_5(G)$ is the set of all subgroups of the form $stab_G(V_*, f_{|V_*})$, where $V_* \in U(\mathbf{F}_*)$ for some $\mathbf{F}_* \in \mathcal{MSF}$.

(8) $\mathcal{ES}$ is the set of subgroups of $GU(V)$ which are nonabelian of exponent three and order 27 and which act absolutely irreducibly on V.

(9) For $G = U(V)$ or $PGU(V)$, $\mathcal{C}_6(G) := \left\{N_G(\overline{E}) : E \in \mathcal{ES}\right\}$.

(10) I is the index set $\{1, 2, 3, 5, 6\}$ and $J = I \setminus \{5\}$.

(11) For $G = U(V)$ or $PGU(V)$, $\mathcal{I}_5^*(G)$ is the set of all subgroups of G of the form $PSO(V_*, f_{|V_*})$, $\Omega(V_*, f_{|V_*})$, $U(V_*, f_{|V_*})$ or $PGU(V_*, f_{|V_*})$, where $V_* \in U(\mathbf{F}_*)$ for some $\mathbf{F}_* \in \mathcal{SF}$.

(12) For $G = U(V)$ or $PGU(V)$ and $j \in I$, $\mathcal{I}_j(G)$ is the ideal in the subgroup lattice of G generated by $\mathcal{C}_j(G)$. Also, $\mathcal{S}^*(G)$ is the set of subgroups not contained in $(\cup_{j \in J}\mathcal{I}_j(G)) \cup \mathcal{I}_5^*(G)$ and not containing $U(V)$.

As above, the following lemma is essentially due to Mitchell.

Lemma 6.4 *Let V be a 3-dimensional unitary space over $\mathbf{F}_{q^2}$ with $q = p^a$ odd. If $G = U(V)$ or $PGU(V)$ then $H \in \mathcal{S}^*(G)$ if and only if H is one of the groups described on the list below, and p and a satisfy the given conditions.*

(1) If a is odd and $p \equiv 3, 5, 6 \bmod 7$ then $\mathcal{S}^*(G)$ contains one $PGU(V)$-conjugacy class of $\frac{|PGU(V)|}{168}$ subgroups isomorphic to $L_2(7)$.

(2) If a is odd and $p \equiv 11, 14 \bmod 15$ then $\mathcal{S}^*(G)$ contains one $PGU(V)$-conjugacy class of $\frac{|PGU(V)|}{360}$ subgroups isomorphic to A_6.

(3) If a is odd and $p = 5$ then $\mathcal{S}^*(G)$ contains one $PGU(V)$-conjugacy class of $\frac{|PGU(V)|}{720}$ subgroups isomorphic to M_{10}, one $PGU(V)$-conjugacy class of $\frac{|PGU(V)|}{720}$ subgroups isomorphic to A_6 and one $PGU(V)$-conjugacy class of $\frac{|PGU(V)|}{2520}$ subgroups isomorphic to A_7.

(4) If a is even and $p \neq 5$ or if $p \equiv 1, 4 \bmod 5$ then $\mathcal{S}^*(G)$ contains one $PGU(V)$-conjugacy class of $\frac{|PGU(V)|}{60}$ subgroups isomorphic to A_5.

Proof: As above, the necessary results are contained in [34],[10] and [27]. □

We will proceed as we did in the determination of the formula for the Möbius numbers of the orthogonal groups in prime dimension. That is, the sum of the Möbius numbers of the proper subgroups of G which are not in $\mathcal{C}_5(G)$ will be determined for all values of $q = p^a$, and then for a fixed prime p, induction on a will be employed. The difference here will be that the members of $\mathcal{S}^*(G)$ are known, so the calculation can be completed. We begin by restating results from Chapter 3 in the appropriate form.

Lemma 6.5 *(1) Let V be a 3-dimensional linear space over $\mathbf{F}_q$ with q odd, and let $G = L(V)$ or $PGL(V)$. Let C be a Coxeter torus of $PGL(V)$ and set $N = N_G(C)$. Then*

$$\sum_{H \in \mathcal{I}_1(G)} \mu(1, H) = [G : N]$$

(2) Let V be a nondegenerate 3-dimensional unitary space over $\mathbf{F}_{q^2}$ with q odd, and let $G = U(V)$ or $PGU(V)$. Let C be a Coxeter torus of $PGU(V)$ and set $N = N_G(C)$. Then

$$\sum_{H \in \mathcal{I}_1(G)} \mu(1, H) = [G : N]$$

Proof: This follows immediately from Theorems 3.22 and 3.23. □

The next step is to examine $\mathcal{I}_2(G) \setminus \mathcal{I}_1(G)$. We recall some previous definitions.

Definition 6.6 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ with q odd. If q is a square, let f be a nondegenerate Hermitian form on V.*

(1) $\mathcal{T}$ is a transversal to $(\mathbf{F}_q^*)^3$ in $\mathbf{F}_q$ containing 1, so $\mathcal{T} = \{1, t_2, t_3\}$ if $3|q-1$ and $\mathcal{T} = \{1\}$ otherwise. If q is a square and $3|\sqrt{q}+1$ then $t^{\sqrt{q}+1} = 1$ for all $t \in \mathcal{T}$.

(2) For each $g \in PGL(V)$, g^* is an element of $GL(V)$ which maps to g under the natural projection and satisfies $det(g^*) \in \mathcal{T}$.

(3) Fix a basis e_1, e_2, e_3 for V such that if q is a square, the given basis is orthonormal with respect to f. For each $t_i \in \mathcal{T}$, p_i is the element of $GL(V)$ satisfying $e_1 p_i = e_2, e_2 p_i = e_3$ and $e_3 p_i = t_i e_1$. Also, g_i is the element of $PGL(V)$ such that $g_i^* = p_i$.

Lemma 6.7 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ with q odd and let $F = \{X_1, X_2, X_3\} \in \mathcal{F}$. Let T be the kernel of the permutation action of $M = M_F$ on F and set $\tilde{M} = M/T$. Let $H \leq M$. Then $H \notin \mathcal{I}_1(PGL(V))$ if and only if one of the following conditions holds.*

(1) $3|q-1$ and H contains an M- conjugate of g_2.

(2) 3 divides $|\tilde{H}|$ and $H \cap T \neq 1$.

Proof: We may assume that $e_i \in X_i$ for each i, where e_1, e_2, e_3 is the basis described in Definition 6.6. First note that M is the split extension of T by the group S which contains the image in $PGL(V)$ of the elements of $GL(V)$ which are permutation matrices with respect to our basis. Now if 3 does not divide $|\tilde{H}|$ then H is not transitive on the X_i and it follows immediately that $H \in \mathcal{I}_1(PGL(V))$. Note that 3 divides $|\tilde{H}|$ if and only if there exists some $h \in H$ such that $X_1 h = X_2, X_2 h = X_3$ and $X_3 h = X_1$. Such an h is conjugate to some p_i by an element of T whose preimage in $GL(V)$ scales the e_i appropriately. Note that if h is conjugate to g_3 in M then h^2 is conjugate to g_2 in M. If $3|q-1$ then t_2 is not a cube in $\mathbf{F}_q$, and it follows immediately that p_2 acts irreducibly on V, so that any group containing g_2 is not contained in $\mathcal{I}_1(PGL(V))$. It is now sufficient to show that a subgroup of M which contains g_1 is reducible if and only if it intersects T trivially. If $g_1 \in H \leq M$ and $H \cap T = 1$ then $|H| = 3$ or 6, so $\langle g_1 \rangle \lhd H$. Thus $K = \langle p_1, Z \rangle \lhd H^*$. Assume for contradiction that H is irreducible. Then by Clifford's Theorem (see [25], p. 79) and the fact that $[H^* : K] \leq 2$, K has at most two homogeneous constituents on V. However, Z stabilizes every subspace of V and p_1 has three distinct eigenvalues, giving the desired contradiction. If some nontrivial $g \in T$ fixes the 1-space generated by $v = ae_1 + be_2 + ce_3$ then $0 \in \{a, b, c\}$, so $\mathbf{F}_q v$ is not fixed by g_1. It remains to show that no 2-space from V is fixed by both g_1 and some nontrivial $g \in T$. Assume for contradiction that W is such a 2-space, and let H^* be the preimage of $stab_M(W)$ in $GL(V)$. Let $J^* = \{{}^t h^{-1} : h \in H^*\}$. Then J^* stabilizes some 1-space from V, and the image of J^* in $PGL(V)$ contains g_1 and intersects T nontrivially, contradicting the result just obtained. □

Corollary 6.8 *Let V be a 3-dimensional linear or nondegenerate unitary space over $\mathbf{F}_q$ with q odd. If V is a linear space let $F = \{X_1, X_2, X_3\} \in \mathcal{F}$, and if V is a unitary space assume $F \in \mathcal{UF}$. If G is one of $L(V)$, $PGL(V)$, $U(V)$ or $PGU(V)$, set $M = M_F \cap G$. Let $\mathcal{I}_{2,1}(M) = \{H \leq M : H \notin \mathcal{I}_1(G)\}$. Then*

$$\sum_{H \in \mathcal{I}_{2,1}(M)} \mu(1, H) = \begin{cases} -2(q-1)^2 & \text{in case (L1)} \\ -\frac{8}{3}(q-1)^2 & \text{in cases (L2) and (L3)} \\ -2(\sqrt{q}+1)^2 & \text{in case (U1)} \\ -\frac{8}{3}(\sqrt{q}+1)^2 & \text{in cases (U2) and (U3).} \end{cases}$$

Proof: We may assume that $e_i \in X_i$ for each i. Let T be the kernel of the action of M on the X_i and set $\tilde{M} = M/T$. Note that T is the image in $PGL(V)$ or $PGU(V)$ of the diagonal subgroup of $SL(V), GL(V), SU(V)$ or $GU(V)$ with respect to the basis

e_1, e_2, e_3, so that

$$|T| = \begin{cases} (q-1)^2 & \text{in cases (L1) and (L2)} \\ \frac{(q-1)^2}{3} & \text{in case (L3)} \\ (\sqrt{q}+1)^2 & \text{in cases (U1) and (U2)} \\ \frac{(\sqrt{q}+1)^2}{3} & \text{in case (U3).} \end{cases}$$

Define a closure $\hat{}$ on the lattice of subgroups of M by $\hat{H} = HT$. Note that 3 divides $|\tilde{H}|$ if and only if $\hat{H} = \langle g_1, T\rangle$ or M. Also, since $\hat{1} = T \neq 1$, $\sum_{\hat{H}=K} \mu(1, H) = 0$ for any $K \leq M$ by Theorem 2.3. It follows that

$$\sum_{3 \mid |\tilde{H}|} \mu(1, H) = 0.$$

Now let $P_1(M)$ be the set of subgroups of M which contain a $PGL(V)$-conjugate of g_1 and intersect T trivially. By Lemma 6.7, we have

$$\sum_{H \in \mathcal{I}_{2,1}(M)} \mu(1, H) = -\sum_{H \in P_1(M)} \mu(1, H).$$

In cases (L1) and (U1), g_1 generates a Sylow 3-subgroup of M, and any element of $N_M(\langle g_1\rangle) \cap T$ centralizes g_1. If $g \in T$ is such an element, then g fixes the unique eigenspace of g_1, which is generated by $e_1 + e_2 + e_3$. It follows that $g = 1$. It now follows from a Frattini argument (see [2], p.20) applied to $\langle g_1\rangle \in Syl_3(\langle g_1, T\rangle)$ that $N_M(\langle g_1\rangle) \cong S_3$, and there are $\frac{|M|}{6} = |T|$ $PGL(V)$-conjugates of $\langle g_1\rangle$ in M. For each of these conjugates, there exists one element of $P_1(M)$ isomorphic to Z_3 and one isomorphic to S_3. Since $\mu(1, Z_3) = -1$ and $\mu(1, S_3) = 3$, in these cases we have

$$\sum_{H \in \mathcal{I}_{2,1}(M)} \mu(1, H) = -2|T|,$$

and the lemma is correct in these cases.

Now assume that one of cases (L2), (L3), (U2) or (U3) holds and let ω be a primitive cube root of 1 in $\mathbf{F}_q$. If $g \in C_T(g_1)$ then g permutes the three eigenspaces of g_1, which are described in the proof of Lemma 6.7. Any nontrivial element of T permuting the 1-spaces must permute them cyclically. It follows that if $e_1 g^* = e_1, e_2 g^* = \omega e_2$ and

$e_3 g^* = \omega^2 e_3$ then $C_T(g_1) = \langle g \rangle$. If $s \in N_M(\langle g_1 \rangle)$ is as above, then $N_M(\langle g_1 \rangle) = \langle g_1, s, g \rangle$ is isomorphic to an extension of an elementary abelian group of order nine by an involution which inverts every element of this kernel. The subgroups of $N_M(\langle g_1 \rangle)$ which contain g_1 and intersect T trivially are $\langle g_1 \rangle$ and three subgroups isomorphic to S_3. Note that $N_M(\langle g_1 \rangle) \leq U(V)$. Thus if a is the number of $PGL(V)$-conjugates of $\langle g_1 \rangle$ in M which are not contained in T,

$$\sum_{H \in \mathcal{I}_{2,1}(M)} \mu(1, H) = -8a.$$

If $G = PGL(V)$ or $PGU(V)$ then every $PGL(V)$-conjugate of g_1 in $M \setminus T$ is conjugate to either g_1 or g_1^2 by an element of T, so all $PGL(V)$-conjugates of $\langle g_1 \rangle$ which are not contained in T are already conjugate in M. It follows that

$$a = \begin{cases} \frac{6(q-1)^2}{18} & \text{in cases (L2) and (L3)} \\ \frac{6(\sqrt{q}+1)^2}{18} & \text{in cases (U2) and (U3)} \end{cases}$$

The proof is now complete. □

Lemma 6.9 *Let V be a 3-dimensional linear or nondegenerate unitary space over $\mathbf{F}_q$ with q odd. If V is a linear space let $F = \{X_1, X_2, X_3\} \in \mathcal{F}$, and if V is a unitary space assume $F \in \mathcal{UF}$. If G is one of $L(V)$, $PGL(V)$, $U(V)$ or $PGU(V)$, set $M = M_F \cap G$. Let $H \leq M$ be irreducible. If H stabilizes another element of $\mathcal{F}$ in the linear case or H stabilizes another element of $\mathcal{UF}$ in the unitary case, then H and G satisfy one of the conditions listed below. Furthermore, if H and G satisfy one of these conditions, then H is irreducible.*

(1) Case (L2) or case (U2) holds, H is generated by a $PGL(V)$-conjugate of g_2 and H stabilizes $\frac{|C_G(H)|}{9}$ frames.

(2) One of cases (L2), (L3), (U2) or (U3) holds, H is conjugate to a subgroup of $N_M(g_1)$ in $PGL(V)$, $|H| = 9$ or 18, and H stabilizes four frames.

Proof: As above, we assume $e_i \in X_i$ and we let T be the kernel of the permutation action of M on the X_i. By Lemma 6.7, the subgroups $H \leq M$ satisfying the given conditions are irreducible. It also follows from Lemma 6.7 that if $H \leq M$ is irreducible then H contains an element which permutes the X_i cyclically. It is easy to see that any such element is conjugate to some g_i by an element of T. Note that g_3^2 is conjugate to g_2 in cases (L2) and (U2). Thus if $H \leq M$ is irreducible, we may assume that either $g_1 \in H$ or one of cases (L2) or (U2) holds and $g_2 \in H$.

By Main Lemma 3.87, g_2 stabilizes $\frac{|C_G(g_2)|}{9}$ frames. If $3|(q-1)$ let ω be a primitive cube root of 1 in $\mathbf{F}_q$. Set

$$\begin{array}{lll} u_1 = e_1 + e_2 + e_3 & u_2 = e_1 + \omega e_2 + \omega^2 e_3 & u_3 = e_1 + \omega^2 e_2 + \omega e_3 \\ v_1 = e_1 + e_2 + \omega e_3 & v_2 = e_1 + \omega e_2 + e_3 & v_3 = \omega e_1 + e_2 + e_3 \\ w_1 = e_1 + e_2 + \omega^2 e_3 & w_2 = e_1 + \omega^2 e_2 + e_3 & w_3 = \omega^2 e_1 + e_2 + e_3 \end{array}$$

and for $i \in [3]$ let U_i, V_i and W_i be the subspaces of V generated by u_i, v_i and w_i, respectively. It is easy to see that the frames $\{U_1, U_2, U_3\}$, $\{V_1, V_2, V_3\}$ and $\{W_1, W_2, W_3\}$, along with F, are fixed by $N_M(\langle g_1 \rangle)$. Furthermore, if $F \in \mathcal{UF}$ and $3|\sqrt{q}+1$, then the other three frames are also in $\mathcal{UF}$. Thus if G and H satisfy one of the given conditions, H stabilizes more than one frame.

Assume that one of cases (L2) or (U2) holds, and let $E = \{\mathbf{F}_q y_1, \mathbf{F}_q y_2, \mathbf{F}_q y_3\} \in \mathcal{F}$ be stabilized by g_2 with $E \neq F$. Let $y_1 = ae_1 + be_2 + ce_3$. Since g_2 acts irreducibly on V, we may assume that $y_2 = be_1 + ce_2 + t_2 ae_3$ and $y_3 = ce_1 + t_2 ae_2 + t_2 be_3$. Let T be the kernel of the action of M_F on the X_i and assume for contradiction that some $1 \neq g \in T$ stabilizes E. Let $g' = diag(1, r, s) \in GL(V)$ map to g under the natural projection. If $0 \in \{a, b, c\}$ then exactly one of a, b, c is zero, and it is easy to see that $g = 1$ in this case. Therefore, none of a, b, c is zero. It follows that none of the y_i is an eigenvector for g', so g permutes the y_i cyclically and $r^3 = s^3 = 1$. Replacing g by g^2 if necessary, we may assume that $\mathbf{F}_q(ae_1 + rbe_2 + sce_3) = \mathbf{F}_q y_2$ and $\mathbf{F}_q(ae_1 + r^2 be_2 + s^2 ce_3) = \mathbf{F}_q y_3$. This gives

$$\frac{a}{b} = \frac{rb}{c} = \frac{sc}{t_2 a}$$

and

$$\frac{a}{c} = \frac{r^2 b}{t_2 a} = \frac{s^2 c}{t_2 b}.$$

Now

$$\frac{bcs}{a^2} = t_2 = \frac{s^2 c^2}{ab},$$

so $s = \frac{b^2}{ac}$, and $t_2 = (\frac{b}{a})^3$. This contradicts the fact that t_2 is not a cube in $\mathbf{F}_q$, so if $g_2 \in H$ and $H \cap T \neq 1$ then the only frame fixed by H is F. It follows from Lemma 3.79 and the fact that the normalizer of a Coxeter torus is maximal in $PGL(V)$ that there is no group containing g_2 which is isomorphic to S_3. Thus the only subgroup of M_F containing g_2 which fixes more than one frame is g_2.

Now let $E = \{\mathbf{F}_q y_1, \mathbf{F}_q y_2, \mathbf{F}_q y_3\} \in \mathcal{F}$ be stabilized by g_1 with $E \neq F$. If $1 \neq g \in T$ also fixes E, then arguing as above we may assume that $g^* = diag(1, \omega, \omega^2)$. Thus cases (L1) and (U1) cannot hold. Given Lemma 6.7, it is now sufficient to show that the only frames fixed by both g_1 and g are the four listed above. If $E = \{Y_1, Y_2, Y_3\} \in \mathcal{F}$ is stabilized by $H = \langle g_1, g \rangle$, then the kernel K of the action of H on the Y_i must have order three. The Y_i are therefore the common eigenspaces of $K^* \leq GL(V)$. Since H has four subgroups of order three, H stabilizes at most four frames and we are done. □

Corollary 6.10 *Let V be a 3-dimensional linear or unitary space over $\mathbf{F}_q$ with q odd, and let G be one of $L(V), PGL(V), U(V)$ or $PGU(V)$. Then*

$$\sum_{H \in \mathcal{I}_2(G) \setminus \mathcal{I}_1(G)} \mu(1, H) = \begin{cases} -\frac{|G|}{3} & \textit{in cases (L1) and (U1)} \\ -[G : C_G(g_2)] & \textit{in cases (L2) and (U2)} \\ -\frac{|G|}{3} & \textit{in cases (L3) and (U3).} \end{cases}$$

Proof: Fix a frame $F = \{X_1, X_2, X_3\} \in \mathcal{F}$ such that $F \in \mathcal{UF}$ in the unitary case. Note that M_F contains elements of $PGL(V) \setminus L(V)$ when $3|(q-1)$ and M_F contains elements of $PGU(V) \setminus U(V)$ when $3|(\sqrt{q}+1)$. It follows that G acts transitively on $\mathcal{F}$ in the linear case and G acts transitively on $\mathcal{UF}$ in the unitary case. Let $M = G \cap M_F$. Using

Corollary 6.8 and Lemma 6.9, we see that in cases (L1) and (U1) we have

$$\sum_{H \in \mathcal{I}_2(G) \setminus \mathcal{I}_1(G)} \mu(1,H) = -[G:M]\,\frac{|M|}{3} = -\frac{|G|}{3}.$$

In cases (L2) and (U2), assume that $e_i \in X_i$ and let $N = N_M(\langle g_1 \rangle)$ and $K = C_M(g_1)$. Any subgroup of M satisfying condition (2) of Lemma 6.9 is conjugate in M to either N or K, so any subgroup of G satisfying this condition is conjugate in G to K or N. Also, the number X of conjugates of K satisfying condition (2) is equal to the number of such conjugates of N. The proper subgroups of K are the identity subgroup and four subgroups of order three, so $\mu(1,K) = 3$. It follows easily from Theorem 1.4 that $\mu(1,N) = -27$. Of course, $\mu(1,\langle g_2 \rangle) = -1$. Now using Corollary 6.8 and Lemma 6.9 we can calculate that

$$\sum_{H \in \mathcal{I}_2(G) \setminus \mathcal{I}_1(G)} \mu(1,H) = -\frac{|G|}{3} - [G:C_G(g_2)] + 72X,$$

and in these cases it is sufficient to show that $X = \frac{|G|}{216}$. Let Y be the number of subgroups of M which are isomorphic to K and satisfy condition (2) of Lemma 6.9. Then $4X = [G:M]Y$. Let T be the kernel of the action of M on the X_i. There are $2|T|$ elements of M which permute the X_i cyclically, of which $\frac{2|T|}{3}$ are conjugate to g_1 in $PGL(V)$. These $\frac{2|T|}{3}$ elements generate $\frac{|T|}{3}$ subgroups, each of which is contained in a unique subgroup of M satisfying condition (2). Each of the Y subgroups of M under consideration contains three subgroups which permute the X_i cyclically, so $Y = \frac{|T|}{9} = \frac{|M|}{54}$, and $X = \frac{|G|}{216}$ as claimed.

Note that in case (U3), both K and N as described in the previous paragraph are contained in $PGU(V)$. Therefore, the adjustment for overcounting the groups satisfying condition (2) of Lemma 6.9 in cases (L3) and (U3) is $|G|$. Now it follows from Corollary 6.8 that

$$\sum_{H \in \mathcal{I}_2(G) \setminus \mathcal{I}_1(G)} \mu(1,H) = -[G:M]\,\frac{4|M|}{3} + |G| = -\frac{|G|}{3},$$

and the proof is complete. □

We next examine elements of $\mathcal{I}_3(G) \setminus (\mathcal{I}_1(G) \cup \mathcal{I}_2(G))$.

Lemma 6.11 *Let V be a 3-dimensional linear or unitary space over $\mathbf{F}_q$ with q odd, and let G be one of $L(V), PGL(V), U(V)$ or $PGU(V)$. In the linear case, let C be a Coxeter torus of $PGL(V)$. In the unitary case, let C be a Coxeter torus of $PGU(V)$. Set $N = N_G(C)$, and let H be any subgroup of N.*

(1) $H \in \mathcal{I}_1(G) \cup \mathcal{I}_2(G)$ if and only if H is a 3-group. Furthermore, any 3-group $H \leq N$ is cyclic of order three or elementary abelian of order nine.

(2) If H is not a 3-group then H is not contained in any G-conjugate of N besides N.

Proof: By Lemma 3.16(2), any nontrivial subgroup of C is not contained in $\mathcal{I}_1(G)$. By Lemma 3.92, any nontrivial subgroup of N which intersects C trivially is generated by a $PGL(V)$-conjugate of either g_1 or g_2, and is therefore a 3-group contained in $\mathcal{I}_1(G) \cup \mathcal{I}_2(G)$. Since the order of a maximal element of $\mathcal{I}_2(G)$ divides $6(q-1)^2$ and $|N|$ divides $3(q^2+q+1)$, it follows from Proposition 3.14 that the only prime dividing the order of a nontrivial subgroup of N which is contained in $\mathcal{I}_2(G)$ is three. Furthermore, C contains a nontrivial 3-subgroup if and only if we are in case (L2) or (U2). In those cases, a nontrivial 3-subgroup of $Y \leq C$ is generated by a $PGL(V)$-conjugate of g_2 and by Lemma 3.90, $C_G(Y) = N$. To complete the proof of (1), it is now sufficient to show that in cases (L2) and (U2), a subgroup of N which is generated by Y and a complement X to C in N is contained in $\mathcal{I}_2(G)$. In these cases, it follows from Proposition 3.14 that a maximal element of $\mathcal{I}_2(G)$ contains a Sylow 3-subgroup of G, so the proof of (1) is complete.

Let $H \leq N$ be a non-3-group and let $K = H \cap C$. Then K is not a 3-group and $C_G(K) = C$ by Lemma 3.90. Now any conjugate of C containing K also centralizes K and is therefore equal to C, so (2) holds. $\square$

Corollary 6.12 *Let V be a 3-dimensional linear or unitary space over $\mathbf{F}_q$ with q odd, and let G be one of $L(V), PGL(V), U(V)$ or $PGU(V)$. Define $\mathcal{I}_{321}(G) := \mathcal{I}_3(G) \setminus$*

$(\mathcal{I}_2(G) \cup \mathcal{I}_1(G))$. *Then*

$$\sum_{H \in \mathcal{I}_{321}(G)} \mu(1, H) = \begin{cases} \frac{|G|}{3} - [G:N] & \text{in cases (L1),(L3),(U1) and (U3)} \\ 0 & \text{in cases (L2) and (U2)} \end{cases}$$

Proof: Let N be as in Lemma 6.11. Let N_3 be the set of 3-subgroups of N and let M_3 be the set of subgroups of N not contained in N_3. It follows from Lemma 3.16 that every element of $\mathcal{C}_3(G)$ is conjugate to N in G, since in case (L2) or (U2) N is not contained in $L(V)$ or U(V), respectively. By Lemma 6.11,

$$\sum_{H \in \mathcal{I}_{321}(G)} \mu(1, H) = [G:N] \sum_{H \in M_3} \mu(1, H) = -[G:N] \sum_{H \in N_3} \mu(1, H).$$

We now apply Lemma 3.92. In cases (L1), (L3), (U1) and (U3), $N \setminus C$ consists of $2|C|$ $PGL(V)$-conjugates of g_1, so N_3 contains the identity subgroup and $|C| = \frac{|N|}{3}$ cyclic subgroups of order three. This gives

$$\sum_{H \in \mathcal{I}_{321}(G)} \mu(1, H) = -[G:N](1 - \frac{|N|}{3}) = \frac{|G|}{3} - [G:N].$$

In cases (L2) and (U2), $N \setminus C$ consists of $2|C|$ elements of order three, which generate $|C|$ complements to C in N. Let Y be the center of N, so $Y \leq C$ and $|Y| = 3$. Then every maximal element of N_3 contains Y. It follows from Lemma 2.6 that $\sum_{H \in N_3} \mu(1, H) = 0$.

□

Now we consider the elements of $\mathcal{I}_6(G)$. We first discuss the structure of an element of $\mathcal{C}_6(G)$, quoting results that appear in [28].

Lemma 6.13 *Let V be a 3-dimensional linear or unitary space over a field of order $q = p^a$, where $p > 3$ is prime. Let e_1, e_2, e_3 be a basis for V which is orthonormal if V is a unitary space. Assume $3 | q - 1$, and if V is a unitary space, assume $3 | \sqrt{q} + 1$. Let ω be a primitive cube root of 1 in $\mathbf{F}_q$. Let x be the element of $U(V)$ such that the matrix of x^* with respect to the given basis is $diag(1, \omega, \omega^2)$. Let R be the subgroup of $U(V)$ generated by x and g_1, so R is elementary abelian of order nine. Let G be one of $PGL(V)$, $L(V)$, $PGU(V)$ or $U(V)$. Then every element of $\mathcal{C}_6(G)$ is conjugate to*

$N_G(R)$, which is the split extension of R by a subgroup S of $SL_2(3)$ acting naturally on R. S is isomorphic to one of $SL_2(3)$ or Q_8. Also, if $3 \not| q-1$ then $\mathcal{I}_6(G) = \emptyset$ in both cases (L1) and (U1).

Proof: See [28], pages 151-152. □

Lemma 6.14 *Let V, G, R, S be as in Lemma 6.13 above, and let $H \leq RS$. If $H \notin \mathcal{I}_2(G)$ then $\mu(1, H) = 0$.*

Proof: By Lemma 6.9(2) and its proof, R stabilizes exactly four frames, so RS acts on the set Γ containing these four frames. Since RS is maximal in G (see [28], p.241), $RS = N_G(R)$. Now S contains a unique subgroup X of order two, and by Lemma 6.9(2), the kernel of the action of RS on Γ is RX. Now RS/RX is isomorphic to one of A_4 or the Klein 4-group K, and if $H \leq RS$ does not stabilize an element of Γ then $H/(H \cap RX)$ is isomorphic to one of Z_2, K or A_4. It follows that $H/(H \cap R)$ is isomorphic to one of Z_4, Q_8 or $SL_2(3)$. Each of these groups has a nontrivial Frattini subgroup of order two, and the lemma now follows from two applications of Theorem 2.4. □

Corollary 6.15 *Let V be a 3-dimensional linear or unitary space over a field $\mathbf{F}_q$ of odd order, and let G be one of $L(V), PGL(V), U(V)$ or $PGU(V)$. Set $J = \{1, 2, 3, 6\}$ and $\mathcal{J} = \bigcup_{j \in J} \mathcal{I}_j(G)$. Then*

$$\sum_{H \in \mathcal{J}} \mu(1, H) = 0.$$

Proof: This follows from Lemma 6.5, Corollaries 6.10 and 6.12, and Lemma 6.14. Note that in cases (L2) and (U2), $C_G(g_2)$ is the normalizer of a Coxeter torus of G. □

It is now necessary to get a more detailed description of those subgroups of G which are not contained in $\mathcal{J}$.

Lemma 6.16 *Let V be a 3-dimensional linear or unitary space over a field $\mathbf{F}_q$ of odd order, and let G be one of $L(V), PGL(V), U(V)$ or $PGU(V)$. If G is a linear group let*

$\mathcal{I} = \mathcal{I}^*_{58}(G)$. If G is a unitary group let $\mathcal{I} = \mathcal{I}^*_5(G)$. Let $H \in \mathcal{I}$ and let $K \leq H$. If H is a linear or unitary group, set $J' = J = \{1,2,3,6\}$. If H is an orthogonal group, set $J' = \{1,2\}$. If $j \in J'$ and $K \in \mathcal{I}_j(H)$ with respect to the natural action of H on the space V_* over which H is defined, then $K \in \mathcal{I}_j(G)$.

Proof: Let $\mathbf{F}_*$ be the field over which V_* is defined. If $K \in \mathcal{I}_1(H)$ then the embedding of K in H is a reducible projective $\mathbf{F}_*$-representation of K, which is certainly reducible as an $\mathbf{F}_q$-representation, so $K \in \mathcal{I}_1(G)$. If $K \in \mathcal{I}_2(H)$ then K permutes the elements of an $\mathbf{F}_*$-frame $F = \{X_1, X_2, X_3\}$ from V. Let Y_i be the $\mathbf{F}_q$-span of X_i. Then $\{Y_1, Y_2, Y_3\}$ is a frame from V which lies in $\mathcal{UF}$ in the unitary case, and K permutes the Y_i, so $K \in \mathcal{I}_2(G)$. If $K \in \mathcal{I}_3(H) \setminus \mathcal{I}_1(H)$ then we may assume that V_* is a field $\mathbf{E}_*$ of order $|\mathbf{F}_*|^3$ and K normalizes a cyclic subgroup $\langle k \rangle$, where k acts on V_* as multiplication by some $\alpha \in \mathbf{E}_*$. Since $\mathbf{E}_*$ embeds in $\mathbf{F}_{q^3}$, k is contained in a Coxeter torus $C \leq PGL(V)$, and $N_G(\langle k \rangle) = N_G(C)$. It follows that $K \in \mathcal{I}_3(G)$. Finally, if $K \in \mathcal{I}_6(H)$ then K normalizes an elementary abelian $E \leq H$ such that $|E| = 9$ and E^* acts absolutely irreducibly on V_*. Then E^* acts absolutely irreducibly on V, so $K \in \mathcal{I}_6(G)$. $\Box$

Corollary 6.17 *Let V be a 3-dimensional linear or unitary space over a field $\mathbf{F}_q$ of odd order p^a, with p prime. Let G be one of $L(V), PGL(V), U(V)$ or $PGU(V)$. If G is a linear group let $\mathcal{I} = \mathcal{I}^*_{58}(G)$ and let $S = L(V)$. If G is a unitary group let $\mathcal{I} = \mathcal{I}^*_5(G)$ and let $S = U(V)$. Let $J = \{1,2,3,6\}$ and set $\mathcal{J} = \bigcup_{j \in J} \mathcal{I}_j(G)$. Then every subgroup of G which does not contain S is contained in exactly one of $\mathcal{I}, \mathcal{J}$ or $\mathcal{S}^*(G)$, unless $p = 3$. In that case, all subgroups of G not containing S are contained in exactly one of the given classes except for the subgroups described in the next sentence. If $V_* \in U(\mathbf{F}_*)$ or $L(\mathbf{F}_*)$ with $|\mathbf{F}_*| = 3$ and f is an $\mathbf{F}_*$-symmetric form on V_* then $stab_G(V_*, f)$ and $stab_G(V_*, f) \cap L(V)$ are contained in both $\mathcal{I}$ and $\mathcal{I}_2(G)$.*

Proof: By the definition of $\mathcal{S}^*(G)$, every subgroup of G not containing S is contained in $\mathcal{I} \cup \mathcal{J} \cup \mathcal{S}^*(G)$, and $\mathcal{S}^*(G) \cap (\mathcal{I} \cup \mathcal{J}) = \emptyset$. It follows from part of the proof of Theorem 5.2 that if W is a 3-dimensional orthogonal space over $\mathbf{F}_3$ then the action of $SO(W)$ on W is imprimitive, so the exception stated above certainly exists. It remains to show that no $H \leq G$ can be contained in $\mathcal{I} \cap \mathcal{J}$ unless H satisfies the conditions given in the exception. Let $H \in \mathcal{I}$. By Lemmas 2.10.5 and 2.10.6 of [28], H acts absolutely irreducibly on V, so $H \notin \mathcal{I}_1(G)$. If the exceptional conditions given above do not hold, then H is almost simple, since $H \in \mathcal{I}$. On the other hand, the elements of $\mathcal{I}_j(G)$ are solvable when $j = 2, 3, 6$. □

We can now determine the Möbius number of $PGL(V)$ whenever $L(V) < PGL(V)$, that is, whenever $3|(q-1)$, and that of $PGU(V)$ whenever $U(V) < PGU(V)$, that is, whenever V is defined over $\mathbf{F}_{q^2}$ and $3|q+1$.

Theorem 6.18 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ or a 3-dimensional unitary space over $\mathbf{F}_{q^2}$, where $q = p^a$ and p is an odd prime. If V is a linear space and $L(V) < PGL(V)$ then $\mu(1, PGL(V)) = 0$. If V is a unitary space and $U(V) < PGU(V)$ then $\mu(1, PGU(V)) = 0$.*

Proof: We will proceed by induction on a. Let $J = \{1, 2, 3, 6\}$ and for $G = L(V)$, $PGL(V)$, $U(V)$ or $PGU(V)$ set $\overline{\mathcal{J}}(G) = \left\{H < G : H \notin \bigcup_{j \in J} \mathcal{I}_j(G)\right\}$. By Corollary 6.15, $\mu(1, G) = -\sum_{H \in \overline{\mathcal{J}}(G)} \mu(1, H)$. Note that if H is an orthogonal group and $H \in \mathcal{I}_8(PGL(V))$ or if $H \in \mathcal{S}^*(PGL(V))$, then $H \leq L(V)$, since H contains no normal subgroup of index three. A similar statement holds when $H \leq PGU(V)$. Thus if $a = 1$ and $L(V) < PGL(V)$, then $\overline{\mathcal{J}}(PGL(V)) = \overline{\mathcal{J}}(L(V)) \cup \{L(V)\}$. Similarly, if $a = 1$ and $U(V) < PGU(V)$, then we have $\overline{\mathcal{J}}(PGU(V)) = \overline{\mathcal{J}}(U(V)) \cup \{U(V)\}$. The claim of the lemma for $a = 1$ follows immediately. Now assume $a > 1$. If $L(V) < PGL(V)$, then every element of $\overline{\mathcal{J}}(PGL(V)) \setminus \overline{\mathcal{J}}(L(V))$ besides $L(V)$ is isomorphic to $PGL(W)$ or $PGU(W)$, where W is a 3-dimensional linear or unitary space defined over a subfield of $\mathbf{F}_q$ such that $L(W) < PGL(W)$ in the linear case and $U(W) < PGU(W)$ in the unitary case. A similar statement holds in the unitary case. By our inductive hypothesis, the Möbius number of any one of these subgroups is zero, and the Lemma follows. □

We will finish the computation of $\mu(1, G)$ when $G = L(V)$ or $U(V)$ by using Corollaries 6.15 and 6.17 and then separately examining three classes of subgroups, namely, the members of $\mathcal{S}^*(G)$, the members of $\mathcal{I}$ which are orthogonal groups, and the members of $\mathcal{I}$ which are linear or unitary groups. This last class will be handled by induction on q. Our first step is to list the Möbius numbers of the elements of $\mathcal{S}^*(G)$.

Lemma 6.19 *(1)* $\mu(1, A_5) = -60 = -|A_5|$.

(2) $\mu(1, L_2(7)) = 0$.

(3) $\mu(1, A_6) = 720 = 2|A_6|$.

(4) $\mu(1, M_{10}) = 0$.

(5) $\mu(1, A_7) = -2520 = -|A_7|$.

Proof: Since $A_5 \cong L_2(5)$ and $A_6 \cong L_2(9)$, claims (1),(2) and (3) follow from Theorems 5.1 and 5.2. Since M_{10} is a nonsplit extension of A_6 by Z_2 (see [18], p.40), $\mu(1, M_{10}) = 0$ by Crapo's complement theorem. All nonsolvable transitive proper subgroups of A_7 are isomorphic to $L_2(7)$ (see [19]). Corollary 1 of [37] says that the sum of the Möbius numbers of the nonsolvable transitive subgroups of A_p is $-\frac{p!}{2}$ for any odd prime p. Given this result, claim (5) follows from claim (2). $\square$

Corollary 6.20 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ or a 3-dimensional unitary space over $\mathbf{F}_{q^2}$, where $q = p^a$ and p is an odd prime. If V is a linear space, define*

$$c_p(a) := \frac{\sum\limits_{H \in \mathcal{S}^*(L(V))} \mu(1, H)}{|PGL(V)|},$$

and if V is a unitary space define

$$d_p(a) := \frac{\sum\limits_{H \in \mathcal{S}^*(U(V))} \mu(1, H)}{|PGU(V)|}.$$

The values of $c_p(a)$ and $d_p(a)$ are given in the table below.

$p \bmod 15$	$a \bmod 2$	$c_p(a)$	$d_p(a)$
$1, 4$	0	1	-1
	1	1	-1
$11, 14$	0	1	-1
	1	-1	1
$2, 7, 8, 13$	0	1	-1
	1	0	0
3	0	-1	-1
	1	0	0
5	0	0	0
	1	0	0

Proof: This follows immediately from Lemmas 6.2, 6.4 and 6.19. □

Now we determine the contribution of orthogonal subgroups to $\mu(1, G)$.

Lemma 6.21 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ or a three dimensional unitary space over $\mathbf{F}_{q^2}$, where $q = p^a$ with p an odd prime. Let b be a divisor of a, and if $p = 3$ assume that $b > 1$. In the linear case, $\mathcal{I}^*_{58}(L(V))$ contains one $PGL(V)$-conjugacy class of subgroups isomorphic to $PSO_3(p^b)$ and one $PGL(V)$-conjugacy class of subgroups isomorphic to $P\Omega_3(p^b)$. These classes both contain $\frac{|PGL(V)|}{|PSO_3(p^b)|}$ subgroups. In the unitary case, $\mathcal{I}^*_5(U(V))$ contains one $PGU(V)$-conjugacy class of subgroups isomorphic to $PSO_3(p^b)$ and one $PGU(V)$-conjugacy class of subgroups isomorphic to $P\Omega_3(p^b)$. Each of these classes contains $\frac{|PGU(V)|}{|PSO_3(p^b)|}$ subgroups.*

Proof: Set $r = p^b$. We will use the isomorphisms $\Omega_3(r) \cong L_2(r)$ and $SO_3(r) \cong PGL_2(r)$. Assume temporarily that $r \neq 9$. By [47] §7(x) and Theorem 10, any embedding of $L_2(r)$ in $L(V)$ or $U(V)$ is a 3-dimensional projective representation of $L_2(r)$, which can be lifted to a unique 3-dimensional linear representation of $SL_2(r)$ in characteristic p.

In [44], it is shown that $SL_2(r)$ has $log_p r$ irreducible representations of degree three, all of which can be realized over $\mathbf{F}_r$ and over no smaller field, and all of which are conjugate conjugate by automorphisms of $\mathbf{F}_r$. It follows that $L(V)$ contains one $PGL(V)$-conjugacy class of irreducible subgroups isomorphic to $L_2(r)$. Since the representation of $\Omega_3(r)$ on its natural orthogonal space is absolutely irreducible by Proposition 2.10.6 of [28], these irreducible subgroups are exactly the members of $\mathcal{I}^*_{58}(G)$ which are isomorphic to $\Omega_3(r)$. Since $PGL(V)$ contains no normal subgroup of index two and $SO_3(r)$ contains such a subgroup, the image any embedding of $SO_3(r) \cong PGO_3(r)$ in $PGL(V)$ must lie in $L(V)$. By Clifford's Theorem (see [25], p.79), the restriction of an irreducible 3-dimensional projective representation of $PGL_2(r)$ to $L_2(r)$ is irreducible, so any irreducible embedding of $SO_3(r)$ in $L(V)$ is simply an extension of one of the embeddings of $\Omega_3(r)$ which we have already described. We already know that every subgroup of $L(V)$ containing one of our subgroups isomorphic to $\Omega_3(r)$ or $SO_3(r)$ is almost simple. It follows immediately that the subgroups isomorphic to $SO_3(r)$ are self normalizing, which proves our claim about the size of the conjugacy classes. The only claim in the unitary case which does not follow immediately from the results in the linear case is the claim that all the elements of $\mathcal{I}_5(U(V))$ isomorphic to $SO_3(r)$ are conjugate in $U(V)$. Note that any such subgroup is of the form $SO(V_*, f_{|V_*})$ for some $V_* \in U(\mathbf{F}_r)$. Let H be a hyperbolic plane in V_* and let x generate an orthogonal complement to H. Let α be an element of $\mathbf{F}_q \setminus \mathbf{F}_*$ such that α^2 is a nonsquare in $\mathbf{F}_*$. Let W_* be the $\mathbf{F}_*$-span of H and αx. Then $W_* \in U(\mathbf{F}_*)$ and $(W_*, f_{|W_*})$ has the same stabilizer in $U(V)$ as does $(V_*, f_{|V_*})$. Thus we may assume in the unitary case that any element of $\mathcal{I}^*_5(U(V))$ stabilizes an element of some $U(\mathbf{F}_*)$ which has an orthogonal basis x_1, x_2, x_3 such that $(x_i, x_i) = 1$ for all i. The existence of a unique $U(V)$-conjugacy class containing all elements of $\mathcal{I}^*_5(U(V))$ of a given isomorphism type now follows from the transitivity of $U(V)$ on orthonormal bases for V.

The only reason that the above argument cannot be applied directly to the case $r = 9$ is that the universal covering group of $L_2(9) \cong A_6$ is not $SL_2(9)$. However, the existence of a unique conjugacy class of irreducible embeddings of $L_2(9)$ in $PGL_2(3^a)$ for all even a follows from information on page four of [27]. The remainder of the proof in this case is the same as above. □

Lemma 6.22 *Let p be an odd prime and let a be a positive integer. If $p = 3$ assume $a > 1$. Then*

$$\mu(1, \Omega_3(p^a)) + \mu(1, SO_3(p^a)) = \begin{cases} |PSO_3(p)| & \text{if } p \equiv 1,4 \bmod 5 \text{ and } a = 1 \\ |PSO_3(p^2)| & \text{if } p \equiv 2,3 \bmod 5 \text{ and } a = 2 \\ 0 & \text{otherwise} \end{cases}$$

Proof: This follows immediately from Theorems 5.1 and 5.2. □

Corollary 6.23 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ or a 3-dimensional unitary space over $\mathbf{F}_{q^2}$, where $q = p^a$ with p and odd prime. In the linear case, let F be the set of elements of $\mathcal{I}_8(L(V)) \setminus \mathcal{I}_2(L(V))$ which are isomorphic to $PSO_3(p^b)$ or $P\Omega_3(p^b)$ for some divisor b of a, and define*

$$f_p(a) := \frac{\sum_{H \in F} \mu(1, H)}{|PGL(V)|}.$$

In the unitary case, let F be the set of elements of $\mathcal{I}_5(U(V)) \setminus \mathcal{I}_2(U(V))$ which are isomorphic to $PSO_3(p^b)$ or $P\Omega_3(p^b)$ for some divisor b of a, and define

$$g_p(a) := \frac{\sum_{H \in F} \mu(1, H)}{|PGU(V)|}.$$

The values of $f_p(a)$ and $g_p(a)$ are given in the table below.

$p \bmod 5$	$a \bmod 2$	$f_p(a)$	$g_p(a)$
$1,4$	0	1	1
	1	1	1
$2,3$	0	1	1
	1	0	0
5	0	0	0
	0	0	0

Proof: This follows immediately from Lemmas 6.21 and 6.22. □

The only subgroups which have not yet been accounted for are the simple linear and unitary groups in $\mathcal{I}^*_{58}(L(V))$ and the simple unitary subgroups in $\mathcal{I}^*_5(U(V))$. We restate a result from [34].

Lemma 6.24 *Let V be a 3-dimensional linear space over $\mathbf{F}_q$ or a 3-dimensional unitary space over $\mathbf{F}_{q^2}$, where $q = p^a$ with p an odd prime. If V is a linear space then for each proper divisor b of a, $\mathcal{I}^*_{58}(L(V))$ contains one $PGL(V)$-conjugacy class of $\frac{|PGL(V)|}{|PGL_3(p^b)|}$ subgroups isomorphic to $L_3(p^b)$. Also, if a is even then for each divisor b of $\frac{a}{2}$, $\mathcal{I}^*_{58}(L(V))$ contains one $PGL(V)$-conjugacy class of $\frac{|PGL(V)|}{|PGU_3(p^b)|}$ subgroups isomorphic to $U_3(p^b)$. If V is a unitary space, then for each proper divisor b if a such that $\frac{a}{b}$ is odd, $\mathcal{I}^*_5(U(V))$ contains one $PGU(V)$-conjugacy class of $\frac{|PGU(V)|}{|PGU_3(p^b)|}$ subgroups isomorphic to $U_3(p^b)$.*

Proof: Except for the sizes of the conjugacy classes, this result is stated explicitly in [34]. The fact that the normalizers of the given groups are as stated follows immediately from the fact that the only overgroups of these groups in $PGL(V)$ are almost simple. □

Corollary 6.25 *Let p be a fixed odd prime. Define functions α_p and β_p on the positive integers by*

$$\alpha_p(a) := \frac{\mu(1, L_3(p^a))}{|PGL_3(p^a)|}$$

and

$$\beta_p(a) := \frac{\mu(1, U_3(p^a))}{|PGU_3(p^a)|}.$$

For a positive integer a, let $D(a)$ be the set of divisors of a, let $D^*(a)$ be the set of proper divisors of a. Let $D^o(a)$ be the set of proper divisors b of a such that $\frac{a}{b}$ is odd and let $D^e(a) = D^*(a) \setminus D^o(a)$. Then

$$\alpha_p(a) = -(c_p(a) + f_p(a) + \sum_{b \in D^e(a)} \beta_p(b) + \sum_{b \in D^*(a)} \alpha_p(b))$$

and

$$\beta_p(a) = -(d_p(a) + g_p(a) + \sum_{b \in D^o(a)} \beta_p(b)).$$

Proof: This follows from Corollary 6.15, Corollary 6.17, Theorem 6.18, and Lemmas 6.21 and 6.24. □

We can now compute $\mu(1, L_3(p^a))$ and $\mu(1, U_3(p^a))$ using induction on a.

Theorem 6.26 *Let p be an odd prime and let a be a positive integer. Then*

$$\mu(1, L_3(p^a)) = \begin{cases} -6|L_3(p^a)| & \text{if } a = 1 \text{ and } p \equiv 1, 4 \bmod 15 \\ -6|L_3(p^a)| & \text{if } a = 2 \text{ and } p \equiv 2, 7, 8, 13 \bmod 15 \\ 0 & \text{otherwise} \end{cases}$$

Also,

$$\mu(1, U_3(p^a)) = \begin{cases} -6|U_3(p^a)| & \text{if } a = 1 \text{ and } p \equiv 11, 14 \bmod 15 \\ 0 & \text{otherwise} \end{cases}$$

Proof: We will use Corollary 6.25. Let $\alpha_p, \beta_p, c_p, d_p, f_p$ and g_p be as defined above. We will examine several cases, depending on $p \bmod 15$.

Case (1) - $p \equiv 3, 5 \bmod 15$, so $p = 3$ or 5: In this case, $c_p(a) + f_p(a) = d_p(a) + g_p(a) = 0$ for all a. By Corollary 6.25, $\alpha_p(1) = \beta_p(1) = 0$, and then $\alpha_p(a) = \beta_p(a) = 0$ for all a by induction on a.

Case (2) - $p \equiv 1, 4 \bmod 15$: In this case we have $c_p(a) + f_p(a) = 2$ for all a and $d_p(a) + g_p(a) = 0$ for all a. From the second fact, we get $\beta_p(a) = 0$ for all a using Corollary 6.25 and induction on a. Again using the Corollary, we get

$$\alpha_p(a) = -(2 + \sum_{b \in D^*(a)} \alpha_p(b)).$$

Using induction on a, we see that $\alpha_p(1) = -2$ and $\alpha_p(a) = 0$ for $a > 1$. Note that since $p \equiv 1 \bmod 3$ we have $[PGL_3(p) : L_3(p)] = 3$, so $\mu(1, L_3(p)) = -2|PGL_3(p)| = -6|L_3(p)|$.

Case (3) - $p \equiv 2, 7, 8, 13 \bmod 15$: Here we have $d_p(a) + g_p(a) = 0$ for all a and

$$c_p(a) + f_p(a) = \begin{cases} 2 & \text{if } a \text{ is even} \\ 0 & \text{if } a \text{ is odd} \end{cases}$$

As in the above cases, using the first fact and Corollary 6.25, we get $\beta_p(a) = 0$ for all a. Then

$$\alpha_p(a) = \begin{cases} -(2 + \sum_{b \in D^*(a)} \alpha_p(b)) & \text{if } a \text{ is even} \\ -\sum_{b \in D^*(a)} \alpha_p(b) & \text{if } a \text{ is odd} \end{cases}$$

This gives $\alpha_p(1) = 0$, $\alpha_p(2) = -2$ and $\alpha_p(a) = 0$ for $a > 2$ by induction on a. Since $p^2 \equiv 1 \bmod 3$, we have $\mu(1, L_3(p^2)) = -2|PGL_3(p^2)| = -6|L_3(p^2)|$.

Case (4) - $p \equiv 11, 14 \bmod 15$: Here we have

$$c_p(a) + f_p(a) = \begin{cases} 2 & \text{if } a \text{ is even} \\ 0 & \text{if } a \text{ is odd} \end{cases}$$

Also,

$$d_p(a) + g_p(a) = \begin{cases} 0 & \text{if } a \text{ is even} \\ 2 & \text{if } a \text{ is odd} \end{cases}$$

From the second fact, we get $\beta_p(1) = -2$ and $\beta_p(a) = 0$ for $a > 1$ by induction on a. Since $p \equiv 2 \bmod 3$, $[PGU_3(p) : U_3(p)] = 3$, and $\mu(1, U_3(p)) = -2|PGU_3(p)| = -6|U_3(p)|$. The determined values of β give $\alpha_p(1) = 0$ and by induction, $\alpha_p(a) = 0$ for $a > 1$. $\square$

Chapter 7

The Möbius numbers of the Suzuki groups

If $q = 2^a$ with $a > 1$ odd, there exists a finite simple group $Sz(q)$ of order $q^2(q-1)(q^2+1)$. The Suzuki groups $Sz(q)$ were discovered by Suzuki. Their structure is described in [50]. In this section, we will determine $\mu(1, Sz(q))$. We list the facts from [50] which will be useful to us.

Theorem 7.1 (Suzuki) *Let $a > 1$ be odd and set $q = 2^a$. Let $G = Sz(q)$.*

(1) G has a 2-transitive permutation representation of degree $q^2 + 1$ in which the stabilizer of any three points is trivial. The stabilizer of a point in this representation is a Frobenius group H. The kernel Q of H is a Sylow 2-subgroup of G, with $|Q| = q^2$. A complement D to Q in H is cyclic of order $q - 1$.

(2) For each divisor b of a with $1 < b < a$, G contains one conjugacy class of self-normalizing subgroups isomorphic to $Sz(2^b)$. Any subgroup of G which is not in one of these conjugacy classes is contained in a conjugate of one of the maximal subgroups listed below.

(a) H.

(b) $B_0 = N_G(D)$, which is dihedral of order $2(q - 1)$.

(c) A subgroup B_1 which is a split extension of a cyclic group A_1 of order $q + \sqrt{2q} + 1$ by a cyclic group of order four.

(d) A subgroup B_2 which is a split extension of a cyclic group A_2 of order $q-\sqrt{2q}+1$ by a cyclic group of order four.

(3) If $g \in G$ is a nonidentity element of odd order then $C_G(g)$ is conjugate to one of D, A_1 or A_2.

Proof: (1) is Theorem 10 of [50], (2) is Theorem 9, and (3) is stated in the proof of Theorem 9 (and follows from Theorem 4). □

Note that it follows immediately from (3) above that if $1 \neq g \in X$ with X conjugate to D, A_1 or A_2 then $C_G(g) = X$.

Theorem 7.2 *For an odd integer $a > 1$, define*

$$\sigma(a) := \frac{\mu(1, Sz(2^a))}{|Sz(2^a)|}.$$

Then for all such a,

$$\sigma(a) = \mu(a),$$

where μ is the usual number theoretic Möbius function.

Proof: Fix an odd integer $a > 1$ and set $G = Sz(2^a)$. Let $\mathcal{H}$ be the set of G-conjugates of H, and let $\mathcal{I}$ be the ideal in the subgroup lattice of G generated by $\mathcal{H}$. By Theorem 7.1(1) and Lemmas 2.6 and 2.17,

$$\sum_{J\in\mathcal{I}} \mu(1, J) = 1 - (q^2+1) + \binom{q^2+1}{2} = \binom{q^2}{2}.$$

Let $\mathcal{B}_0$ be the set of subgroups of B_0 which are not contained in any conjugate of H, let $\mathcal{B}_1$ be the set of subgroups of B_1 which are not contained in any subgroup of G conjugate to one of H or B_0, and let $\mathcal{B}_2$ be the set of subgroups of B_2 which are not contained in any subgroup of G conjugate to one of H, B_0 or B_1. For $i = 0, 1, 2$, let $\mathcal{B}_i^*$ be the set of G-conjugates of the elements of $\mathcal{B}_i$. Let $D''(a)$ be the set of divisors b of

a such that $1 < b < a$, and let $\mathcal{S}$ be the set of subgroups of G which are isomorphic to $Sz(2^b)$ for some $b \in D''(a)$. By Theorem 7.1(2), the set of proper subgroups of G is the disjoint union of $\mathcal{I}$, $\mathcal{B}_0^*$, $\mathcal{B}_1^*$, $\mathcal{B}_2^*$, and $\mathcal{S}$.

Let Γ be the set of subgroups of G which are conjugate to one of D, A_1 or A_2. By Theorem 7.1(3), if J, L are distinct elements of Γ then $J \cap L = 1$. Using this fact and the fact that H is a Frobenius group, we get the following results.

(0) Let $J \leq B_0$. Then $J \in \mathcal{B}_0$ if and only if J is dihedral.

(1) Let $J \leq B_1$. Then $J \in \mathcal{B}_1$ if and only if J is not a 2-group.

(2) Let $J \leq B_2$. Then $J \in \mathcal{B}_2$ if and only if J is not a 2-group.

(3) If $J \in \mathcal{B}_i^*$ then J is contained in a unique conjugate of B_i. Thus for $i = 0, 1, 2$,

$$\sum_{J \in \mathcal{B}_i^*} \mu(1, J) = [G : B_i] \sum_{J \in \mathcal{B}_i} \mu(1, J).$$

We now apply these results. Let C_0 be the set of cyclic subgroups of B_0. Note that C_0 consists of the subgroups of B_0 which are not in $\mathcal{B}_0$. All subgroups of D are in C_0, and the remaining elements of C_0 are the $q - 1$ subgroups of B_0 which have order two. It follows that

$$\sum_{J \in \mathcal{B}_0^*} \mu(1, J) = -[G : B_0] \sum_{J \in C_0} \mu(1, J) = \frac{|G|}{2}.$$

Let T_1 be the set of 2-subgroups of B_1. By Theorem 7.1(3), T_1 consists of the identity subgroup, $\frac{|B_1|}{4}$ subgroups of order two, and $\frac{|B_1|}{4}$ cyclic subgroups of order four. This gives

$$\sum_{J \in \mathcal{B}_1^*} \mu(1, J) = [G : B_1] \left(\frac{|B_1|}{4} - 1\right).$$

A similar argument shows that

$$\sum_{J \in \mathcal{B}_2^*} \mu(1, J) = [G : B_2] \left(\frac{|B_2|}{4} - 1\right).$$

Let $\mathcal{J} = \mathcal{I} \cup (\bigcup_{i=0}^{2} \mathcal{B}_i^*)$. Since $[G : B_1] + [G : B_2] = \binom{q^2}{2}$, we have

$$\sum_{J \in \mathcal{J}} \mu(1, J) = |G|.$$

We can now finish the proof by multiplicative induction on a. If a is prime, then $\mathcal{S} = \emptyset$ and every proper subgroup of G is contained in $\mathcal{J}$. It follows that $\sigma(a) = -1 = \mu(a)$ for all odd primes a. Now if a is composite, then by the above results and the inductive hypothesis, we have

$$\sigma(a) = -(1 + \sum_{b \in D''(a)} \sigma(b)) = -(1 + \sum_{b \in D''(a)} \mu(b)) = \mu(a).$$

The proof is complete. □

Chapter 8

The Möbius number of the subgroup lattice of the symmetric group

8.1 Introduction and statement of the main results

In [45], it was asked whether the Möbius number $\mu(1, S_n)$ of the subgroup lattice of the symmetric group S_n is equal to $(-1)^{n-1}\frac{|Aut(S_n)|}{2}$ for all $n > 1$. This equality has been shown to hold for $n \leq 11$, by Wensley for $n \leq 8$ ([53]) and by Pahlings and Pfeiffer for $9 \leq n \leq 11$ ([37]). In this chapter, we will give a formula for $\mu(1, S_n)$, involving the Möbius numbers of certain transitive subgroups, that holds for all $n \in N$, and then refine this formula for certain values of n to give a formula involving the Möbius numbers of certain primitive subgroups. Using this second formula, along with the O'Nan-Scott Theorem and the classification of finite simple groups, we will calculate $\mu(1, S_n)$ for all n which are prime, twice a prime, or a power of two. This will give three infinite classes for which the equality given above always holds, and a class for which the equality does not hold, thereby giving a negative answer to Stanley's question. In the case $n = 2p$, we will get a formula for $\mu(1, S_n) + \mu(1, A_n)$ which will allow us to calculate $\mu(1, A_n)$ in certain cases. This will give counterexamples to two recent conjectures, the conjecture of Pahlings that $\mu(1, S_n) + \mu(1, A_n) = 0$ (see [37]), and the conjecture of Welker on the homotopy type of the chain complex associated to the subgroup lattice of A_n (see [52]). The exact calculation of $\mu(1, S_n)$ depends on the knowledge of $\mu(1, H)$ for certain H satisfying $L_2(q) \leq H \leq Aut(L_2(q))$, for odd prime powers q. The calculation of $\mu(1, H)$ for these groups was carried out in Chapter 5. The basic definitions and main results described here are given below.

Definition 8.1 *Let $G \leq S_n$.*

(1) G is transitive if for all $i, j \in [n]$ there exists some $g \in G$ such that $i^g = j$. G is intransitive otherwise.

(2) G is imprimitive if G is transitive and there exists some $B \subseteq [n]$ with $1 < |B| < n$ such that $B \cap B^g \in \{B, \emptyset\}$ for all $g \in G$. Equivalently, G is imprimitive if G is transitive and there exists a partition $[n] = \dot{\bigcup}_{i=1}^{k} B_i$ such that for all $g \in G$ and $i \in [k]$ there exists some $j \in [k]$ with $B_i^g = B_j$.

(3) G is primitive if G is transitive and not imprimitive.

Clearly, every subgroup of S_n is either intransitive, imprimitive or primitive, and we will use this partition of the subgroup lattice of S_n into these three types to make our calculations. Note that if $G \leq S_n$ is imprimitive then by transitivity all the B_i described in (2) above must have the same cardinality.

Definition 8.2 *Let $n \in N$. An odd involution is an element of order 2 in S_n which is not contained in A_n. The following sets of subgroups of S_n will appear throughout this chapter:*

(a) $\mathcal{C}_n = \{H < S_n : H$ is transitive and contains an odd involution $\}$
(b) $\mathcal{P}_n = \{H \in \mathcal{C}_n : H$ is primitive$\}$
(c) $\mathcal{I}_n = \mathcal{C}_n \setminus \mathcal{P}_n$

Note that in (a) above, $H \in \mathcal{C}_n$ implies that H is a proper subgroup of S_n.

Proposition 8.3 *For all $n \in \mathbf{N}$*

$$\mu(1, S_n) = (-1)^{n-1}\frac{n!}{2} - \sum_{H \in \mathcal{C}_n} \mu(1, H)$$

Theorem 8.4 *For the following values of n,*

$$\mu(1, S_n) = (-1)^{n-1}\frac{n!}{2} - \sum_{H \in \mathcal{P}_n} \mu(1, H)$$

(1)	$n = p$	*p prime*
(2)	$n = p^2$	*p prime*
(3*a*)	$n = 2p$	*p an odd prime*
(3*b*)	$n = pr$	*p, r distinct odd primes*
(4)	$n = 2^a$	$a \in \mathbf{N}$

Note that case (1) above follows immediately from Proposition 8.3. There are no values of n known to the author for which the formula given in Theorem 8.4 does not hold.

Theorem 8.5 *Let p be prime. Then*

$$\mu(1, S_p) = (-1)^{p-1}\frac{p!}{2}$$

Proposition 8.3 and Theorem 8.5 were obtained independently by Herbert Pahlings (see [37]). Corollary 8.33, which is an improvement of an earlier version proved by the author, appears in [37].

Theorem 8.6 *Let $n = 2p$, p an odd prime.*

$$\mu(1, S_n) = \begin{cases} -n! & \textit{if } n-1 \textit{ is prime and } p \equiv 3 \pmod 4 \\ \frac{n!}{2} & \textit{if } n = 22 \\ -\frac{n!}{2} & \textit{otherwise} \end{cases}$$

This result settles Stanley's question, but does not prove that there are infinitely many n for which $\mu(1, S_n) \neq (-1)^{n-1}\frac{n!}{2}$.

Theorem 8.7 *Let $n = 2^a$, $a \in \mathbf{N}$. Then*

$$\mu(1, S_n) = -\frac{n!}{2}$$

8.2 The structure and Möbius number of certain orbit lattices

The results in this section will be used throughout this chapter. They are presented together here since they might also be of interest in other combinatorial settings (see for example [42]).

Definition 8.8 *Let $G \leq S_n$. The orbit lattice of G (called the lattice of periods in [42]) is*

$$\mathcal{P}(G,[n]) = \{X \in \Pi_n : \text{ the orbits of some } H \leq G \text{ are the parts of } X\}$$

The importance of $\mathcal{P}(G,[n])$ to the calculation of $\mu(1,G)$ is made clear by the following lemma, which appears in many places and is an immediate consequence of Crapo's closure theorem.

Lemma 8.9 *Let $G \leq S_n$ be transitive and let $\mathbf{P} = \mathcal{P}(G,[n])$. Set*

$$\mathcal{T}(G) = \{H \leq G : H \text{ is transitive}\}.$$

Then

$$\sum_{H \in \mathcal{T}(G)} \mu(1,H) = \mu_{\mathbf{P}}(\hat{0},\hat{1})$$

Proof: Let $^-$ be the closure on the subgroup lattice of G such that $\overline{H}$ is the subgroup of G which is maximal with respect to having the same orbits as H. Then $\overline{1} = 1$ and $\overline{H} = G$ if and only if H is transitive. Now apply Theorem 2.3. $\square$

Corollary 8.10 *Let $G \leq S_n$ with $G^* = G \cap A_n$ transitive. Set $\mathbf{P} = \mathcal{P}(G,[n])$ and $\mathbf{P}^* = \mathcal{P}(G^*,[n])$. Let $\mathcal{T}$ be the set of transitive subgroups of G which are not contained in G^*. Then*

$$\sum_{H \in \mathcal{T}} \mu(1,H) = \mu_{\mathbf{P}}(\hat{0},\hat{1}) - \mu_{\mathbf{P}^*}(\hat{0},\hat{1})$$

Applying Corollary 8.10 to S_n and A_n will prove Proposition 8.3, which will be refined to produce the main results of this chapter. Clearly $\mathcal{P}(S_n,[n]) = \Pi_n$. Let R_1 be the first rank of Π_n, that is, the set of all partitions of $[n]$ into one pair and $n-2$ singletons. It is easy to show that $\mathcal{P}(A_n, [n]) = \Pi_n \setminus R_1$.

The next result follows immediately from Theorem 2.4, and will be used repeatedly.

Proposition 8.11 *Let $H \leq S_n$ with $H \not\leq A_n$. If H does not contain an odd involution, then $\mu(1, H) = 0$.*

Proof: If $H \not\leq A_n$ and H contains no odd involution, then H contains no complement to $H \cap A_n$. □

We can now prove Proposition 8.3 by examining the orbit lattices for S_n and A_n.

Proof of 8.3: Set $\mathbf{P} = \mathcal{P}(S_n, [n])$ and $\mathbf{P}^* = \mathcal{P}(A_n, [n])$. By Corollary 8.10 and Proposition 8.11,

$$\mu(1, S_n) + \sum_{H \in \mathcal{C}_n} \mu(1, H) = \mu_{\mathbf{P}}(\hat{0}, \hat{1}) - \mu_{\mathbf{P}^*}(\hat{0}, \hat{1})$$

Note that if $0 < X \in \mathbf{P}^*$ then $\mu^*_{\mathbf{P}}(X, \hat{1}) = \mu_{\mathbf{P}}(X, \hat{1})$. It follows that

$$\mu_{\mathbf{P}}(\hat{0}, \hat{1}) - \mu_{\mathbf{P}^*}(\hat{0}, \hat{1}) = -\sum_{X \in R_1} \mu_{\mathbf{P}}(X, \hat{1})$$

Now $|R_1| = \binom{n}{2}$, and for each $X \in R_1$ the interval $\left[X, \hat{1}\right]_P$ is isomorphic to Π_{n-1}. The proposition now follows immediately from Lemma 2.7. □

We next study certain orbit lattices which will appear throughout this chapter.

Definition 8.12 *(a) An equipartition of $[n]$ is any $\Psi \in \Pi_n$ such that Ψ has k parts of size l, with $kl = n$. Unless otherwise stated, we assume $1 < k < n$.*

(b) For any equipartition $\Psi \in \Pi_n$, we define G_Ψ to be the stabilizer of Ψ in S_n, that is, the group of all $g \in S_n$ which permute the parts of Ψ.

G_Ψ and $G_\Psi \cap A_n$ are transitive. We will describe $\mathcal{P}(G_\Psi, [n])$ and $\mathcal{P}(G_\Psi \cap A_n, [n])$ and then apply Lemma 8.9.

Definition 8.13 *Let* $\Psi = [E_1; \ldots ; E_k]$ *be an equipartition of* $[n]$ *and let* $X = [X_1; \ldots ; X_r] \in \Pi_n$. (Ψ, X) *is a balanced pair if* $\Psi \vee_{\Pi_n} X = \hat{1}_{\Pi_n}$ *and for all* $i \in [r]$, $|X_i \cap E_j|$ *is independent of* $j \in [k]$.

For example, if $\Psi = [\{1,2,3\}\,;\{4,5,6\}]$, $X = [\{1,4\}\,;\{2,3,5,6\}]$ and $Y = [\{1,2,5\}\,;\{3,4,6\}]$ then (Ψ, X) is a balanced pair, but (Ψ, Y) is not a balanced pair since $|\,\{1,2,5\} \cap \{1,2,3\}\,| \neq |\,\{1,2,5\} \cap \{4,5,6\}\,|$

Lemma 8.14 *Let* $\Psi = [E_1; \ldots ; E_k]$ *be an equipartition of* $[n]$ *with* $|E_1| = l$ *and let* $X = [X_1; \ldots ; X_r] \in \Pi_n$. *Set* $G = G_\Psi$, $\mathbf{P} = \mathcal{P}(G, [n])$, $G^* = G \cap A_n$, *and* $\mathbf{P}^* = \mathcal{P}(G^*, [n])$. *Then*

(1) $X \in \mathbf{P}$ *if and only if for each part* Y_t *of* $Y = \Psi \vee_{\Pi_n} X$, *the parts of* Ψ *contained in* Y_t *and the parts of* X *contained in* Y_t *determine a balanced pair of partitions of* Y_t.

(2) $\mathbf{P}^* \subseteq \mathbf{P}$, *and* $W \in \mathbf{P} \setminus \mathbf{P}^*$ *if and only if* W *is of one of the types described below.*

Type A: $W = [\{x, y\}\,; n-2 \text{ singletons}]$ *with* $\{x, y\} \subseteq E_i$ *for some* $i \in [k]$.

Type B: $W = [\{x_1, y_1\}\,;\{x_2, y_2\}\,; \ldots ;\{x_l, y_l\}\,; n-2l \text{ singletons}]$, *with*
l *odd and* $\{x_1, \ldots, x_l\}$ *and* $\{y_1, \ldots, y_l\}$ *both parts of* Ψ.

Type C: $W = [\{x_1, x_2\}\,;\{x_3\}\,; \ldots ;\{x_l\}\,; W_l; \ldots ; W_s]$, *with* l *even,*
$\{x_1, \ldots, x_l\}$ *a part of* Ψ, $|W_j \cap E_t| \leq 1$ *for all* $j > 1$ *and* $t \in [k]$
(and W *is not of type* A*).*

Proof: (1) $(\Rightarrow)$ Let $H \leq G$ have orbits given by $X \in \mathbf{P}$, and assume that X_i, E_c, and E_d are all contained in Y_t with $x \in X_i \cap E_c$ and $y \in X_i \cap E_d$. There is some $h \in H$ with $x^h = y$, so $(X_i \cap E_c)^h = X_i \cap E_d$ and $|X_i \cap E_c| = |X_i \cap E_d|$. It remains to show that if X_i and E_c are contained in the same part of Y then $X_i \cap E_c \neq \emptyset$.

Let $I_c = \{i \in [r] : X_i \cap E_c \neq \emptyset\}$ and let $D_c = \{d \in [k] : E_d \cap X_i \neq \emptyset$ for some $i \in I_c\}$. If $d \in D_c$, there is some $i \in I_c$ such that $X_i \cap E_c$ and $X_i \cap D_d$ are both nonempty, so $(X_i \cap E_c)^h = X_i \cap E_d$ for some $h \in H$. Since h stabilizes Ψ, $E_c^h = E_d$, so $(X_j \cap E_c)^h = X_j \cap E_d$ for all $j \in I_c$. It follows that $I_c = I_d$ and that $\cup_{d \in D_c} E_d = \cup_{i \in I_c} X_i$ is the part of Y containing E_c, and we are done.

($\Leftarrow$) For each $i \in [r]$ we may write

$$X_i = \{x_{a_1 1}, x_{a_2 1}, \ldots, x_{a_m 1}, x_{a_1 2}, \ldots, x_{a_m 2}, \ldots, x_{a_m c_i}\}$$

with $a_1 < a_2 < \ldots < a_m$ and $x_{a_j b} \in E_{a_j}$. Set

$$h_i = (x_{a_1 1} x_{a_2 1} \ldots x_{a_m 1} x_{a_1 2} \ldots x_{a_m 2} \ldots x_{a_m c_i})$$

Let $h = \prod_{i=1}^{r} h_i$. Then $h \in G$ and $\langle h \rangle$ has orbits given by X, so $X \in \mathbf{P}$.

(2) ($\Rightarrow$) Let $W = [W_1; \ldots; W_s] \in \mathbf{P}$ and let $H = G \cap \prod_{i=1}^{s} S_{W_i}$ be the subgroup of G which is maximal with respect to having orbits given by W. Let $H^* = H \cap A_n$. If $H^* = H$ then $W \in \mathbf{P}^*$. Now assume $[H : H^*] = 2$. For each $i \in [s]$, fix $x_i \in W_i$. If the stabilizer H_{x_i} is not contained in A_n, then $[H^* : {H^*}_{x_i}] = [H : H_{x_i}]$ and W_i is an H^*-orbit. If $H_{x_i} \leq A_n$ then $[H^* : {H^*}_{x_i}] = \frac{1}{2}[H : H_{x_i}]$ and W_i splits into two H^*-orbits. It follows that $W \in \mathbf{P} \setminus \mathbf{P}^*$ if and only if $H \not\leq A_n$ and $H_x \leq A_n$ for some $x \in [n]$. Assume that these last two conditions hold, so $W \in \mathbf{P} \setminus \mathbf{P}^*$. We may assume that $x \in E_1 \cap W_1$ (and that $|W_1| > 1$).

If $|W_1 \cap E_1| > 2$, let $y, z \in (W_1 \cap E_1) \setminus \{x\}$. Then $(yz) \in H_x$, contradicting $H_x \leq A_n$. If $|W_i \cap E_j| > 1$ for some $(i, j) \neq (1, 1)$, let $y, z \in W_i \cap E_j$. Then $(yz) \in H_x$, again a contradiction. Therefore, $|W_1 \cap E_1| \leq 2$ and $|W_i \cap E_j| \leq 1$ for $(i, j) \neq (1, 1)$.

We first consider the case $|W_1 \cap E_1| = 2$. If $|W_i| = 1$ for all $i > 1$ then W is of type A. Now assume $|W_i| > 1$ for some $i > 1$. By part (1) of this lemma, $|W_1 \cap E_j| = 0$ or 2 for all $j \in [k]$. Since $|W_1 \cap E_j| \leq 1$ for $j > 1$, $W_1 \subseteq E_1$. It follows that E_1 is the union of W_1 and $n-2$ singletons, each of which is a part of W. If l is even then W is of type C. Now assume that l is odd. We may assume that $|W_2| > 1$. Since $|W_2 \cap E_j| \leq 1$ for all $j \in [k]$, we may assume that $W_2 \cap E_2$ and $W_2 \cap E_3$ are nonempty. Now using the notation from the proof of part (1), we have $I_2 = I_3$, so we may assume that $|W_i \cap E_2| = |W_i \cap E_3| = 1$ for $2 \leq i \leq l+1$. It follows that there exists a product of l transpositions in H which exchanges E_2 and E_3 and fixes x. Since l is odd, this contradicts $H_x \leq A_n$. Therefore, if $|W_1 \cap E_1| = 2$ then W is of type A or type C.

Finally, we consider the case $|W_1 \cap E_1| = 1$. In this case, $|W_i \cap E_j| = 0$ or 1 for all pairs (i, j). Let $h \in H$, and let $\overline{h} \in S_k$ give the action of h on the parts of Ψ. Each m-cycle of $\overline{h}$ determines l m-cycles of h. If l is even, then $h \in A_n$, and since h is arbitrary, $H \leq A_n$, a contradiction. Therefore, l is odd. If $|W_1| > 2$ then we may assume that $|W_1 \cap E_2| = |W_1 \cap E_3| = 1$, and as in the previous paragraph there exists a product of l transpositions in H_x exchanging E_2 and E_3, a contradiction. Therefore, $|W_1| = 2$ and we may assume $|W_1 \cap E_2| = 1$. By part (1), we may assume that $|W_i \cap E_1| = |W_i \cap E_2| = 1$ for $1 \leq i \leq l$. If $|W_i| = 1$ for $i > l$ then W is of type B. Otherwise, we may assume that $|W_{l+1} \cap E_3| = |W_{l+1} \cap E_4| = 1$. Again, we get a contradiction by producing a product of l transpositions in H_x which exchange E_3 and E_4. Therefore, if $|W_1 \cap E_1| = 1$ then W is of type B and we are done.

$(\Leftarrow)$ All partitions of types A,B, and C satisfy the condition given in (1) and are therefore in $\mathbf{P}$. If W is of type A, then the only subgroup of S_n having orbits given by W is generated by a transposition, so $W \notin \mathbf{P}^*$. If W is of type B, then the only subgroup of G with orbits given by W is generated by an involution which is the product of l transpositions, and since l is odd, $W \notin \mathbf{P}^*$. If W is of type C, then any $h \in G$ with $x^h = y$ is of the form $h = (xy)g$, where g acts on $\{E_2, \ldots, E_k\}$. Let $\overline{g} \in S_{k-1}$ describe this action of g. Any m-cycle of $\overline{g}$ determines l m-cycles of g. Since l is even, $g \in A_n$, so $h \notin A_n$. Therefore, no subgroup of G^* has orbits given by W, and $W \notin \mathbf{P}^*$. $\square$

Corollary 8.15 *Let* $\Psi = [E_1; \ldots; E_k]$ *be an equipartition of* $[n]$, *with* $|E_i| = l$. *Set* $\mathbf{P} = \mathcal{P}(G_\Psi, [n])$. *Then*

$$\mu_{\mathbf{P}}(\hat{0}, \hat{1}) = (-1)^{k+l}(k-1)!l!^{k-1}(l-1)!$$

Proof: Here we will allow $k = 1$ and proceed by induction on k. The case $k = 1$ is trivial, since $\mathbf{P} = \Pi_n$. Now assume $k > 1$ and set $E = [E_1; \bigcup_{i>1} E_i] \in \mathbf{P}$. We will use Weisner's Theorem. Let $\hat{0} < X = [X_1; \ldots; X_r] \in \mathbf{P}$ with $X \wedge_{\mathbf{P}} E = \hat{0}$. Assume (for contradiction) that $|X_i \cap E_1| > 1$ for some i, so $\{x, y\} \subseteq X_i \cap E_1$. Then $(xy) \in G_\Psi$ has orbits given by $Y = [\{x, y\}\,; n-2 \text{ singletons}]$, so $Y \in \mathbf{P}$ with $\hat{0} < Y \leq X \wedge_{\mathbf{P}} E$, a contradiction. Therefore, we may assume that $|X_i \cap E_1| = 1$ for $1 \leq i \leq l$ and $X_i \cap E_1 = \emptyset$ for $l < i \leq r$. Let $X_i \cap E_1 = \{x_i\}$ for $i \in [l]$. Then $X \wedge_{\Pi_n} E = [\{x_1\}\,; \ldots; \{x_l\}\,; X_1 \setminus x_1; \ldots; X_l \setminus x_l; X_{l+1}; \ldots; X_r]$. By Lemma 8.14, $X \wedge_{\Pi_n} E \in \mathbf{P}$, so $X \wedge_{\Pi_n} E = X \wedge_{\mathbf{P}} E$. Since $X \wedge_{\mathbf{P}} E = \hat{0}$, X has the following properties: $|X_i| = 2$ if $1 \leq i \leq l$, $|X_i| = 1$ if $l < i \leq r$, and by Lemma 8.14, $\cup_{i=1}^{l} X_i = E_1 \cup E_j$ for some $j > 1$. Note that any X with these properties is in $\mathbf{P}$. There are $(k-1)l!$ ways to choose such an X. Fix any such $X = [\{x_1, y_1\}\,; \ldots; \{x_l, y_l\}\,; n-2l \text{ singletons}]$, with $x_i \in E_1$, $y_i \in E_j$. Identifying the symbols x_i and y_i (and thereby the parts E_1 and E_j) determines a lattice isomorphism $\left[X, \hat{1}\right]_{\mathbf{P}} \cong \mathbf{Q}$, where $\mathbf{Q} = \mathcal{P}(G_\Phi, [n] \setminus E_1)$ and $\Phi = [E_2; \ldots; E_k]$. By induction, $\mu_{\mathbf{Q}}(\hat{0}, \hat{1}) = (-1)^{k+l-1}(k-2)!l!^{k-2}(l-1)!$, and by Theorem 2.5, $\mu_{\mathbf{P}}(\hat{0}, \hat{1}) = -(k-1)l!\mu_{\mathbf{Q}}(\hat{0}, \hat{1}) = (-1)^{k+l}(k-1)!l!^{k-1}(l-1)!$. □

Lemma 8.16 *Let* $\Psi = [E_1; \ldots; E_k]$ *be an equipartition of* $[n]$ *with* $|E_1| = l$. *Set* $G = G_\Psi$, $\mathbf{P} = \mathcal{P}(G, [n])$, $G^* = G \cap A_n$, $\mathbf{P}^* = \mathcal{P}(G^*, [n])$. *Let* $W \in \mathbf{P} \setminus \mathbf{P}^*$. *Then*

(1) If W *is of type A or type C, then* $\mu_{\mathbf{P}}(W, \hat{1}) = 0$.

(2) If W *is of type B, then* $\mu_{\mathbf{P}}(W, \hat{1}) = (-1)^{k+l+1}(k-2)!l!^{k-2}(l-1)!$

Proof: (2) follows immediately from Corollary 8.15 and its proof, so we need to prove (1). If W is of type A or type C, we may assume that $W_1 \subseteq E_1$ with $|W_1| = 2$, and

$|W_i \cap E_j| = 1$ for $(i,j) \neq (1,1)$. Let $E = [E_1; \cup_{i>1} E_i] \in \mathbf{P}$. Note that $W < E$. We will show that if $Y \in \mathbf{P}$ with $Y \wedge_{\mathbf{P}} E = W$, then $Y = W$. Theorem 2.5 will then give (1). Let $Y = [Y_1; \ldots; Y_n] \in \mathbf{P}$ with $Y > W$. We may assume that $W_1 \subseteq Y_1$. If $Y \leq E$ then $Y \wedge_{\mathbf{P}} E = Y > W$, so assume $Y \not\leq E$. Then $Y_1 \cap E_i \neq \emptyset$ for some $i > 1$. Since $|Y_1 \cap E_1| \geq 2$, $|Y_1 \cap E_i| \geq 2$ by Lemma 8.14. Since $W < Y$, there exist (by Lemma 8.14) $J \subseteq [k]$ and $R \subseteq [r]$ such that $1, i \in J$, $1 \in R$, and $\cup_{j \in J} E_j = \cup_{r \in R} W_r$. Set $F = \left[E_1; \cup_{j \in J \setminus \{1\}} E_j; \cup_{j \in [k] \setminus J} E_j\right]$, and let $Z = Y \wedge_{\Pi_n} F$. By Lemma 8.14, both F and Z are in $\mathbf{P}$. Since $W < Y$ and $W \leq F$, $W \leq Z$. Since Z has a part containing $Y_1 \cap E_i$ and W has no such part, $W < Z \leq Y \wedge_{\mathbf{P}} E$ and we are done. □

Corollary 8.17 *Let $\Psi = [E_1; \ldots; E_k]$ be an equipartition of $[n]$ with $|E_1| = l$. Let $G = G_\Psi$, $\mathbf{P} = \mathcal{P}(G, [n])$, $G^* = G \cap A_n$, $\mathbf{P}^* = \mathcal{P}(G^*, [n])$. Then*

(1) If l is odd, then $\mu_{\mathbf{P}}(\hat{0}, \hat{1}) - \mu_{\mathbf{P}^*}(\hat{0}, \hat{1}) = (-1)^{k+l} \frac{1}{2} k! l!^{k-1} (l-1)!$

(2) If l is even, then $\mu_{\mathbf{P}}(\hat{0}, \hat{1}) = \mu_{\mathbf{P}^*}(\hat{0}, \hat{1})$

Proof: Every W of type A or B in $\mathbf{P} \setminus \mathbf{P}^*$ is an atom in $\mathbf{P}$, and by Corollary 8.17 every W of type C satisfies $\mu_{\mathbf{P}}(W, \hat{1}) = 0$. It follows that $\mu_{\mathbf{P}^*}(X, \hat{1}) = \mu_{\mathbf{P}}(X, \hat{1})$ for every $X \in \mathbf{P}^*$. Therefore,

$$\mu_{\mathbf{P}}(\hat{0}, \hat{1}) - \mu_{\mathbf{P}^*}(\hat{0}, \hat{1}) = - \sum_{W \in \mathbf{P} \setminus \mathbf{P}^*} \mu_{\mathbf{P}}(W, \hat{1})$$

If l is odd, there are $\binom{k}{2} l!$ partitions W of type B in $\mathbf{P} \setminus \mathbf{P}^*$. The Corollary now follows from Lemmas 8.14 and 8.16. □

Definition 8.18 *(1) Let $\rho = [R_1; \ldots; R_k]$ and $\theta = [T_1; \ldots; T_l]$ be equipartitions of $[n]$. We call $\{\rho, \theta\}$ an orthogonal pair if $kl = n$ and $|R_i \cap T_j| = 1$ for all $i \in [k]$ and $j \in [l]$.*

(2) If $\{\rho, \theta\}$ is an orthogonal pair of equipartitions of $[n]$, then $G_{\rho,\theta} := G_\rho \cap G_\theta \leq S_n$.

(3) If $\{\rho = [R_1; \ldots; R_k], \theta = [T_1 : \ldots; T_l]\}$ is an orthogonal pair of equipartitions of $[n]$, then $A(\rho, \theta)$ is the $k \times l$ array whose entry in position (i,j) is $R_i \cap T_j$.

Let $\{\rho, \theta\}$ be an orthogonal pair of equipartitions of $[n]$. Using $A(\rho,\theta)$, we identify $[n]$ with $[k] \times [l]$ in the obvious way, and $G_{\rho,\theta}$ then consists of all elements of S_n which permute the rows and columns of $A(\rho,\theta)$. It is clear that $G_{\rho,\theta}$ is transitive, and since any permutation of the rows commutes with any permutation of the columns, we have $G_{\rho,\theta} \cong S_k \times S_l$. Moreover, if $K \leq S_k$ and $L \leq S_l$ have orbits given respectively by $A = [A_1; \ldots; A_r] \in \Pi_k$ and $B = [B_1; \ldots; B_s] \in \Pi_l$, then the orbits of $K \times L \leq G_{\rho,\theta}$ are given by $A \times B = [A_1 \times B_1; \ldots; A_r \times B_s] \in \Pi_{k \times l}$.

We will study orthogonal pairs $\{\rho, \theta\}$ such that $\gcd(k,l) = 1$. This condition is necessary for proving the following lemma, which describes the set of coatoms in $\mathcal{P}(G_{\rho,\theta}, [n])$.

Lemma 8.19 *Let $\{\rho = [R_1; \ldots; R_k]\,,\ \theta = [T_1; \ldots; T_l]\}$ be an orthogonal pair with $kl = n$ and $\gcd(k,l) = 1$. Set $G = G_{\rho,\theta}$ and $\mathbf{P} = \mathcal{P}(G,[n])$. For $I \subseteq [k]$, set $X_I = [\cup_{i \in I} R_i; \cup_{i \notin I} R_i]$ and for $J \subseteq [l]$, set $Y_J = [\cup_{j \in J} T_j; \cup_{j \notin J} T_j]$. Let $\mathcal{M}$ be the set of coatoms of $\mathbf{P}$. Then*

$$\mathcal{M} = \{X_I : \emptyset \neq I \subset [k]\} \cup \{Y_J : \emptyset \neq J \subset [l]\}$$

Proof: If we set $K = S_I \times S_{[k]\setminus I} \leq S_k$ and $L = S_l$, then the argument in above paragraph shows that $X_I \in \mathbf{P}$. The proof for Y_J is the same.

Now let $E = [E_1; \ldots; E_m] \in \mathbf{P}$. Define

$$I_1 = \{i \in [k] : E_1 \cap R_i \neq \emptyset\}\,, J_1 = \{j \in [l] : E_1 \cap T_j \neq \emptyset\}\,.$$

If $I_1 \neq [k]$ then $E \leq X_{I_1}$ by Lemma 8.14. Similarly, if $J_1 \neq [l]$ then $E \leq Y_{J_1}$. If $I_1 = [k]$ and $J_1 = [l]$ then by Lemma 8.14 there exist $c, d \in N$ such that $|E_1 \cap R_i| = c$ for all $i \in [k]$ and $|E_1 \cap T_j| = d$ for all $j \in [l]$. Therefore, $ck = |E_1| = dl$. Since $\gcd(k,l) = 1$, $c = l$ and $|X_1| = n$. This means $E = \hat{1}$ and we are done. $\square$

The example $n = 4$, $\rho = [\{1,2\}\{3,4\}]$, $\theta = [\{1,3\}\{2,4\}]$, $E = [\{1,4\}\{2,3\}] \in \mathcal{M}$

shows that Lemma 8.19 does not hold without the condition $\gcd(k,l)=1$.

We will use Lemma 8.19 to compute $\mu_{\mathbf{P}}(\hat{0},\hat{1})$ without giving an explicit description of $\mathbf{P}=\mathcal{P}(G_{\rho,\theta},[n])$. The main tool will be Lemma 2.13.

Lemma 8.20 *Let $\{\rho=[R_1;\ldots;R_k]\,,\ \theta=[T_1;\ldots;T_l]\}$ be an orthogonal pair with $kl=n$ and $\gcd(k,l)=1$. Set $G=G_{\rho,\theta}$ and $\mathbf{P}=\mathcal{P}(G,[n])$. Let $\mathbf{P}'$ be the meet semilattice generated by the coatoms of $\mathbf{P}$ with $\hat{1}$ adjoined. Then $\mathbf{P}'\cong\Pi_k\times\Pi_l$.*

Proof: Let $\hat{1}\neq X\in\mathbf{P}'$. Then by Lemma 8.19, $X=(\bigwedge_{i=1}^{a}X_{I_i})\wedge(\bigwedge_{j=1}^{b}Y_{J_j})$ for some $I_1,\ldots,I_a\subseteq[k]$ and $J_1,\ldots,J_b\subseteq[l]$. Define $\gamma_i=[I_i;[k]\setminus I_i]\in\Pi_k$ for each $i\in[a]$, and define δ_j similarly for each $j\in[b]$. Set $\Gamma=\bigwedge_{i=1}^{a}\gamma_i\in\Pi_k$ and $\Delta=\bigwedge_{j=1}^{b}\delta_j\in\Pi_l$. It is straightforward to verify that the map $X\mapsto(\Gamma,\Delta)$ is the desired isomorphism - note that X determines a partition of the rows of $A(\rho,\theta)$ which is given by Γ and a partition of the columns which is given by Δ. $\Box$

Corollary 8.21 *Let $\rho,\ \theta,\ G=G_{\rho,\theta},\ \mathbf{P}=\mathcal{P}(G,[n])$ be as in Lemma 8.20. Then*

$$\mu_P(\hat{0},\hat{1})=(-1)^{k+l}(k-1)!(l-1)!$$

Proof: This follows from Lemma 2.7, Lemma 8.20 and the fact that

$$\mu_{(P\times Q)}((w,x),(y,z))=\mu_P(w,x)\mu_Q(y,z)$$

(see [45], Proposition 3.8.2). $\Box$

When k and l are odd and relatively prime, we can also compute $\mu_{\mathbf{P}^*}(\hat{0},\hat{1})$, where $G^*=G_{\rho,\theta}\cap A_n$ and $\mathbf{P}^*=\mathcal{P}(G^*,[n])$. As above, we will use the array $A(\rho,\theta)$ to identify $[n]$ with $[k]\times[l]$.

Lemma 8.22 *Let $\{\rho=[R_1;\ldots;R_k]\,,\ \theta=[T_1;\ldots;T_l]\}$ be an orthogonal pair with k,l odd and $\gcd(k,l)=1$. Set $G=G_{\rho,\theta}$, $\mathbf{P}=\mathcal{P}(G,[n])$, $G^*=G\cap A_n$, $\mathbf{P}^*=\mathcal{P}(G^*,[n])$. Let $\mathcal{M}$ and $\mathcal{M}^*$ be the respective sets of coatoms of $\mathbf{P}$ and $\mathbf{P}^*$. Then G^* is transitive and $\mathcal{M}^*=\mathcal{M}$.*

Proof: Let $(g,h) \in G \cong S_k \times S_l$. Since k and l are odd, when we consider $G \leq S_n$, $(g,h) \in A_n$ if and only if $sgn_{S_k}(g) = sgn_{S_l}(h)$. Since $k,l > 2$, $A_k \times A_l \leq G^*$ is transitive. Recall from Lemma 8.19 that $\mathcal{M} = \{X_I : \emptyset \neq I \subset [k]\} \cup \{Y_J : \emptyset \neq J \subset [l]\}$. Let $\emptyset \neq I \subset [k]$, and set $K = S_I \times S_{[k]\setminus I} \leq S_k$ and $L = S_l$. Using the description of G given after Definition 8.18, it is straightforward to verify that $(K \times L) \cap G^*$ has orbits given by X_I, so $X_I \in \mathcal{M}^*$. A similar argument shows that $Y_J \in \mathcal{M}^*$. Since $\mathbf{P}^* \subseteq \mathbf{P}$, $\mathcal{M}^* = \mathcal{M}$. □

Corollary 8.23 *Let* $\{\rho = [R_1; \ldots; R_k]\,,\ \theta = [T_1; \ldots; T_l]\}$ *be an orthogonal pair with* k,l *odd and* $\gcd(k,l) = 1$. *Set* $G = G_{\rho,\theta}$, $\mathbf{P} = \mathcal{P}(G,[n])$, $G^* = G \cap A_n$, $\mathbf{P}^* = \mathcal{P}(G^*,[n])$. *Let* $\mathcal{M}$ *be the set of coatoms in* $\mathbf{P}$ *and define* $\mathbf{P}'$ *as in Lemma 8.20. Let* Ξ *be the set of all* $X \in \mathbf{P}$ *such that the only* $H \leq G$ *with orbits given by* X *is generated by an odd involution. Then*

$$\mu_{\mathbf{P}}(\hat{0},\hat{1}) - \mu_{\mathbf{P}^*}(\hat{0},\hat{1}) = -\sum_{X \in \Xi \cap \mathbf{P}'} \mu_{\hat{\mathbf{P}}}(X,\hat{1}).$$

Proof: Define

$$\Omega = \left\{\mathcal{J} \subseteq \mathcal{M} : \wedge_{\mathbf{P}} \{M \in \mathcal{J}\} \neq \hat{0}\right\},$$

and

$$\Omega^* = \left\{\mathcal{J} \in \Omega : \wedge_{\mathbf{P}^*} \{M \in \mathcal{J}\} = \hat{0}\right\}.$$

By Lemmas 8.22 and 2.6, $\mu_{\mathbf{P}}(\hat{0},\hat{1}) - \mu_{\mathbf{P}^*}(\hat{0},\hat{1}) = \sum_{\mathcal{J} \in \Omega^*} (-1)^{|\mathcal{J}|}$. Note that if $\mathcal{J} \in \Omega \setminus \Omega^*$ and $H \leq G$ is maximal with respect to having orbits given by $X = \wedge_{\mathcal{P}} \{M \in \mathcal{J}\}$, then $H \cap A_n \neq 1$, so $X \notin \Xi$. It follows that $\mathcal{J} \in \Omega^*$ if and only if $\wedge_{\mathbf{P}} \{M \in \mathcal{J}\} \in \Xi$. For $X \in \Xi$, set $\mathcal{M}_X = \{\mathcal{J} \subseteq \mathcal{M} : \wedge_{\mathbf{P}} \{M \in \mathcal{J}\} = X\}$. Then by Lemma 2.6, $\mu_{\mathbf{P}}(X,\hat{1}) = -\sum_{\mathcal{J} \in \mathcal{M}_X} (-1)^{|\mathcal{J}|}$. By Lemma 2.13, $\mu_{\mathbf{P}}(X,\hat{1}) = \mu_{\mathbf{P}'}(X,\hat{1})$ for all $X \in \Xi \cap \mathbf{P}'$ and $\mu_{\mathbf{P}}(X,\hat{1}) = 0$ for all $X \in \Xi \setminus \mathbf{P}'$. Therefore,

$$\mu_{\mathbf{P}}(\hat{0},\hat{1}) - \mu_{\mathbf{P}^*}(\hat{0},\hat{1}) = \sum_{X \in \Xi} \sum_{\mathcal{J} \in \mathcal{M}_X} (-1)^{|\mathcal{J}|} = -\sum_{X \in \Xi \cap \mathbf{P}'} \mu_{\hat{\mathbf{P}}}(X,\hat{1}).$$

□

We now determine the elements of Ξ.

Lemma 8.24 *Let* $\{\rho = [R_1; \ldots; R_k]\,,\ \theta = [T_1; \ldots; T_l]\}$ *be an orthogonal pair with* k, l *odd and* $\gcd(k, l) = 1$*. Set* $G = G_{\rho,\theta}$*,* $\mathbf{P} = \mathcal{P}(G, [n])$*,* $G^* = G \cap A_n$*,* $\mathbf{P}^* = \mathcal{P}(G^*, [n])$*. Set* $\{a_{ij}\} = R_i \cap T_j$*, and let* $X \in \mathbf{P}$*. Let* Ξ *be as in Corollary 8.23. Then* $X \in \Xi$ *if and only if* X *satisfies one of the following conditions:*

(a) There exist $c, d \in [k]$ *such that*

$$X = [\{a_{c1}, a_{d1}\}\,; \{a_{c2}, a_{d2}\}\,; \ldots; \{a_{cl}, a_{dl}\}\,; n - 2l \textit{ singletons}]\,.$$

(b) There exist $c, d \in [l]$ *such that*

$$X = [\{a_{1c}, a_{1d}\}\,; \{a_{2c}, a_{2d}\}\,; \ldots; \{a_{kc}, a_{kd}\}\,; n - 2k \textit{ singletons}]\,.$$

Proof: If X satisfies (a) then the only subgroup of G with orbits given by X is generated by $(a_{c1}a_{d1})\ldots(a_{cl}a_{dl})$. Since l is odd, $X \in \Xi$. A similar argument shows that if X satisfies (b) then $X \in \Xi$.

Now let $\hat{0} < X \in \mathbf{P}'$, and let $X \mapsto (\Gamma \in \Pi_k, \Delta \in \Pi_l)$ be the map described in the proof of Lemma 8.20. Let $K \leq S_k$ and $L \leq S_l$ be the respective stabilizers of Γ and Δ. Then $K \times L \leq G$ has orbits given by X, so $K \times L$ is generated by an odd involution. It follows that one of Γ, Δ is an atom in the partition lattice containing it, and the other is $\hat{0}$. Therefore, (a) or (b) holds. □

Corollary 8.25 *Let* $\{\rho = [R_1; \ldots; R_k]\,,\ \theta = [T_1; \ldots; T_l]\}$ *be an orthogonal pair with* k, l *odd and* $\gcd(k, l) = 1$*. Set* $G = G_{\rho,\theta}$*,* $\mathbf{P} = \mathcal{P}(G, [n])$*,* $G^* = G \cap A_n$*,* $\mathbf{P}^* = \mathcal{P}(G^*, [n])$*. Then*

$$\mu_{\mathbf{P}}(\hat{0}, \hat{1}) - \mu_{\mathbf{P}^*}(\hat{0}, \hat{1}) = \frac{1}{2}(k!(l-1)! + l!(k-1)!).$$

Proof: Let $X \in \Xi$ satisfy condition (a) of Lemma 8.24, and let $X \mapsto (\Gamma, \Delta)$ be the map described above. Then $\Gamma = [\{c, d\}\,; k - 2 \text{ singletons}]$ and $\Delta = \hat{0}$. By Lemma 8.20,

$\mu_{\hat{\mathbf{P}}}(X, \hat{1}) = \mu_{\Pi_k}(\Gamma, \hat{1})\mu_{\Pi_l}(\hat{0}, \hat{1}) = -(k-2)!(l-1)!$. There are $\binom{k}{2}$ $X \in \Xi$ satisfying (a). Similarly, if $X \in \Xi$ satisfies condition (b) of Lemma 8.24 then $\mu_{\mathbf{P}'}(X, \hat{1}) = -(l-2)!(k-1)!$, and there are $\binom{l}{2}$ such X. The corollary now follows from Corollary 8.23. □

8.3 The O'Nan-Scott Theorem and primitive almost simple groups of prime power degree

We will calculate $\mu(1, S_n)$ for those n for which it is possible to do so with a two part procedure. The first part involves obtaining the results given in Theorem 8.4. This reduces the calculation of $\mu(1, S_n)$ to the calculation of the sum of the Möbius numbers of the primitive proper subgroups of S_n which contain an odd involution. In order to have any hope of carrying out this second part, one must have some description of these primitive subgroups. Such a description is given by the O'Nan-Scott Theorem. The version given below will suffice for our purposes. A more detailed version, along with a proof, is given in [31]. To determine the elements of $\mathcal{P}_n$ when n is prime or a power of two, we will use a theorem of Guralnick (see [19]) which lists all possible simple groups S such that there is a primitive permutation group of prime power degree containing a minimal normal subgroup isomorphic to S. We begin our discussion of the O'Nan-Scott Theorem with a description of wreath products.

Definition 8.26 *Let H be any group and let $G \leq S_m$ be any permutation group. The wreath product $G[H]$ is a semidirect product, whose kernel is a direct product of m copies of H, and whose complement is isomorphic to G. This complement acts on the kernel by permuting the components of the direct product as G permutes $[n]$. In other words, if we write an element of $G[H]$ as (g, v), where $g \in G$ and $v = (h_1, \ldots, h_m) \in H^m$, then multiplication in the wreath product is determined by the relation*

$$(g, 1)(1, (h_1, \ldots, h_m))(g^{-1}, 1) = (1, (h_{1^g}, \ldots, h_{m^g})).$$

There are two natural actions for a wreath product $G[H]$, one of which is never primitive and one of which frequently is.

Definition 8.27 *Let $G \leq S_k$ and $H \leq S_l$ be permutation groups.*

(1) The imprimitive action of $G[H]$ on the Cartesian product $[k] \times [l]$ is defined by extending the following definitions for the actions of G and H to the entire group.

$$(i,j)^{(1,(h_1,\ldots,h_k))} := (i, j^{h_i}),$$

and

$$(i,j)^{(g,1)} := (i^g, j).$$

(2) The product action of $G[H]$ on the Cartesian product of k copies of $[l]$ is defined by extending the following actions of G and H to the entire group.

$$(i_1,\ldots,i_k)^{(1,(h_1,\ldots,h_k))} := (i_1^{h_1},\ldots,i_k^{h_k}),$$

and

$$(i_1,\ldots,i_k)^{(g^{-1},1)} := (i_{1^g},\ldots,i_{k^g}).$$

It is well known and straightforward to show that the imprimitive and product actions are well defined. We will say that $H \leq S_n$ has the product action if $n = k^l$ and $[n]$ can be identified with $[k]^l$ in such a way that the embedding of H in S_n can be extended to an embedding of $S_k[S_l]$ in S_n whose image has the product action. The results in the lemma below are also well known and appear in [7].

Lemma 8.28 *(1) Let $G \leq S_n$ be imprimitive. Then there exist $1 < k, l < n$ such that $[n]$ can be identified with $[k] \times [l]$ in so that the embedding of G in S_n can be extended to an embedding of $S_k[S_l]$ whose image has the imprimitive action.*

(2) Let $G \leq S_k$ be transitive and $H \leq S_l$ be primitive. If the stabilizer of a point in H is nontrivial, then the product action of $G[H]$ on $[l]^k$ is primitive.

Part (1) of the above lemma will be used implicitly throughout this chapter. We can now state a version of the O'Nan-Scott Theorem which will be sufficient for our purposes.

Theorem 8.29 (O'Nan-Scott) *Let $G \leq S_n$ be primitive. Then one of the following cases holds.*

(1) G is affine. That is, $n = p^d$ for some prime p and positive integer d, and $[n]$ is identified with a d-dimensional vector space V over $\mathbf{F}_p$. G contains a subgroup isomorphic to V (which we will call V) acting by translation, that is $v^w = v + w$ for all $v, w \in V$. Furthermore, G is contained in the semidirect product of V by $Aut(V) \cong GL(V)$, and the image of G under the natural projection of this semidirect product onto $GL(V)$ acts irreducibly on V.

(2) G is almost simple. That is, there exists a finite simple group S and embeddings $S \hookrightarrow G \hookrightarrow Aut(S)$.

(3) G has the diagonal action. In this case, there exist some nonabelian simple group S and positive integer a such that $n = |S|^a$ and G contains a normal subgroup N which is a direct product of $a + 1$ copies of S.

(4) G has the product action, so $n = k^l$ with $k, l > 1$ and G is as defined above.

(5) G has the twisted wreath action. In this case, there exists some nonabelian simple group S and some integer $a > 1$ such that $n = |S|^a$ and G contains a normal subgroup which is a direct product of a copies of S.

Now we state Guralnick's theorem on primitive almost simple groups of prime power degree.

Theorem 8.30 ([19], Theorem 1) *Let S be a nonabelian simple group and let H be a subgroup of S of index p^a, where p is prime. Then one of the following cases holds.*

(1) $S = A_n$, $H \cong A_{n-1}$ and $n = p^a$.

(2) $S = L_d(q)$, H is the stabilizer of a 1-space or a $(d-1)$-space in the action of S on its natural projective space, d is prime and $p^a = \frac{q^d-1}{q-1}$.

(3) $S = L_2(11)$, $H \cong A_5$ and $p^a = 11$.

(4) $S = M_{23}$, $H \cong M_{22}$ and $p^a = 23$.

(5) $S = M_{11}$, $H \cong M_{10}$ and $p^a = 11$.

(6) $S = U_4(2) \cong PSp_4(3)$ and $p^a = 27$.

Since an embedding of a simple group S in S_{p^a} as a transitive subgroup is determined by the action of S by translation on the cosets of a subgroup of S of index p^a, the above theorem determines all transitive actions of prime power degree for nonabelian simple groups. We will also make use of the following corollary.

Corollary 8.31 ([19], Corollary 2) *If S is a transitive nonabelian simple subgroup of S_{p^a} with p prime, then S is primitive.*

Guralnick actually shows that all the groups described in the Theorem are 2-transitive, except in case (6). We will only need the fact that they are primitive.

We will examine the cases listed in Theorem 8.4. It follows from the classification of finite simple groups that cases (3) and (5) of the O'Nan-Scott Theorem cannot occur for these degrees.

8.4 The case $n = p$

If $n = p$ is prime, then $\mathcal{C}_n = \mathcal{P}_n$ and it follows trivially from Proposition 8.3 that $\mu(1, S_n) = \frac{n!}{2} - \sum_{H \in \mathcal{P}_n} \mu(1, H)$. We next describe $\mathcal{P}_n$. From Theorem 8.30 and Corollary 8.31, we get the following Lemma.

Lemma 8.32 *Let p be a prime and let $H \leq S_p$ be primitive with $S \leq H$ a nonabelian simple normal subgroup. Then one of the following cases holds:*

(1) $S = A_p$.

(2) $S = L_d(q)$ acting on the 1-spaces or hyperplanes of its natural projective space, with d prime and $p = \frac{q^d-1}{q-1}$.

(3) $S = L_2(11)$ acting on cosets of A_5.

(4) S is one of the Mathieu groups M_{23} or M_{11}.

Proof: This follows immediately from Theorem 8.30 and Corollary 8.31. □

Corollary 8.33 *Let p be a prime. Then any transitive proper subgroup of S_p which is not contained in A_p has a normal p-subgroup.*

Proof: We must examine cases (2),(3),(4) of Lemma 8.32. Since the Mathieu groups of case (4) are complete (see [18], pages 40,43) and the action of $L_2(11)$ on the cosets of A_5 does not extend to $PGL_2(11)$ (see [14], (260)), the only interesting case is (2). In this case, the action of $L = L_2(q)$ can be extended to the semidirect product $AP \leq Aut(L)$, where $A \cong Aut(\mathbf{F}_q)$ and $P \cong PGL_2(q)$, but not to $Aut(L)$ if $d > 2$ (see [18], section 3.9, and note that a graph automorphism of $L_d(q)$ maps the stabilizer of a 1-space to the stabilizer of a hyperplane). First assume $d > 2$. If A contains an involution, then q is a square, from which it follows easily that $\frac{q^d-1}{q-1}$ is composite, a contradiction. Therefore, $[AP : P] = |A|$ is odd. Since d is odd, so is $[P : L] = gcd(d, q-1)$. Therefore, $[AP : L]$ is odd, and since $L \leq A_p$, $AP \leq A_p$. If $d = 2$, then $p = q + 1$ is a Fermat prime, so $q = 2^{2^a}$. In this case, $P = L$, so $AP = AL$. We will show that either $A \leq A_p$ or $AL = S_p$. Let x generate $A \cong Z_{2^a}$. For $0 \leq b \leq a$, the fixed points of x^{2^b} on the projective line over $\mathbf{F}_q$ are those spanned by $(0,1)$ and $(1,\alpha)$ with $\alpha \in \mathbf{F}_{2^{2^b}}$. Therefore, x has 3 fixed points and $\frac{2^{2^b}-2^{2^{b-1}}}{2^b}$ 2^b-cycles for $1 \leq b \leq a$. It follows that $x \in A_p$ unless $a = 2$, in which case $p = 5$, $L = L_2(4) \cong A_5$, and $AL = S_5$. Now the only transitive proper subgroups of S_p which are not almost simple are affine and contain a normal p-subgroup (see [6], Chapter X Theorem XIII and Chapter XVI, Theorem VII), and we are done. □

Lemma 8.34 *Let $\mathcal{TS}_p$ be the set of transitive subgroups of S_p which contain a normal p-subgroup and which contain an odd involution. Then*

$$\sum_{H \in \mathcal{TS}_p} \mu(1, H) = 0$$

Proof: Any $H \in \mathcal{TS}_p$ is contained in exactly one of $(p-2)!$ subgroups isomorphic to $Z_{p-1}Z_p$. Let $N = AP$ be one such subgroup, so $N = N_{S_p}(P)$ with $|P| = p$. Then N contains one conjugacy class of involutions, each of which fixes a point. If $p \equiv 1 \pmod 4$ then these involutions are contained in A_p and $\mathcal{TS}_p = \emptyset$. Now assume $p \equiv 3 \pmod 4$. For each $k \in \mathbf{N}$ such that $2|k|(p-1)$, N contains a unique subgroup $BP \in \mathcal{TS}_p$ with $|BP| = kp$ (and all subgroups of N contained in $\mathcal{TS}_p$ are of this form). BP contains p complements to P, all of which are maximal in BP and cyclic of order k. By Theorem 2.4, $\mu(1, BP) = -p\mu(k)$. Therefore,

$$\sum_{H \in \mathcal{TS}_p} \mu(1, H) = -(p-2)!p \sum_{2|k|(p-1)} \mu(k) = 0$$

The last equality above holds because $\frac{p-1}{2}$ is odd, so that $\sum_{2|k|(p-1)} \mu(k) = -\sum_{k|\frac{p-1}{2}} \mu(k) = 0$. □

Theorem 8.35 *Let p be an odd prime. Then*

$$\mu(1, S_p) = \frac{p!}{2}$$

Proof: This follows immediately from the above results. □

8.5 The case $n = 2p$

Stanley's question is answered in this section. We note at this point that several lemmas from this section and the next one were proved previously by Lucchini. Namely, Lemmas 8.38, 8.53, 8.56 and Proposition 8.52 are either stated in or follow immediately from the proofs and results in [33].

Definition 8.36 *Let $n = 2p$, p an odd prime. An equipartition $\Psi \in \Pi_n$ is of type D if Ψ has 2 parts of size p. Ψ is of type E if Ψ has p parts of size 2.*

Clearly every equipartition of $[n]$ is of type D or type E. Our first step is to determine $\sum_{H \leq G_\Psi, H \in \mathcal{I}_n} \mu(1, H)$ for each equipartition $\Psi \in \Pi_n$. Note that if $H \leq G_\Psi$ for some equipartition Ψ, then H is of course imprimitive, so $H \in \mathcal{I}_n$ if and only if $H \in \mathcal{C}_n$.

Lemma 8.37 *Let Ψ be an equipartition of $[n = 2p]$, p an odd prime. Set $G = G_\Psi$, $\mathbf{P} = \mathcal{P}(G, [n])$, $G^* = G \cap A_n$, $\mathbf{P}^* = \mathcal{P}(G^*, [n])$. Then*

(1) If Ψ is of type D, then $\sum_{H \leq G, H \in \mathcal{I}_n} \mu(1, H) = -p!(p-1)!$

(2) If Ψ is of type E, then $\sum_{H \leq G, H \in \mathcal{I}_n} \mu(1, H) = 0$

Proof: In either case, $\sum_{H \leq G, H \in \mathcal{I}_n} \mu(1, H) = \mu_{\mathbf{P}}(\hat{0}, \hat{1}) - \mu_{\mathbf{P}^*}(\hat{0}, \hat{1})$ by Corollary 8.10. The lemma now follows immediately from Corollary 8.17. □

We next determine which transitive subgroups of S_{2p} stabilize more than one equipartition.

Lemma 8.38 *Let $n = 2p$, p an odd prime, and let $H \leq S_n$ be transitive. H stabilizes more than one equipartition of $[n]$ if and only if one of the following two cases holds:*

(1) There exists an orthogonal pair $\{\sigma, \tau\}$ such that the only equipartitions stabilized by H are σ and τ.

(2) $H \cong D_{2p}$ is regular, and H stabilizes one partition σ of type D, and p partitions $\tau_1, \tau_2, \ldots, \tau_p$ of type E, all of which are orthogonal to σ.

Proof: Assume $H \leq S_n$ is transitive and stabilizes more than one equipartition. Since H is transitive, there is some $h \in H$ with $|h| = p$. If $|supp(h)| = p$, then the only equipartition stabilized by h is $[supp(h); [n] \setminus supp(h)]$. Therefore, $supp(h) = [n]$ and we may assume $h = (12 \ldots p)(p+1 \ldots 2p)$. The only equipartitions stabilized by h are

$$\begin{aligned} \sigma &= [\{1, \ldots, p\}; \{p+1, \ldots, 2p\}], \\ \tau_1 &= [\{1, p+1\}; \{2, p+2\}; \ldots; \{p, 2p\}], \end{aligned}$$

$$\begin{aligned}\tau_2 &= [\{1, p+2\}; \{2, p+3\}; \ldots; \{p, p+1\}], \\ \ldots & \\ \tau_p &= [\{1, 2p\}; \{2, p+1\}; \ldots; \{p, 2p-1\}].\end{aligned}$$

Therefore, if (1) does not hold, H stabilizes τ_i and τ_j for some $i \neq j$. For each τ_i let $g_i \in S_n$ be the involution whose 2-cycles are the parts of τ_i, so for example $g_1 = (1\ p+1)(2\ p+2)\ldots(p\ 2p)$. Then the stabilizer $G_{\tau_i} = C_{S_n}(g_i)$, and for any i, j, $G_{\tau_i} \cap G_{\tau_j} = C_{S_n}(< g_i, g_j >)$. Now for any $i \neq j$, $< g_i, g_j >=< g_k : k \in [p] >\cong D_{2p}$ is a right regular representation of D_{2p} with respect to some numbering of the elements of D_{2p}. It is well known that the centralizer in S_n of such a group is the left regular representation of D_{2p} with respect to the same numbering (see [7], p.3), so (2) holds. □

Given the above lemmas, we will compute $\sum_{H \in \mathcal{I}_n} \mu(1, H)$ using inclusion-exclusion. We require one more fact.

Lemma 8.39 *Let $\{\sigma, \tau\}$ be an orthogonal pair of equipartitions of $[n = 2p]$. Let $G = G_{\sigma,\tau}$. Then $G \cap A_n$ is not transitive.*

Proof: Let $\sigma = [B_1; B_2]$, $\tau = [C_1; \ldots; C_p]$. Define $A(\sigma, \tau) = (a_{ij})$ with $\{a_{ij}\} = B_i \cap C_j$ as before. Note that if $g \in G$ fixes B_1 (setwise), then g has the same cycle shape on B_2 as it does on B_1, so $g \in A_n$. Now let $h = \prod_{j=1}^{p}(a_{1j} a_{2j})$. Since p is odd, $h \in G \setminus A_n$. Every $k \in G$ with $B_1^k = B_2$ is of the form $k = hg$, where g fixes B_1. Therefore, any such k is not in A_n. □

Theorem 8.40 *Let $n = 2p$, p an odd prime. Then*

$$\mu(1, S_n) = (-1)^{n-1}\frac{n!}{2} - \sum_{H \in \mathcal{P}_n} \mu(1, H)$$

Proof: By Proposition 8.3, it is sufficient to show that $\sum_{H \in \mathcal{I}_n} \mu(1, H) = 0$. Let $\mathcal{E}$ be the set of equipartitions of $[n]$ and let $\mathcal{O}$ be the set of orthogonal pairs of equipartitions of $[n]$. Then by Lemma 8.38

$$\sum_{H\in\mathcal{I}_n}\mu(1,H)=\sum_{\Psi\in\mathcal{E}}\sum_{H\leq G_\Psi,H\in\mathcal{I}_n}\mu(1,H)-\sum_{\{\sigma,\tau\}\in\mathcal{O}}\sum_{H\leq G_{\sigma,\tau},H\in\mathcal{I}_n}\mu(1,H)$$

Indeed, if $H\in\mathcal{I}_n$ stabilizes an orthogonal pair and no other partitions then $\mu(1,H)$ is counted twice in the first sum and once in the second sum, and if $H\cong D_{2p}$ is regular then $\mu(1,H)$ is counted $p+1$ times in the first sum and p times in the second sum.

Now there are $\frac{1}{2}\binom{2p}{p}$ equipartitions of type D in $\mathcal{E}$, so by Lemma 8.37

$$\sum_{\Psi\in\mathcal{E}}\sum_{H\leq G_\Psi,H\in\mathcal{I}_n}\mu(1,H)=-\frac{1}{2}\binom{2p}{p}p!(p-1)!$$

Also, $|\mathcal{O}|=\frac{1}{2}\binom{2p}{p}p!$, so by Corollary 8.21 and Lemma 8.39

$$\sum_{\{\sigma,\tau\}\in\mathcal{O}}\sum_{H\leq G_{\sigma,\tau},H\in\mathcal{I}_n}\mu(1,H)=-\frac{1}{2}\binom{2p}{p}p!(p-1)!$$

and we are done. □

We now calculate $\sum_{H\in\mathcal{P}_n}\mu(1,H)$. By the O'Nan-Scott theorem, any $H\in\mathcal{P}_n$ is almost simple. Liebeck and Saxl have determined all the possibilities for $soc(H)$ whenever H is an almost simple primitive permutation group of degree mp, where p is prime and $m<p$ ([32]). By examining each case to see if it is possible that $m=2$, we get the following theorem.

Theorem 8.41 *Let $n=2p$, p an odd prime, and let $H\leq S_n$ be primitive. Let $S=soc(H)$, the nonabelian simple normal subgroup of H. If $S\neq A_n$, then one of the following cases holds:*
(a) $n=10$, $S=A_5$ acting on $\binom{[5]}{2}$.
(b) $n=q+1$, $q=r^{2^a}$ for some odd prime r, $S=L_2(q)$ acting on 1-spaces.
(c) $n=22$, $S=M_{22}$.

Proof: We will go down the list of possibilities for S given in [32] and determine which of the given degrees can be $2p$. The cases where it is clearly impossible that $n=2p$ will be listed without comment.

(1) $S = A_c$ acting on 2-sets, $n = \binom{c}{2}$ and $p = c$ or $c-1$. If $p = c$ then $\frac{c-1}{2} = 2$, so $c = 5$ and case (a) holds. If $p = c-1$ then $c = 4$, but A_4 is not simple.

(2) $S = A_7$ acting on 3-sets and $n = 35$.

(3) $S = A_7$ acting on 1-spaces in a 4-dimensional space over $\mathbf{F}_2$ and $n = 15$.

(4) $S = L_d(q)$ acting on 1-spaces or $(d-1)$-spaces from its natural projective space with $d \geq 2$ and $n = \frac{q^d-1}{q-1}$. Say $d = kl$ with $k, l > 1$. Then $n = \frac{q^k-1}{q-1}\sum_{i=0}^{l-1} q^{ik}$. Both of these two factors are greater than two. Thus we may assume d is prime. If d is odd then n is odd, so we may assume $d = 2$ and q is odd. Write $q = r^m$. If $m = kl$ with $k > 1$ odd, then $n = (r^k+1)\sum_{i=0}^{l-1}(-1)^i q^{ik}$. Again both factors are greater than two. Thus case (b) above holds.

(5) $S = L_d(q)$ acting on 2-spaces or $(d-2)$-spaces from its natural projective space, $n = \frac{(q^d-1)(q^{d-1}-1)}{(q^2-1)(q-1)}$, $p | \frac{q^d-1}{q-1}$ and $d \geq 4$.

(6) $S = L_7(q)$ acting on 3-spaces or 4-spaces from its natural projective space, $n = \frac{(q^7-1)(q^6-1)(q^5-1)}{(q^3-1)(q^2-1)(q-1)}$ and $p | \frac{q^7-1}{q-1}$.

(7a) $S = L_d(q)$ acting on incident point-hyperplane pairs from its natural projective space, $n = \frac{(q^d-1)(q^{d-1}-1)}{(q-1)^2}$, $p | \frac{q^d-1}{q-1}$ and $d \geq 3$.

(7b) $S = L_d(q)$ acting on nonincident point-hyperplane pairs from its natural projective space, $n = \frac{q^{d-1}(q^{d-1}-1)}{q-1}$, $p | \frac{q^d-1}{q-1}$ and $d \geq 3$.

(8) $S = L_4(3)$ acting on cosets of a subgroup which is an extension of $PSp_4(3)$ by Z_2 and $n = 117$.

(9) $S = PSp_{2d}(q)$ acting on 1-spaces (or totally isotropic 2-spaces if $d = 2$) from its natural projective space, $n = \frac{q^{2d}-1}{q-1}$, $p|q^d+1$ and d is a power of two. Here we have $\frac{q^d-1}{q-1}|2$, which is impossible unless $d = 1$. In that case, $S \cong L_2(q)$ (see [2], p.253), and the action on the natural projective space is the same as that of $L_2(q)$, since all 1-spaces are isometric. Thus case (b) above holds.

(10) $S = Sp_{2d}(q)$ acting on one of its orbits on quadratic forms for its natural projective space, q is even, $n = \frac{q^d(q^d+1)}{2}$ or $\frac{q^d(q^d-1)}{2}$, and $p = q^d+1$ or q^d-1. Furthermore, if $p = q^d+1$ then d is a power of two and if $p = q^d-1$ then $q = 2$ and d is prime. Here we have $\frac{q^d}{2} = 2$, so either $q = d = 2$ or $q = 4$ and $d = 1$. In the first case, we have $S = Sp_4(2)$. This group is not simple, but its commutator subgroup is isomorphic to $L_2(9)$ (see [2], p.253). Now the only subgroup of index ten in $L_2(9)$ is the stabilizer of a 1-space in the natural action (see [14], (260)), so case (b) above holds. In the second case, we have $S = Sp_2(4) \cong A_5$ (again [2], p.253) and $n = 10$. Any subgroup of index 10 in A_5 normalizes a Sylow 3-subgroup, so there is only one conjugacy class of primitive subgroups isomorphic to A_5 in S_{10}. Thus case (a) above must hold.

(11) $S = Sp_4(q)$ acting on the cosets of a subgroup isomorphic to $S_2[SL_2(q)]$, q is even, $n = \frac{q^2(q^2+1)}{2}$ and $p = q^2+1$. Here we must have $q = 2$, but as in (10), $Sp_4(2)$ is not simple.

(12) $S = U_d(q)$ acting on singular 1-spaces from its natural projective space, $n = \frac{(q^d+1)(q^d-1)}{q^2-1}$, $p|\frac{q^d+1}{q+1}$ and $d \geq 3$ is prime.

(13) $S = P\Omega_{2d+1}(q)$ acting on singular 1-spaces from its natural projective space, $n = \frac{(q^d-1)(q^{d-1}+1)}{q-1}$ and $p = \frac{q^d-1}{q-1}$. Here $q^{d-1}+1 = 2$, so $d = 1$, which contradicts p prime.

(14) $S = \Omega^+_{2d}(2)$ acting on nonsingular 1-spaces from its natural projective space, $n = 2^{d-1}(2^d-1)$, $p = 2^d-1$ and $d > 4$ is prime.

(15a) $S = P\Omega^-_{2d}(q)$ acting on singular 1-spaces from its natural projective space, $n = \frac{(q^d+1)(q^{d-1}-1)}{q-1}$, $p|q^d+1$ and d is a power of two. Since $\frac{q^{d-1}-1}{q-1}|2$, we have $d = 2$. However, $P\Omega^-_4(2) \cong L_2(q) \times L_2(q)$ is not simple (see [2], p.253), so this case cannot hold.

(15b) $S = P\Omega^-_{2d}(q)$ acting on singular 1-spaces from its natural projective space, $n = q^{d-1}(q^d+1)$, $p|q^d+1$ and d is a power of two. Here either $d = 1$ or $q = d = 2$. However, neither $P\Omega^-_2(q)$ nor $P\Omega^-_4(2)$ is simple ([2], p.253), so this case cannot hold.

(16) $S = P\Omega_{2d+1}(q)$ acting on singular 1-spaces from its natural projective space, $n = \frac{q^{2d}-1}{q-1}$, $p|q^d+1$ and d is a power of two. Here we must have $d = 1$, so $S = P\Omega_3(q) \cong L_2(q)$ acting on $q+1$ singular 1-spaces. The only primitive action of $L_2(q)$ on $q+1$ points is its natural action on 1-spaces from its natural 2-dimensional projective space (see [14], (260)), so case (b) above holds.

(17a) $S = L_2(q)$ acting on the cosets of a dihedral subgroup of order $q+1$ or $q-1$, $n = \binom{q}{2}$ or $\binom{q+1}{2}$, $p = q$ if q is odd, and $p = q+1$ or $q-1$ if q is even. If q is odd, we have $\frac{q+1}{2} = 2$ or $\frac{q-1}{2} = 2$. In the first case, $S = L_2(5) \cong A_5$ and $n = 10$. As in (10), case (a) holds. In the second case, $q = 3$, but $L_2(3) \cong A_4$ is not simple.

(17b) $S = L_2(q)$ acting on the cosets of a subgroup isomorphic to $PGL_2(\sqrt{q})$, q is a square, $n = \frac{\sqrt{q}(q+1)}{gcd(2,q-1)}$ and $p|q+1$. Here we must have $q = 4$, so $S = L_2(4) \cong A_5$ and $n = 10$. Again, case (a) must hold.

(17c) $S = L_2(q)$ acting on the cosets of a subgroup isomorphic to A_5, $n = \frac{q(q^2-1)}{120}$ and $p = q$.

(17d) $S = L_2(q)$ acting on the cosets of a subgroup isomorphic to S_4, $n = \frac{q(q^2-1)}{48}$ and $p = q$.

(17e) $S = L_2(q)$ acting on the cosets of a subgroup isomorphic to A_4, $n = \frac{q(q^2-1)}{24}$, $p = q$ and $q \equiv 3, 5 \bmod 8$. Note that if $\frac{q^2-1}{24} = 2$ then $q \not\equiv 3, 5 \bmod 8$.

(18) $S = Sz(q)$, $n = q^2 + 1$ with $q = 2^{2m+1}$.

(19) $S = {}^2G_2(q)$, $n = q^3 + 1$ and $p | q^2 - q + 1$.

(20) $S = M_{24}$, $n = 276$ and $p = 23$.

(21) $S = M_{23}$, $n = 253$ or 506 and $p = 23$.

(22) $S = M_{22}$, $n = 22$ or 77 and $p = 11$. Here case (c) holds if $n = 22$.

(23) $S = M_{12}$, $n = 66$ and $p = 11$.

(24) $S = J_1$, $n = 266$ and $p = 19$.

(25) $S = Co_3$, $n = 276$ and $p = 23$.

Note that there is a misprint in [32]. The groups listed as $P\Omega^-$ in (15) above are listed as $P\Omega^+$ in the paper. All cases given in [32] have been examined, and the proof is complete. □

We can determine $\mu(1, S_n)$ for all $n = 2p$ through careful examination of the groups described in Theorem 8.41. We begin with case (c) from the above lemma.

Lemma 8.42 *Let $H \cong Aut(M_{22})$. Then*

(1) H has one conjugacy class of maximal subgroups of index 22.

(2) If K is a maximal subgroup of index 22 in H, then the image of the homomorphism from H to S_{22} determined by the action of H on the cosets of K contains an odd involution.

(3) $\mu(1,H) = -|H|$.

Proof: The first claim follows immediately from information on page 42 of [18], since M_{22} contains a unique conjugacy class of subgroups of index 22. The second claim follows from examination of the permutation character for the action of H on K, as given in [10], where it is shown that the image of H in S_{22} contains an involution with no fixed points. The third claim was proved by Pfeiffer using the GAP software ([38]). $\square$

Lemma 8.43 *Let $L \cong L_2(r^{2^a})$ and let $A = Aut(L)$. Let $P \cong PGL_2(r^{2^a}) \leq A$. If $L \leq H \leq A$ with $[H : H \cap P] > 2$ then $\mu(1,H) = 0$.*

Proof: It is well known that $A/P \cong Z_{2^a}$ (see [18], Section 7), so $H/H \cap P$ is a cyclic 2-group, as is any complement C to $H \cap P$ in H. If $|C| > 2$ then $|C|$ is not squarefree and $\mu(1,C) = 0$. The lemma follows from Theorem 2.4. $\square$

In the notation of the above lemma, it remains to examine groups H satisfying $L \leq H \leq \langle f \rangle P$, where f is the the automorphism of L induced by an automorphism of $\mathbf{F}_{r^{2^a}}$ of order 2. Since $\langle f \rangle P/L \cong V$ (the Klein 4-group), these groups are $L, P, \langle f \rangle L, X$, and $\langle f \rangle P$. Here X satisfies $[X : L] = 2$ and $X \notin \{P, \langle f \rangle L\}$.

Lemma 8.44 *Let $q = r^{2^a}$, where r is an odd prime. Let $L = L_2(q)$ and $P = PGL_2(q)$. Let f be the automorphism of P induced by the automorphism of $\mathbf{F}_q$ having order two. Let X satisfy $L < X < \langle f \rangle P$ with $X \neq P$ or $\langle f \rangle L$. Then $\mu(1,X) = \mu(1, \langle f \rangle P) = 0$.*

Proof: Assume (for contradiction) that C is a complement to L in X. Then C is generated by an involution of the form fx, $x \in P \setminus L$. This means that $f(x) = x^{-1}$, where $f(x) = f^{-1}xf$. Consider the algebraic group $\overline{L} \cong L_2(\overline{\mathbf{F}}_r)$. We may assume that

f is the Frobenius endomorphism of $\overline{L}$ such that the fixed points of f^2 in $\overline{L}$ are the elements of P. By Lang's Theorem (see [43], I,2.2), there is some $y \in \overline{L}$ such that $x = y^{-1}f(y)$. Then $x^{-1} = f(y)^{-1}y$ and $f(x) = f(y)^{-1}f^2(y)$, so by the definition of x, $y = f^2(y)$. This means $y \in P$. Since L is characteristic in P, $f(y)$ and y^{-1} are in the same coset of L in P. It follows that $x \in L$, a contradiction. Therefore, there is no complement to L in X. Now assume (again for contradiction) that C is a complement to L in $\langle f\rangle P$. Then C contains three involutions which are not in L. Neither P nor $\langle f\rangle L$ contains two of these involutions, so one of them must be contained in X. However, such an involution generates a complement to L in X, contradicting what we proved above. Therefore, $\langle f\rangle P$ contains no complement to L. Now apply Theorem 2.4. □

Lemma 8.45 *Let L, P, A, f be as above. Set $n = r^{2^a} + 1$ and let $\varphi : A \hookrightarrow S_n$ be the homomorphism induced by the natural action of A on the projective line. Let $t \in P \setminus L$ be an involution. Then*

(1) $\varphi(t) \notin A_n$

(2) $\varphi(f) \notin A_n$ if and only if $a = 1$ and $r \equiv 3 \pmod 4$

Proof: (1) If $r^{2^a} \equiv 1 \pmod 4$ then $\varphi(t)$ has no fixed points and is therefore a product of $\frac{r^{2^a}+1}{2}$ transpositions. If $r^{2^a} \equiv 3 \pmod 4$ then $\varphi(t)$ has two fixed points and is therefore a product of $\frac{r^{2^a}-1}{2}$ transpositions. In either case, $\varphi(t)$ is odd.

(2) If $a > 1$ then f is a square in A, so $\varphi(f) \in A_n$. If $a = 1$ then $\varphi(f)$ has $1 + r$ fixed points and is therefore a product of $\frac{1+r^2-(1+r)}{2} = \frac{r(r-1)}{2}$ transpositions. □

Since $\varphi(L) \le A_n$, the above lemma says that it remains to determine $\mu(1, P)$ and $\mu(1, \langle f\rangle L)$ when $L \cong L_2(r^2)$ and f is a field automorphism. In the case of $\langle f\rangle L$, we may further assume that $r \equiv 1$ or $4 \pmod 5$, since $r^2 + 1 = 2p$ and in the case $p = 5$ we have $\langle f\rangle L_2(9) \cong S_6$. The required calculations have been made in Chapter 5, and we obtain the following result.

Theorem 8.46 *Let $n = 2p$, p an odd prime, and let $H \in \mathcal{P}_n$. Then one of the following holds:*

(a) $\mu(1, H) = 0$.

(b) $H \cong PGL_2(r)$, *where* $r = n - 1$ *is prime and* $r \equiv 5 \pmod 8$. *In this case,* $\mu(1, H) = \frac{|H|}{2}$.

(c) $n = 10$, $H \cong S_5$ *acting on* $\binom{[5]}{2}$, *and* $\mu(1, H) = \frac{|H|}{2}$.

(d) $n = 10$, $H \cong S_6$ *acting on the projective line over* $\mathbf{F}_9$, *and* $\mu(1, H) = -|H|$.

(e) $n = 22$, $H \cong Aut(M_{22})$, *and* $\mu(1, H) = -|H|$.

We now have enough information to determine $\mu(1, S_{2p})$.

Theorem 8.47 *Let $n = 2p$ with p an odd prime.*

$$\mu(1, S_n) = \begin{cases} -n! & \text{if } n-1 \text{ is prime and } p \equiv 3 \pmod 4 \\ \frac{n!}{2} & \text{if } n = 22 \\ -\frac{n!}{2} & \text{otherwise} \end{cases}$$

Proof: We use the results stated in the Theorem 8.46. In the first case given in this theorem, $\mathcal{P}_n$ contains one conjugacy class of self-normalizing subgroups isomorphic to $PGL_2(n-1)$, each satisfying $\mu(1, P) = \frac{|P|}{2}$, so $\sum_{H \in \mathcal{P}_n} \mu(1, H) = \frac{n!}{2}$. If $n = 10$, then $\mathcal{P}_n$ contains $\frac{10!}{5!}$ subgroups isomorphic to S_5 and $\frac{10!}{2 \times 6!}$ subgroups isomorphic to S_6. By parts (c) and (d) of Theorem 8.46, $\sum_{H \in \mathcal{P}_n} \mu(1, H) = 0$. If $n = 22$ then $\mathcal{P}_n$ contains one conjugacy class of self-normalizing subgroups isomorphic to $Aut(M_{22})$, each satisfying $\mu(1, H) = -|H|$, so $\sum_{H \in \mathcal{P}_n} \mu(1, H) = -n!$. For every other $n = 2p$, any $H \in \mathcal{P}_n$ satisfies $\mu(1, H) = 0$, so $\sum_{H \in \mathcal{P}_n} \mu(1, H) = 0$. Now apply Theorem 8.40. □

We finish this section by examining $\mu(1, A_n)$ for $n = 2p$. Pahlings has conjectured ([37]) that $\mu(1, S_n) + \mu(1, A_n) = 0$ for all n, and Welker has conjectured ([52]) that the chain complex associated to the lattice of subgroups of A_n has the homotopy type of a wedge of $\frac{n!}{2}$ spheres S^{n-4} for all $n > 6$, from which it would follow that $|\mu(1, A_n)| = \frac{n!}{2}$ for all $n \neq 6$. By Theorem 8.47, at least one of these conjectures must be false. The following theorem will provide counterexamples to both conjectures.

Theorem 8.48 *Let $n = 2p$, p an odd prime. Let $\mathcal{PR}_n^-$ be the set of all primitive $H < S_n$ such that $soc(H) \neq A_n$. Then*

$$\mu(1, S_n) + \mu(1, A_n) = -\sum_{H \in \mathcal{PR}_n^-} \mu(1, H)$$

Proof: The theorem is equivalent to the statement that $\sum \mu(1, H) = 0$, where the sum is taken over all subgroups of S_n which are not primitive. By Lemma 8.9,

$$\sum_{H \text{ intransitive}} \mu(1, H) = -\sum_{H \text{ transitive}} \mu(1, H) = -\mu_{\Pi_n}(\hat{0}, \hat{1}) = (n-1)!$$

It remains to calculate $\sum_{H \in \mathcal{IM}_n} \mu(1, H)$, where $\mathcal{IM}_n$ is the set of all transitive but imprimitive subgroups of S_n. We will use inclusion-exclusion as in the proof of Theorem 8.40. Fix an equipartition $\Phi \in \Pi_n$ of type D. Let $\mathcal{T}_\Phi$ be the set of transitive subgroups of G_Φ. By Corollary 8.15,

$$\sum_{H \in \mathcal{T}_\Phi} \mu(1, H) = -p!(p-1)!$$

Similarly, if Φ is an equipartition of type E, then

$$\sum_{H \in \mathcal{T}_\Phi} \mu(1, H) = -2^{p-1}(p-1)!$$

There are $\frac{1}{2}\binom{n}{p}$ equipartitions of type D and $\frac{n!}{p!2^p}$ equipartitions of type E, so we can calculate

$$\sum_{\Phi \in \mathcal{E}} \sum_{H \in \mathcal{T}_\Phi} \mu(1, H) = -2(n-1)!$$

where $\mathcal{E}$ is the set of equipartitions of $[n]$. By Lemmas 8.38 and 8.39, all subgroups which appear more than once in the above double sum are in $\mathcal{I}_n$. More precisely, each regular D_{2p} appears $p+1$ times and any other subgroup which stabilizes an orthogonal pair appears twice. Let $\mathcal{O}$ be the set of orthogonal pairs of equipartitions of $[n]$. As in the proof of Theorem 8.40, we must adjust the double sum by subtracting

$$\sum_{\{\sigma,\tau\}\in\mathcal{O}} \sum_{H\leq G_{\sigma,\tau}, H\in\mathcal{I}_n} \mu(1,H) = -\frac{1}{2}\binom{n}{p} p!(p-1)! = -(n-1)!$$

Therefore,

$$\sum_{H\in\mathcal{IM}_n} \mu(1,H) = -(n-1)!$$

and we are done. □

Corollary 8.49 $\mu(1,S_{62}) + \mu(1,A_{62}) = -62!$

Proof: By Theorem 8.41, $\mathcal{PR}_{62}^-$ consists of one conjugacy class of $\frac{62!}{61(61^2-1)}$ subgroups isomorphic to $PGL_2(61)$ and one conjugacy class containing the same number of subgroups isomorphic to $L_2(61)$. By Theorem 5.1,

$$\mu(1,L_2(61)) = \mu(1,PGL_2(61)) = |L_2(61)| = \frac{61(61^2-1)}{2}.$$

Therefore, $\sum_{H\in\mathcal{PR}_{62}^-} \mu(1,H) = 62!$. □

Corollary 8.50 $\mu(1,A_{14}) = 14!$ *(so the chain complex of the subgroup lattice of A_{14} does not have the homotopy type of $\frac{14!}{2}$ 10-spheres).*

Proof: By Theorem 8.41, $\mathcal{PR}_{14}^-$ consists of one conjugacy class of $\frac{14!}{13(13^2-1)}$ subgroups isomorphic to $PGL_2(13)$ and one conjugacy class containing the same number of subgroups isomorphic to $L_2(13)$. By Theorem 5.1,

$$\mu(1,PGL_2(13)) = |L_2(13)| = -\mu(1,L_2(13)),$$

so $\sum_{H\in\mathcal{PR}_{14}^-} \mu(1,H) = 0$ and $\mu(1,A_{14}) = -\mu(1,S_{14})$. By Theorem 8.47, $\mu(1,S_{14}) = -14!$. □

8.6 The cases $n = p^2$ and $n = pr$

Let p, r be odd primes. The proofs that $\sum_{H\in\mathcal{I}_n} \mu(1,H) = 0$ when $n = p^2$ and $n = pr$ are similar to the proof for $n = 2p$. The proofs of some of the necessary lemmas in these cases will be given in less detail than was given for the proofs of the corresponding lemmas in the case $n = 2p$. We begin with the following easy lemma, which holds for all $n \in \mathbf{N}$ and will also be used in Section 8.7.

Lemma 8.51 *Let $\Phi = [X_1; X_2; \ldots; X_r]$ and $\Psi = [Y_1; Y_2; \ldots; Y_s]$ be equipartitions of $[n]$ such that the stabilizer $G = G_\Phi \cap G_\Psi \leq S_n$ of both Φ and Ψ is transitive. Then there exists some $c \in \mathbf{N}$ such that for all $i \in [r]$, $j \in [s]$, $|X_i \cap Y_j| = 0$ or c.*

Proof: Assume that both $X_i \cap Y_j$ and $X_k \cap Y_l$ are nonempty. Let $x \in X_i \cap Y_j$, $y \in X_k \cap Y_l$. Since G is transitive, there is some $g \in G$ with $x^g = y$. Since g stabilizes both Φ and Ψ, $X_i^g = X_k$ and $Y_j^g = Y_l$. Therefore, $(X_i \cap Y_j)^g = (X_k \cap Y_l)$ and $|X_i \cap Y_j| = |X_k \cap Y_l|$. □

We first examine the case $n = p^2$.

Proposition 8.52 *Let $\sigma = [X_1; \ldots; X_p]$ and $\tau = [Y_1; \ldots; Y_p]$ be distinct equipartitions of $[n = p^2]$, with respective stabilizers $G_\sigma, G_\tau \leq S_n$. Then $G_\sigma \cap G_\tau$ is transitive if and only if $\{\sigma, \tau\}$ is an orthogonal pair.*

Proof: ($\Leftarrow$) was proved in Section 8.2 and ($\Rightarrow$) follows immediately from Lemma 8.51, since p is prime. □

Lemma 8.53 *Let σ, τ, ρ be equipartitions of $[n = p^2]$, with respective stabilizers G_σ, G_τ, $G_\rho \leq S_n$. If $K = G_\sigma \cap G_\tau \cap G_\rho$ is transitive, then $K \leq A_n$. In particular, K contains no odd involution.*

Proof: By Proposition 8.52, σ, τ, and ρ are pairwise orthogonal. Consider the array $A(\sigma, \tau)$ described in Section 8.2, and let $G = G_\sigma \cap G_\tau$. Then $K \leq G$ and $G = G_1 \times G_2$, with each $G_i \cong S_p$. Let K^i be the projection of K on G_i and let $K_i = K \cap G_i$. Assume K is transitive. Then both K^i are transitive subgroups of S_p. Since $K_i \trianglelefteq K^i$, each K_i is either trivial or transitive. If both K_i are trivial, then there is an isomorphism $\psi : K^1 \to K^2$ such that $K = \{(k, \psi(k)) : k \in K^1\}$. Since p is odd, $sgn_{S_n}((k, \psi(k))) = sgn_{S_p}(k) sgn_{S_p}(\psi(k))$. Since K^1 is a primitive subgroup of S_p, K^1 is either almost simple or affine. If K^1 is almost simple then by Corollary 8.33, either

$K^1 \leq A_p$ or $K^1 = S_p$. In either case, k and $\psi(k)$ have the same parity in S_p for all $k \in K^1$, so $K \leq A_{p^2}$. If K^1 is affine and $h, k \in K^1$ have the same order, then h and k are conjugate in S_p. Again k and $\psi(k)$ have the same parity in S_p for all $k \in K^1$, so $K \leq A_n$.

Now we consider the case where K_1 is transitive on the rows of $A = A(\sigma, \tau)$. Let $\rho = [R_1; \ldots; R_p]$. We color the p^2 boxes in the array A with the colors $\{1, \ldots, p\}$ so that box (i,j) gets color k if $a_{ij} \in R_k$. Since ρ is orthogonal to both σ and τ, this makes A a Latin square, and any $y \in K$ permutes the rows and columns of A and the p color classes. If $k \in K_1$ fixes a row of A, then since k fixes all columns of A, k must fix all color classes. It follows immediately that $k = 1$, so K_1 is regular on the rows of A. Therefore, $K_1 \cong Z_p$ and K^1 is affine. Since K^2 is transitive and $K^2/K_2 \cong K^1/K_1$ can be embedded in $N_{S_p}(Z_p) \cong Z_{p-1}$, K_2 is transitive. By the above argument, $K_2 \cong Z_p$ and K^2 is affine. It follows that there is an isomorphism $\psi : K^1 \to K^2$ such that $K = \{(kx, \psi(k)y) : k \in K^1, x \in K_1, y \in K_2\}$. Note that x and y are always even in S_p. As in the above paragraph, k and $\psi(k)$ have the same parity in S_p for all k in K^1, since K^1 is affine. Therefore, kx and $\psi(k)y$ have the same parity in S_p, and $K \leq A_n$. □

Lemma 8.54 *Let $[\sigma, \tau]$ be an orthogonal pair of equipartitions of $[n = p^2]$, with respective stabilizers G_σ, G_τ. Set $G = G_\sigma \cap G_\tau$. Then*

$$\sum_{H \leq G, H \in \mathcal{C}_n} \mu(1, H) = p!(p-1)!$$

Proof: As above, we have $G = G_1 \times G_2$ with each $G_i \cong S_p$. For $H \leq G$, let H^i be the projection of H to G_i. Let $P_1(H) \in \Pi_p$ be given by the orbits of H^1 on the rows of $A(\sigma, \tau)$, and $P_2(H) \in \Pi_p$ be given by the orbits of H^2 on the columns. There is some $M \leq G$ which is maximal with respect to the property $P_i(M) = P_i(H)$ for $i = 1, 2$. Also, for every $P, Q \in \Pi_p$ there exists some $H \leq G$ such that $P_1(H) = P$ and $P_2(H) = Q$. Therefore, there is a closure on the lattice $L(G)$ of subgroups of G whose image is $\overline{L(G)} \cong \Pi_p \times \Pi_p$ and $\overline{H} = \overline{G}$ if and only if H^1 and H^2 are transitive. Similarly, there is a closure on $L(G \cap A_n)$ whose image is isomorphic to $(\Pi_p \times \Pi_p) \setminus R_1$. Here R_1

is the first rank of $\Pi_p \times \Pi_p$, consisting of all pairs (P_1, P_2) such that one P_i consists of $n-2$ singletons and a 2-set, and the other consists of n singletons. Let $\mathbf{P} = \Pi_p \times \Pi_p$. There are $2\binom{p}{2}$ $X \in \mathbf{P}$ such that $X \in R_1$, and for each such X, the interval $\left[X, \hat{1}\right]_{\mathbf{P}}$ is isomorphic to $\Pi_p \times \Pi_{p-1}$. Let $\mathcal{T}_{1,2}$ be the set of all $H \leq G$ such that H^1 and H^2 are transitive. It follows from the above information and easy calculation that

$$\sum_{H \in \mathcal{T}_{1,2}} \mu(1, H) - \sum_{H \in \mathcal{T}_{1,2}, H \leq A_n} \mu(1, H) = -\sum_{X \in R_1} \mu_{\mathbf{P}}(X, \hat{1}) = p!(p-1)!$$

It is now sufficient to show that if $H \in \mathcal{T}_{1,2}$ and H is not transitive, then $H \leq A_n$. Indeed, this will show that $\sum_{H \leq G, H \in \mathcal{C}_n} \mu(1, H)$ is equal to the difference on the left side of the above equation. Let $H_i = H \cap G_i$. If both H^i are transitive and H is not transitive, then both H_i must be trivial. Then H is a diagonal subgroup of G, and the argument used in the proof of Lemma 8.53 shows that $H \leq A_n$. $\square$

Theorem 8.55 *Let $n = p^2$, p an odd prime. Then*

$$\mu(1, S_n) = \frac{n!}{2} - \sum_{H \in \mathcal{P}_n} \mu(1, H)$$

Proof: There are $\frac{n!}{p!^{p+1}}$ equipartitions and $\frac{n!}{2p!^2}$ orthogonal pairs of equipartitions of $[n]$. The theorem now follows from Corollary 8.17 and Lemmas 8.53 and 8.54, using the argument found in the proof of Theorem 8.40. $\square$

Now we look at the case $n = pr$, where $p > r$ with both p, r prime.

Lemma 8.56 *Let $n = pr$, with both p and r odd primes and $p > r$. If $H \in \mathcal{I}_n$, then either H stabilizes a unique equipartition of $[n]$ or H stabilizes an orthogonal pair and no other equipartitions*

Proof: If transitive H stabilizes $\sigma = [X_1; \ldots; X_p]$ and $\tau = [Y_1; \ldots; Y_r]$ then it follows immediately from Lemma 8.51 that $\{\sigma, \tau\}$ is an orthogonal pair, since p, r are prime. An element x of order p in transitive $H \leq S_n$ can stabilize at most one equipartition Ψ with r parts of size p, since the cycles of x must define parts of Ψ and two distinct equipartitions which share a part cannot be stabilized simultaneously by a transitive group.

It remains to show that H cannot stabilize two equipartitions with p parts of size r. Assume (for contradiction) that $H \in \mathcal{C}_n$ does stabilize two such partitions, and let $M \leq H$ be the stabilizer of a point. Then there exist subgroups K, L such that $M \leq K, L \leq H$ with $[K:M] = [L:M] = r$ and $[H:K] = [H:L] = p$. Let $C = core_H(K)$, $D = core_H(L)$. Note that $C \cap D = core_H(M) = 1$. Set $\overline{H} = H/D$, so $\overline{H}$ is a primitive permutation group on the coset space $L\backslash H$. Then $\overline{C} \cong C$, and if $C \neq 1$, C is transitive on $L\backslash H$. Assume (for contradiction) that this is the case, so $[C : L \cap C] = p$. Note that $M \cap C = K \cap L \cap C = L \cap C$, and that M is maximal in K. Therefore, $K = MC$ and $r = [K:M] = [C : M \cap C] = p$, a contradiction. We have shown that $C = 1$, so the action of H on the coset space $K\backslash H$ embeds H in S_p as a transitive subgroup. We must show that any transitive $H \leq S_p$ containing two subgroups K, L of index p, both of which contain a subgroup M of index pr in H, cannot contain an element which acts as an odd involution on the coset space $M\backslash H$. If $H \leq S_p$ is affine, let $P \trianglelefteq H$ with $P \cong Z_p$. Any two subgroups K, L of index p in H are distinct complements to P and therefore intersect trivially. In this case, $M = 1$ and $|H| = pr$ is odd, so H contains no involution. If H is almost simple, then $S = soc(H)$ is one of the groups mentioned in Lemma 8.32. It remains to show that H cannot satisfy all of the required conditions. If S is a Mathieu group or $S \cong L_2(11)$ acting on cosets of A_5 then $H = S$ contains no odd involution. If $S \cong A_p$ then $K \cap S \cong A_{p-1}$ contains no subgroup of index less than $p-1$. Finally, assume that $S = L_d(q)$ acting on 1-spaces. Note that S acts 2-transitively on this set. Thus $[S : S \cap K] = p$ and $[S : S \cap M] = p(p-1)$. It follows immediately that $[K:M] = p - 1 > r$, and we are done. □

Theorem 8.57 *Let $n = pr$, with p, r distinct odd primes. Then*

$$\mu(1, S_n) = \frac{n!}{2} - \sum_{H \in \mathcal{P}_n} \mu(1, H)$$

Proof: There are $\frac{n!}{r!p!^r}$ partitions of $[n]$ into r parts of size p, $\frac{n!}{p!r!^p}$ partitions of $[n]$ into p parts of size r, and $\frac{n!}{p!r!}$ orthogonal pairs of equipartitions of $[n]$. The theorem now follows from Corollary 8.10, Corollary 8.17, Corollary 8.25, and Lemma 8.56, again using the argument found in the proof of Theorem 8.40. □

Remark 8.58 *If p is an odd prime such that $r = \frac{p-1}{2}$ is also prime, then the action of S_p on $\binom{[p]}{2}$ embeds S_p into S_{pr} so that $S_p \in \mathcal{P}_{pr}$.*

This gives another class of examples for which $\mu(1, S_n) \neq (-1)^{n-1}\frac{n!}{2}$. For example, if $n = 55$, the possible socles for elements of $\mathcal{P}_n$ are A_{11} as described above, M_{11}, and $L_2(11)$ acting on the cosets of either A_4 or D_{12} (see [32]). Since M_{11} is complete and $\mu(1, PGL_2(11)) = 0$, the only elements of $\mathcal{P}_{55}$ which contribute to $\mu(1, S_{55})$ are the $\frac{55!}{11!}$ copies of S_{11}. It follows that $\mu(1, S_{55}) = 0$. However, the situation is not always this pleasant. For instance, in order to calculate $\mu(1, S_{21})$ using the above results, one needs to find $\mu(1, H)$ for all $H \in \mathcal{P}_{21}$ with $soc(H) = L_3(4)$. Note also that the embedding of S_5 into S_{10} is of the type described in the remark, and there are other elements of $\mathcal{P}_{10}$ which cancel the contribution of S_5, so that $\sum_{H \in \mathcal{P}_{10}} \mu(1, H) = 0$.

8.7 The case $n = 2^a$

Here we will again make use of Crapo's complement theorem. Let $A_n^\perp$ be the set of complements to A_n in S_n (so $A_n^\perp$ is the set of subgroups which are generated by an odd involution). For $H \in \mathcal{I}_n$, let $\mathcal{S}(H)$ be the set of subgroups of H. Then the set of complements to $H \cap A_n$ in H is $\mathcal{S}(H) \cap A_n^\perp$. This immediately gives the following lemma.

Lemma 8.59 $\sum_{H \in \mathcal{I}_n} \mu(1, H) = -\sum_{t \in A_n^\perp} \sum_{t \leq H \in \mathcal{I}_n} \mu(t, H)$

Our goal is to show that $\sum_{t \leq H \in \mathcal{I}_n} \mu(t, H) = 0$ for any fixed $t \in A_n^\perp$. We will use inclusion-exclusion on the set of equipartitions of $n = 2^a$ stabilized by t as in Section 8.5. Here it is difficult to enumerate the set of all equipartitions stabilized by t, but we will avoid this difficulty by showing that every term in the inclusion-exclusion sum is equal to 0.

Lemma 8.60 *Let $n = 2^a$, and fix $t \in A_n^\perp$ such that t is not generated by a transposition. Let $\{\Psi_1, \Psi_2, \ldots, \Psi_k\}$ be a set of equipartitions of $[n]$ such that $t \leq G_{\Psi_i}$ (the stabilizer* *of Ψ_i in S_n) for all $i \in [k]$ and such that $G = \cap_{i\in[k]} G_{\Psi_i}$ is transitive. Let $\mathcal{TR}_{t,G}$ be the set of transitive subgroups of G which contain t. Then*

$$\sum_{H \in \mathcal{TR}_{t,G}} \mu(t, H) = 0$$

Proof: By Theorem 2.3, it is sufficient to show that there is some $K \leq G$ such that $t < K$ and K has the same orbits as t. Identify the subgroup t with the odd involution t that generates it, and write t as the product of disjoint transpositions $t = t_1 t_2 \dots t_m$ with $m > 1$. Let P_2 be a Sylow 2-subgroup of G containing t. Since $n = 2^a$, P_2 is transitive. Let z be an involution in the center of P_2 (it is well known that such a z exists). Since the fixed points of z are a P_2-orbit and $z \neq 1$, z has no fixed points. Write z as a product of $b = \frac{n}{2}$ disjoint transpositions, $z = z_1 z_2 \dots z_b$. Let $\Phi_z = [Z_1; Z_2; \dots; Z_b]$ be the equipartition of $[n]$ such that $Z_i = supp(z_i)$. Then the stabilizer of Φ_z in S_n is the centralizer of z.

Since t centralizes z, for every t_i one of the following cases holds:

(1) There exists some j such that $t_i = z_j$

(2) There exist j, k, l such that $|supp(t_i) \cap supp(z_k)| = |supp(t_i) \cap supp(z_l)|$
$= |supp(t_j) \cap supp(z_k)| = |supp(t_j) \cap supp(z_l)| = 1$ and $< t_i t_j, z_k z_l >$ is a 4-group.

Since m is odd, there exist an odd number of t_i for which case (1) holds. In particular, there is at least one such t_i, so we may assume that $t_1 = z_1$.

Now fix any $\Psi_i = [X_1; \dots; X_r]$. Since the transitive group P_2 stabilizes both Ψ_i and Φ_z, we may apply Lemma 8.51. Therefore, one of the following holds:

(a) $|X_j \cap Z_k| = 0$ or 1 for all j, k

(b) $|X_j \cap Z_k| = 0$ or 2 for all j, k

Assume (for contradiction) that (a) holds. Since $z \in P_2$, z stabilizes Ψ_i. Since (a) holds, z does not fix any part X_j. Fix any l such that $t_l = z_l$. Then t exchanges the two parts of Ψ_i which intersect $supp(t_l)$. The union of these two parts is the union of the support of some z_h and also the union of the support of some t_k. Since each part has 2^d elements for some $d > 0$, there must be an even number of t_k which satisfy case (1) above involved in the exchange of these two parts. We can throw aside these two parts and continue this process, each time throwing aside evenly many t_k which satisfy case (1). However, we must eventually throw aside an odd number of t_k satisfying case (1), which gives the desired contradiction.

Therefore, each Ψ_i satisfies (b) above. In particular, for every i, $supp(t_1) = supp(z_1)$ is contained in a part of Ψ_i. It follows that $t_1 \in G$ and $< t, t_1 > \leq G$ has the same orbits as t. $\Box$

Corollary 8.61 *Let $n = 2^a$. Then for any $t \in A_n^{\perp}$ which is not generated by a transposition,*

$$\sum_{t \leq H \in \mathcal{I}_n} \mu(t, H) = 0.$$

Proof: Let $\mathcal{E}_t$ be the set of equipartitions of $[n]$ stabilized by t. For each $\mathcal{F} \subseteq \mathcal{E}_t$ let $G_{\mathcal{F}}$ be the stabilizer in S_n of all the equipartitions in $\mathcal{F}$. Define $\mathcal{TR}_{t,G_{\mathcal{F}}}$ as in Lemma 8.60. Then

$$\sum_{t \leq H \in \mathcal{I}_n} \mu(t, H) = \sum_{\mathcal{F} \subseteq \mathcal{E}_t} (-1)^{|\mathcal{F}|} \sum_{H \in \mathcal{TR}_{t,G_{\mathcal{F}}}} \mu(t, H).$$

This double sum is zero, since each subsum is zero by Lemma 8.60. $\Box$

It remains to examine a complement to A_n which is generated by a transposition.

Lemma 8.62 *Let $H \leq S_n$ be the stabilizer of $n - k$ points (so $H \cong S_k$), with $k < n$, and let $H < K \leq S_n$ with $N_K(H) = H$. Then K is the stabilizer of $n - k - 1$ points (so $K \cong S_{k+1}$).*

Proof: We may assume that $supp(H) = [k]$. Let $\Gamma = supp(K)$, so $k < |\Gamma| \leq n$. Let $\Omega \subseteq \Gamma$ be the K-orbit containing $[k]$. If $\Omega = [k]$ then $K = H \times L$ for some $1 \neq L \leq S_{\Gamma \setminus \Omega}$, a contradiction. By conjugating H by appropriate elements of K, we see that $S_\Delta \leq K$ for every $\Delta \subseteq \Omega$ such that $|\Delta| = k$. It follows that $|\Omega| = k+1$ and $S_\Omega \leq K$. Therefore, $K = S_\Omega \times L$ for some $L \leq S_{\Gamma \setminus \Omega}$, and $N_K(H) = H$ forces $L = 1$ (that is, $\Gamma = \Omega$). □

Corollary 8.63 *Let $1 \neq H \leq S_n$ be the stabilizer of k points. Then*

$$\mu(H, S_n) = (-1)^k k!$$

Proof: If $k = 1$ then H is maximal in S_n and the formula holds, so we proceed by induction on k. If $k > 1$, by Lemma 8.62 there are k subgroups $K \leq S_n$ satisfying $H < K$ and $N_K(H) = H$. By inductive hypothesis and the lemma, $\mu(K, S_n) = (-1)^{k-1}(k-1)!$ for all such K. The corollary now follows immediately from the application of Theorem 2.5 to the set $\{K \leq S_n : N_K(H) = H\}$. □

A homotopy version of Corollary 8.63 has been obtained by Gábor Ivanyos ([26]).

Corollary 8.64 *If $t \in A_n^\perp$ is generated by a transposition, then $\mu(t, S_n) = (-1)^{n-2}(n-2)!$.*

Corollary 8.65 *If $t \in A_n^\perp$ is generated by a transposition, then*

$$\sum_{t \leq H \in \mathcal{I}_n} \mu(t, H) = 0.$$

Proof: Let $\mathcal{TR}_t$ be the set of transitive subgroups of S_n containing t. It is well known that the only primitive subgroup of S_n containing t is S_n (see [2], p.62). Therefore, $\mathcal{TR}_t = \{S_n\} \cup \{H \in \mathcal{I}_n : t \leq H\}$. Let $P_t \in \Pi_n$ be the partition given by the orbits of t. An appropriate variation of Lemma 8.9 gives

$$\mu(t,S_n)+\sum_{t\le H\in\mathcal{I}_n}\mu(t,H) = \sum_{H\in\mathcal{TR}_t}\mu(1,H)$$
$$= \mu_{\Pi_n}(P_t,\hat{1})=(-1)^{n-2}(n-2)!=\mu(t,S_n).$$

giving the desired result. □

Theorem 8.66 *Let $n=2^a$. Then*

$$\mu(1,S_n)=-\frac{n!}{2}-\sum_{H\in\mathcal{P}_n}\mu(1,H)$$

Proof: This follows immediately from the discussion at the beginning of this section and Corollaries 8.61 and 8.65. □

As before, we will use the O'Nan-Scott theorem to describe $\mathcal{P}_n$ and then calculate $\sum_{H\in\mathcal{P}_n}\mu(1,H)$.

Lemma 8.67 *Let $n=2^a$. Then $\sum_{H\in\mathcal{P}_n}\mu(1,H)=0$.*

Proof: We may assume $a>2$. By Theorem 8.29, if $H\le S_n$ is primitive, one of the following cases must hold:

(1) H is affine: Then $H\le GV\cong AGL_a(2)$, where $V\cong Z_2^a$ acts regularly and $G\cong GL_a(2)$ acts naturally. Every nonidentity element of V is the product of 2^{a-1} transpositions, so $V\le A_n$. G is simple, so $G\le A_n$. Therefore, $H\le A_n$ and $H\notin\mathcal{P}_n$.

(2) H is almost simple: Using Theorem 8.30, it is clear that if $H\in\mathcal{P}_n$ then $soc(H)\cong L_d(q)$ for some prime d and prime power $q=r^b$, with $2^a=\frac{q^d-1}{q-1}$. It is easy to show that $d=2$ and $b=1$, so q is prime. Therefore, $H\in\mathcal{P}_n$ implies $H\cong PGL_2(q)$, and $2^a=q+1$. Since $a>2$, $q\equiv 7\pmod 8$. By Theorem 5.1, $\mu(1,H)=0$.

(3) H has the product action: Then there is some set Γ with $|\Gamma|=2^k$, $1<k<a$,

such that we can identify $[n]$ with Γ^l, $l = \frac{a}{k}$, and $H \leq KN$. Here $N \cong S_{2^k}^l$ acts on Γ^l componentwise, and $K \cong S_l$ permutes the components. Note that if $k = 1$ then we are in the affine case. We will show that both K and N are contained in A_n, so that $H \notin \mathcal{P}_n$. Let $s \in K$ be the involution such that $(a_1, a_2, a_3, \ldots, a_l)^s = (a_2, a_1, a_3, \ldots, a_l)$. Then the fixed points of s are the $(2^k)^{l-1}$ l-tuples of the form $(a, a, a_3, \ldots, a_l)$. Since $k > 1$, $|supp(s)| = (2^k)^{l-1}(2^k - 1)$ is divisible by 4, and $s \in A_n$. Since K is generated by conjugates of s, $K \leq A_n$. Now let $g = (t, 1, 1, , \ldots, 1) \in N$ with $t \in S_{2^k}$ a transposition. Then $|supp(g)| = 2(2^k)^{l-1}$ is divisible by 4, so $g \in A_n$. Since N is generated by KN-conjugates of g, $N \leq A_n$.

We have examined all possible cases and shown that if $H \in \mathcal{P}_n$ then $\mu(1, H) = 0$. □

Corollary 8.68 *Let $n = 2^a$. Then*

$$\mu(1, S_n) = -\frac{n!}{2}.$$

References

[1] G. E. Andrews, *The Theory of Partitions*, Addison-Wesley, Reading, Mass., 1976.

[2] M. Aschbacher, *Finite Group Theory*, Cambridge studies in advanced mathematics **10**, Cambridge University Press, Cambridge, 1986.

[3] M. Aschbacher, On the maximal subgroups of the finite classical groups, Inv. Math. **76** (1984), 469-514.

[4] Barcelo, H. On the action of the symmetric group on the free Lie algebra and the partition lattice, J. Combin. Theory Ser. A **55** (1990), 93-129.

[5] Barcelo, H. and Bergeron, N. The Orlik-Solomon algebra on the partition lattice and the free Lie algebra, J. Combin. Theory Ser. A **55** (1990), 80-92.

[6] Burnside, W. *Theory of Groups of Finite Order*, Cambridge University Press, 1911.

[7] P. J. Cameron, Finite permutation groups and finite simple groups, Bull. London Math. Soc. **13** (1981), 1-22.

[8] R. W. Carter, Conjugacy classes in the Weyl group, Compositio Math. **25** (1972), 1-59.

[9] R. W. Carter, *On the structure and complex representation theory of finite groups of Lie type. Notes taken by Burkhard Külshammer*, Vorlesungen aus dem Fachbereich Mathematik der Universität Essen **16**, Universität Essen, Fachbereich Mathematik, Essen, 1987.

[10] J. H. Conway, R. T. Curtis, S. P. Norton, R. A. Parker and R. A. Wilson, *Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray*, Oxford University Press, Oxford, 1985.

[11] H. Crapo, The Möbius Function of a Lattice, J. Combin. Theory **1** (1966), 126-134.

[12] H. Crapo, Möbius Inversion in Lattices, Arch. Math. (Basel) **19** (1968), 595-607.

[13] C. W. Curtis and G. I. Lehrer, Homology Representations of Finite Groups, in *Contemporary Mathematics*, vol. 9, (R. Lidl, editor), pp. 1-28, American Mathematical Society, 1982.

[14] L. E. Dickson, *Linear Groups with an Exposition of the Galois Theory*, Dover, New York, 1984.

[15] L. E. Dickson, *Modern Elementary Theory of Numbers*, University of Chicago Press, Chicago, 1939.

[16] M. Downs, The Möbius function of $PSL_2(q)$, with an application to the maximal normal subgroups of the modular group, J. London Math. Soc. (2) **43** (1991), 61-75.

[17] J. Folkman, The homology groups of a lattice, J. Math. Mech. **15** (1966), 631-636.

[18] D. Gorenstein and R. Lyons, *The local structure of finite groups of characteristic 2 type*, Memoirs of the American Mathematical Society **276** (1983), 1-731.

[19] R. Guralnick, Subgroups of Prime Power Index in a Simple Group, J. Algebra **81** (1983), 304-311.

[20] P. Hall, The Eulerian functions of a group, Quart. J. Math. **7** (1936), 134-151.

[21] P. Hanlon, The fixed-point partition lattices, Pacific J. Math. **96** (1981), 319-341.

[22] T. Hawkes, I. M. Isaacs and M. Özaydin, On the Möbius function of a finite group, Rocky Mountain J. Math. **19** (1989), 1003-1034.

[23] T. W. Hungerford, *Algebra*, Graduate Texts in Mathematics **73**, Springer-Verlag, 1974.

[24] B. Huppert, Singer-Zyklen in klassischen Gruppen, Math. Z. **117** (1970) 141-150.

[25] I. M. Isaacs, *Character Theory of Finite Groups*, Pure and Applied Mathematics **69**, Academic Press, New York, 1976.

[26] G. Ivanyos, On the homotopy type of the poset of classes of subgroups of S_n, personal communication, 1995.

[27] C. Jansen, K. Lux, R. Parker and R. Wilson *An atlas of Brauer characters. Appendix 2 by T. Breuer and S. Norton*, London Mathematical Society Monographs, New series **11**, The Clarendon Press, Oxford University Press, New York, 1995.

[28] P. Kleidman and M. Liebeck, *The Subgroup Structure of the Finite Classical Groups*, London Mathematical Society Lecture Note Series **129**, Cambridge University Press, Cambridge, 1990.

[29] C. Kratzer et J. Thévenaz, Fonction de Möbius d'un groupe fini et anneau de Burnside, Comment. Math. Helv. **59** (1984), 425-436.

[30] Lehrer, G. I. and Solomon, L., On the action of the symmetric group on the cohomology of the complement of its reflecting hyperplanes, J. Algebra **104** (1986), 410-424.

[31] M. W. Liebeck, C. E. Praeger and J. Saxl, On the O'Nan-Scott Theorem for finite primitive permutation groups, J. Austral. Math. Soc. Ser. A **44** (1988), 389-396.

[32] M. W. Liebeck and J. Saxl, Primitive permutation groups containing an element of large prime order, J. London Math. Soc. (2) **31** (1985), 237-249.

[33] A. Lucchini, On imprimitive groups with small degree, Rend. Sem. Mat. Univ. Padova **86** (1991), 131-142.

[34] H. H. Mitchell, Determination of the ordinary and modular ternary linear groups, Transactions of the American Mathematical Society **12** (1911), 207-242.

[35] J. Munkres, *Elements of Algebraic Topology*, Addison-Wesley, 1984.

[36] P. Orlik and L. Solomon, Combinatorics and topology of complements of hyperplanes, Invent. Math. **56** (1980), 167-189.

[37] H. Pahlings, Character Polynomials and the Möbius function, Arch. Math. (Basel) **65** (1995), 111-118.

[38] H. Pahlings, personal communication.

[39] G. Pólya and R. C. Read, it Combinatorial enumeration of groups, graphs, and chemical compounds. Polya's contribution translated from the German by Dorothee Aeppli, Springer-Verlag, 1987.

[40] D. Quillen, Homotopy Properties of the Poset of Nontrivial p-Subgroups of a Group, Advances in Math. **28** (1978), 101-128.

[41] S. Roman, *Field Theory*, Graduate Texts in Mathematics **158**, Springer-Verlag, New York, 1995.

[42] G-C. Rota and B. Sagan, Congruences Derived from Group Action, European J. Combin. **1** (1980) 67-76.

[43] T. A. Springer and R. Steinberg, Conjugacy Classes, in *Seminar on Algebraic Groups and Related Finite Groups*, (A. Borel, et al, editors), Lecture Notes in Mathematics **131**, Springer-Verlag, 1970.

[44] B. Srinivasan, On the modular characters of the special linear group $SL_2(p^n)$, Proc. London Math. Soc. (3) **14** (1964), 101-114.

[45] R.P. Stanley, *Enumerative Combinatorics*, vol. 1, Wadsworth and Brooks/Cole, 1986.

[46] R.P. Stanley, *Some aspects of groups acting on finite posets*, J. Combin. Theory (A) **32** (1982), 132-161.

[47] R. Steinberg, *Lectures on Chevalley Groups*, Yale University, 1967.

[48] S. Sundaram, Applications of the Hopf trace formula to computing homology representations, in *Jerusalem combinatorics '93. Papers from the International Conference on Combinatorics held in Jerusalem, May 9-17, 1993* (H. Barcelo and G. Kalai, editors), Contemporary Mathematics **178**, American Mathematical Society, Providence, RI, 1994.

[49] S. Sundaram, The homology representations of the symmetric group on Cohen-Macaulay subposets of the partition lattice, Adv. in Math. **104** (1994), 225-296.

[50] M. Suzuki, *On a class of doubly transitive groups*, Annals of Math. **75** (1962), 105-145.

[51] P. J. Webb, Subgroup complexes, in *The Arcata Conference on Representations of Finite Groups (Arcata, Calif. 1986)*, 349-365, Proc. Sympos. Pure Math. **47**, Part 1, Amer. Math. Soc., Providence, RI, 1987.

[52] V. Welker, Equivariant Homotopy of Posets and Some Applications to Subgroup Lattices, J. Combin. Theory Ser. A **69** (1995), 61-86.

[53] C. D. Wensley, *The supercharacter table of the symmetric group S_7*, preprint.

Vita

John Shareshian

1978 Graduated Teaneck High School, Teaneck, New Jersey.

1978-82 Attended University of Pennsylvania, Philadelphia, Pennsylvania. Majored in Mathematics.

1983 B.S., University of Pennsylvania.

1990-96 Graduate work in Mathematics, Rutgers University, New Brunswick, New Jersey.

1992-93 DIMACS Graduate Assistant, Rutgers University.

1993-94 Teaching Assistant, Rutgers University.

1994-95 National Needs Fellow, Rutgers University.

1995-96 Teaching Assistant, Rutgers University.