Title
The essential p-dimension of finite simple groups of Lie type

Author
Knight, Hannah

Publication Date
2023

UNIVERSITY OF CALIFORNIA,

IRVINE

The essential p-dimension of finite simple groups of Lie type

DISSERTATION

submitted in partial satisfaction of the requirements
for the degree of

DOCTOR OF PHILOSOPHY

in Mathematics

by

Hannah Knight

Dissertation Committee:
Associate Professor Jesse Wolfson, Chair
Professor Daqing Wan
Professor Vladimir Baranovsky

2023

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

I would like to thank Jesse Wolfson for his kind mentorship and generous support. I cannot thank him enough for his patience in helping me understand difficult concepts, dedication in carefully reading and correcting many drafts, and kindness in encouraging me in my work.

I would also like to thank my parents for their constant encouragement and love. Thank you for always being there for me to listen to me, encourage me, empathize with me, advise me, pray for me, and love me.

Thank you also to my friends for caring for me, praying for me, spending time with me, and always encouraging me.

I am also grateful to my fellow students at UCI, for their support and help throughout my time at UCI. I thank the Journal of Algebra for their invaluable aid in editing and publishing my first article, which is contained in the contents of the first half of this dissertation. Financial support was provided by the University of California, Irvine and by NSF Grant Nos. DMS-1811846 and DMS-1944862.

VITA

2013	National Merit Scholar
2013	Wildcat MAC Scholarship Award, University of Arizona
2013-2014	Galileo Circle Science Recruitment Scholar, University of Arizona
2014-2017	Dean's List With Distinction, University of Arizona
2014-2015	Kino School, Tucson, AZ
2015-2016	Quest for Education and Arts, Tucson, AZ
2016-2017	Mathematics Consortium Working Group, Tucson, AZ
2016-2017	Undergraduate Teaching Assistant, University of Arizona
2017	B.S. in Mathematics, University of Arizona
2017	B.M. in Harp, University of Arizona
2017-2022	Graduate Teaching Assistant, University of California, Irvine
2018	NSF/PIMS Summer School - The Roots of Topology, University of Chicago
2019	IPAM Braids, Resolvent Degree and Hilbert's 13th Problem, University of California, Los Angeles
2019	PIMS Workshop on Arithmetic Topology, University of British Columbia
2021-2022	Teacher at Covenant Christian Academy, Westminster, CA
2021-2022	Instructor of Record, University of California, Irvine
2023	Ph.D. in Mathematics, University of California, Irvine

PUBLICATIONS/PREPRINTS

"The essential p-dimension of finite simple groups of Lie type"(Journal of Algebra)

"The essential l-dimension at non-defining primes of finite groups of Lie type" (preprint)

Translation of Tschebotarow's "The Resolvent Problem"

Translation of Tschebotarow's "The Problem of Resolvents and Critical Manifolds"

RESEARCH TALKS

Séminaire Variétés Rationnelles, Sorbonne University (Paris, France) - On the essential p-dimension of finite simple groups

UCLA Algebraic Topology Seminar - On the essential p-dimension of finite simple groups

ABSTRACT OF THE DISSERTATION

The essential p-dimension of finite simple groups of Lie type

by

Hannah Knight

Doctor of Philosophy in Mathematics

University of California, Irvine, 2023

Associate Professor Jesse Wolfson, Chair

In this dissertation, we compute the essential p-dimension of the split finite quasi-simple groups of classical Lie type at the defining prime, specifically the quasi-simple groups arising from the general linear and special linear groups, the symplectic groups, and the orthogonal groups. Also, for odd primes l not equal to the defining prime, we compute the essential l-dimension of the finite groups of classical Lie type, specifically the general linear and special linear groups, the symplectic groups, the orthogonal groups, and the unitary groups, and the non-abelian simple factors in their Jordan-Hölder series.

1 Introduction

In my thesis, I study the essential p-dimension of the finite simple groups of Lie type. In particular, I calculate the essential p-dimension at the defining prime for the finite quasi-simple groups groups of classical Lie type and the essential l-dimension of the groups at a prime l, where $l \neq 2$ and $l \neq p$ (where p is the defining prime). I also calculate the essential 2-dimension for the linear groups in the case $q \equiv 1 \pmod 4$ and for the unitary groups in the case $q \equiv 3 \pmod 4$.

Fix a field k. The essential dimension of a finite group G, denoted $\mathrm{ed}_k(G)$, is the smallest number of algebraically independent parameters needed to define a Galois G-algebra over any field extension F/k (or equivalently G-torsors over $\mathrm{Spec}F$). In other words, the essential dimension of a finite group G is the supremum taken over all field extensions F/k of the smallest number of algebraically independent parameters needed to define a Galois G-algebra over F. The essential p-dimension of a finite group, denoted $\mathrm{ed}_k(G, p)$, is similar: the essential p-dimension of a finite group is the supremum taken over all fields F/k of the smallest number of algebraically independent parameters needed to define a Galois G-algebra over a field extension L/F of degree prime to p. See Section 2 for more formal definitions. See also [4] and [10] for more detailed discussions. For a discussion of some interesting applications of essential dimension and essential p-dimension, see [20].

What is the essential dimension of the finite simple groups? This question is quite difficult to answer. A few results for small groups (not necessarily simple) have been proven. For example, it is known that $\mathrm{ed}_k(S_5) = 2$, $\mathrm{ed}_k(S_6) = 3$ for k of characteristic not 2 [2], and $\mathrm{ed}_k(A_7) = \mathrm{ed}_k(S_7) = 4$ in characteristic 0 [5]. It is also known that for k a field of characteristic 0 containing all roots of unity, $\mathrm{ed}_k(G) = 1$ if and only if G is isomorphic to a cyclic group $\mathbb{Z}/n\mathbb{Z}$ or a dihedral group D_m where m is odd ([4], Theorem 6.2). Various bounds have also been proven. See [4], [13], [20],[16], among others. For a nice summary of the results known in 2010, see [20].

We can find a lower bound to this question by considering the corresponding question for essential p-dimension. The results in my thesis can be summarized in two main theorems:

Theorem 1.1. *Let p be a prime, k a field with char $k \neq p$. Then*

(1) (Theorem 4.1, Bardestani-Mallahi-Karai-Salmasian $p \neq 2$ [1], K. $p = 2$)

$$\mathrm{ed}_k(PSL_n(\mathbb{F}_{p^r}), p) = \mathrm{ed}_k(GL_n(\mathbb{F}_{p^r}), p) = rp^{r(n-2)}.$$

(2) (Theorem 5.1)

$$\mathrm{ed}_k(PSp(2n, p^r), p) = \mathrm{ed}_k(Sp(2n, p^r), p) = \begin{cases} rp^{r(n-1)}, & p \neq 2 \text{ or } n = 2 \\ r2^{r(n-1)-1}(2^{r(n-2)} + 1), & p = 2, n > 2 \end{cases}$$

(3) (Theorem 6.1)

$$\mathrm{ed}_k(P\Omega^{\epsilon}(n, p^r), p) = \mathrm{ed}_k(\Omega^{\epsilon}(n, p^r), p) = \begin{cases} r, & n = 3, p \neq 2 \\ 2r, & n = 4, \text{ any } p \\ rp^{2r(m-2)}, & n = 2m, \ n > 4, \text{ any } p \\ rp^{r(m-1)(m-2)} + rp^{r(m-1)}, & n = 2m+1, \ n \geq 5, \ p \neq 2 \end{cases}$$

Furthermore, $\mathrm{ed}_k(O^{\epsilon}(2m, 2^r), 2) = 1 + \mathrm{ed}_k(\Omega^{\epsilon}(2m, 2^r), 2)$*, and for* $p \neq 2$*,* $\mathrm{ed}_k(\Omega^{\epsilon}(n, p^r), p) = \mathrm{ed}_k(O^{\epsilon}(n, p^r), p)$*.*

Definition 1.2. For l a prime, $n \in \mathbb{Z}$, let $\nu_l(n)$ denote the highest power of l dividing n. And let $\mu_l(n)$ denote the the largest integer d such that $l^d \leq n$.

Theorem 1.3. *Let p be a prime, $q = p^r$, and l a prime with $l \neq p$. Let k be a field with char $k \neq l$. Let d be the smallest positive integer such that $l \mid q^d - 1$. Let $s = \nu_l(q^d - 1)$, and let $n_0 = \lfloor \frac{n}{d} \rfloor$. Assume that k contains a primitive l^s-th root of unity. Then*

(1) (Theorem 7.1) If $l = 2$, assume that $q \equiv 1 \pmod 4$. Then for all l,

$$\mathrm{ed}_k(GL_n(\mathbb{F}_q), l) = \sum_{k=0}^{\mu_l(n_0)} \left(\lfloor \frac{n_0}{l^k} \rfloor - l \lfloor \frac{n_0}{l^{k+1}} \rfloor \right) l^k$$

(2) *(Theorem 8.1) Let $\mu_l(n)'$ denote the smallest k such that $\lfloor \frac{n}{l^k} \rfloor - l \lfloor \frac{n}{l^{k+1}} \rfloor > 0$. If $l = 2$, assume that $q \equiv 1 \pmod 4$. Then for all l,*

$$\mathrm{ed}_k(SL_n(\mathbb{F}_q), l) = \begin{cases} \mathrm{ed}_k(GL_n(\mathbb{F}_q), l), & l \nmid q-1 \\ \mathrm{ed}_k(GL_n(\mathbb{F}_q), l) - l^{\mu_l(n)'}, & l \mid q-1 \end{cases}$$

(3) *(Theorem 9.1) If $l = 2$, assume that $q \equiv 1 \pmod 4$. Then for all l,*

$$\mathrm{ed}_k(PSL_n(\mathbb{F}_q), l) = \mathrm{ed}_k(SL_n(\mathbb{F}_q), l))$$

(4) *(Theorem 10.1) Let $n'|n$. If $l = 2$, assume that $q \equiv 1 \pmod 4$. Then for all l,*

$$\mathrm{ed}_k(SL_n(\mathbb{F}_q)/\{aI : a \in \mathbb{F}_q^\times, a^{n'} = 1\}, l) = \mathrm{ed}_k(PSL_n(\mathbb{F}_q)).$$

(5) *(Theorem 11.1) Assume that $l \neq 2$. Then for all l,*

$$\mathrm{ed}_k(PSp(2n, q), l) = \mathrm{ed}_k(Sp(2n, q), l) = \begin{cases} \mathrm{ed}_k(GL_{2n}(\mathbb{F}_q), l), & d \text{ even} \\ \mathrm{ed}_k(GL_n(\mathbb{F}_q), l), & d \text{ odd} \end{cases}$$

(6) *(Theorem 12.1) Assume that* $l \neq 2$. *Then*

$$\mathrm{ed}_k(P\Omega^\epsilon(n,q),l) = \mathrm{ed}_k(O^\epsilon(n,q),l) = \begin{cases} \mathrm{ed}_k(GL_m(\mathbb{F}_q),l), & n = 2m+1,\ d \text{ odd} \\ & \text{or } n = 2m, d \text{ odd}, \epsilon = + \\ \mathrm{ed}_k(GL_{m-1}(\mathbb{F}_q),l), & n = 2m, d \text{ odd}, \epsilon = - \\ \mathrm{ed}_k(GL_{2m}(\mathbb{F}_q),l), & n = 2m+1,\ d \text{ even} \\ & \text{or } n = 2m,\ d \text{ even}, \epsilon = +, n_0 \text{ even} \\ & \text{or } n = 2m, d \text{ even}, \epsilon = -, n_0 \text{ odd} \\ ed_k(GL_{2m-2}(\mathbb{F}_q),l), & n = 2m, d \text{ even}, \epsilon = +, n_0 \text{ odd} \\ & \text{or } n = 2m, d \text{ even}, \epsilon = -, n_0 \text{ even} \end{cases}$$

(7) *(Theorem 13.1) Assume that* $l \neq 2$. *Then*

$$\mathrm{ed}_k(U(n,q^2),l) = \begin{cases} \mathrm{ed}_k(GL_n(\mathbb{F}_{q^2}),l), & d = 2 \pmod 4 \\ \mathrm{ed}_k(GL_{\lfloor \frac{n}{2} \rfloor}(\mathbb{F}_{q^2}),l), & d \neq 2 \pmod 4 \end{cases}$$

(8) *(Theorem 14.1) Assume that* $l \neq 2$. *Then*

$$\mathrm{ed}_k(SU(n,q^2),l) = \begin{cases} \mathrm{ed}_k(U(n,q^2),l), & l \nmid q+1 \\ \mathrm{ed}_k(SL_n(\mathbb{F}_{q^2}),l), & l \mid q+1 \end{cases}$$

(9) *(Theorem 15.1) Assume that* $l \neq 2$. *Then*

$$\mathrm{ed}_k(PSU(n,q^2),l) = \begin{cases} \mathrm{ed}_k(SU(n,q^2),l), & l \nmid n \text{ or } l \nmid q+1 \\ \mathrm{ed}_k(PSL_n(\mathbb{F}_{q^2}),l), & l \mid n,\ l \mid q+1 \end{cases}$$

(10) *(Theorem 16.1) Assume that* $q \equiv 3 \pmod 4$, *and let* $s' = \nu_2(q+1)$. *Assume that* k *contains a primitive* $2^{s'}$*-th root of unity. Then*

$$\mathrm{ed}_k(U(n,q^2),2) = \sum_{k=0}^{\mu_2(n)} (\lfloor \frac{n}{2^k} \rfloor - 2\lfloor \frac{n}{2^{k+1}} \rfloor)2^k$$

(11) *(Theorem 16.2) Assume that* $q \equiv 3 \pmod 4$*, and let* $s' = \nu_2(q+1)$*. Assume that* k *contains a primitive* $2^{s'}$*-th root of unity. Let* $\mu_2(n)'$ *denote the smallest* k *such that* $\lfloor \frac{n}{2^k} \rfloor - \lfloor \frac{n}{2^{k+1}} \rfloor > 0$*. Then*

$$\mathrm{ed}_k(SU_n(\mathbb{F}_q),2) = \mathrm{ed}_k(U(n,q^2),2) - 2^{\mu_2(n)'}$$

(12) *(Theorem 16.3) Let* $p \neq 2$ *be a prime,* $q = p^r$*,* k *a field with char* $k \neq 2$*. Assume that* $q \equiv 3 \pmod 4$*, and let* $s' = \nu_2(q+1)$*. Assume that* k *contains a primitive* $2^{s'}$*-th root of unity.*

$$\mathrm{ed}_k(PSU(n,q^2),2) = \mathrm{ed}_k(SU(n,q^2),2).$$

Remark 1. In Theorem 5.1, for $p = 2, n = 2, r = 1$, we have $PSp(4,2)' \cong A_6$, and so $\mathrm{ed}_k(PSp(4,2)',2) = \mathrm{ed}_k(A_6,2) = 2$. Except for $p = 2, n = 2, r = 1$, $PSp(2n,p^r) = PSp(2n,p^r)'$ is simple. The methods of this thesis can recover the proof that $\mathrm{ed}_k(PSp(4,2),2) = \mathrm{ed}_k(S_6,2) = 3$ and that $\mathrm{ed}_k(PSp(4,2)',2) = \mathrm{ed}_k(A_6,2) = 2$, but for brevity, because these are known theorems, we will omit the proofs here.

Remark 2. If char $k = p$, then $\mathrm{ed}_k(G,p) = 1$ unless $p \nmid |G|$, in which case $\mathrm{ed}_k(G,p) = 0$ [22].

Remark 3. Dave Benson independently proved $\mathrm{ed}_{\mathbb{C}}(Sp(2n,p),p) = p^{n-1}$ for p odd ([3], Appendix A).

Remark 4. The following results were known prior to my work:

1. $\mathrm{ed}_{\mathbb{C}}(PSL_n(\mathbb{F}_{p^r},p)) = \mathrm{ed}_{\mathbb{C}}(GL_n(\mathbb{F}_{p^r})) = rp^{r(n-2)}$ for $p \neq 2$ ([1], Theorems 1.1 and 1.2).

2. Duncan and Reichstein calculated the essential p-dimension of the pseudo-reflection groups. These groups overlap with the groups above in a few small cases. See the appendix for the overlapping cases.

3. Reichstein and Shukla calculated the essential 2-dimension of double covers of the symmetric and alternating groups in characteristic $\neq 2$: Write $n = 2^{a_1} + \cdots + 2^{a_s}$, where

$a_1 > a_2 > \ldots > a_s \geq 0$. For $\tilde{S_n}$ a double cover of S_n, $\mathrm{ed}_k(\tilde{S_n}, 2) = 2^{\lfloor (n-s)/2 \rfloor}$, and for $\tilde{A_n}$ a double cover of A_n, $\mathrm{ed}_k(\tilde{A_n}, 2) = 2^{\lfloor (n-s-1)/2 \rfloor}$ ([21], Theorem 1.2). These groups overlap with the groups above in a few small cases: $\tilde{A_4} \cong SL_2(3)$, $\tilde{A_5} \cong SL_2(5)$, $\tilde{A_6} \cong SL_2(9)$, $\tilde{S_4^+} \cong GL_2(3)$.

Note. When calculating essential l-dimension we can assume without loss of generality that k contains a primitive l-th root of unity since adjoining an l-th root of unity gives an extension of degree prime to l. However, this is not the case for l^s. For example, the cyclotomic polynomial for adjoining a 9-th root of unity is $x^6 + x^3 + 1$, which has degree divisible by 3.

General Outline for Proofs

The key tools in the proofs of Theorem 1.1 are the Karpenko-Merkurjev Theorem (Theorem 1.4), a lemma of Meyer and Reichstein (Lemma 1.5), and Wigner Mackey Theory.

Theorem 1.4. *[Karpenko-Merkurjev [10], Theorem 4.1] Let G be a p-group, k a field with char $k \neq p$ containing a primitive p-th root of unity. Then $\mathrm{ed}_k(G, p) = \mathrm{ed}_k(G)$ and $\mathrm{ed}_k(G, p)$ coincides with the least dimension of a faithful representation of G over k.*

The Karpenko-Merkurjev Theorem allows us to translate the question for p-groups formulated in terms of extensions and transcendence degree into a question of representation theory.

Lemma 1.5. *[[15], Lemma 2.3] Let k be a field with char $k \neq p$ containing p-th roots of unity. Let H be a finite p-group and let ρ be a faithful representation of H of minimal dimension. Then ρ decomposes as a direct sum of exactly $r = \mathrm{rank}(Z(H))$ irreducible representations*

$$\rho = \rho_1 \oplus \ldots \oplus \rho_r.$$

and if χ_i are the central characters of ρ_i, then $\{\chi_i|_{\Omega_1(Z(H))}\}$ is a basis for $\widehat{\Omega_1}(Z(H))$ over k. ($\Omega_1(Z(H))$ is defined to be the largest elementary abelian p-group contained in $Z(H)$; see Definition 3.1.)

This lemma allows us to translate a question of analyzing faithful representations into a question of analyzing irreducible representations. Our main tool for the case at hand is Wigner-Mackey

Theory. This method from representation theory allows us to classify the irreducible representations for groups of the form $\Delta \rtimes L$ with Δ abelian. (See section 3.)

By Lemma 2.9, it suffices to consider the Sylow p-subgroups. By Corollary 2.12, we may assume that our field k contains p-th roots of unity. Then by the Karpenko-Merkurjev Theorem, we need to find the minimal dimension of a faithful representation of the Sylow p-subgroups. Throughout this thesis, we will use the notation $\mathrm{Syl}_p(G)$ to denote the set of Sylow p-subgroups of G. Let $S \in \mathrm{Syl}_p(G)$. By Lemma 1.5, if the center of S has rank s, a faithful representation ρ of S of minimal dimension decomposes as a direct sum

$$\rho = \rho_1 \oplus \ldots \oplus \rho_s$$

of exactly s irreducibles, and if χ_i are the central characters of ρ_i, then $\{\chi_i|_{\Omega_1(Z(S))}\}$ is a basis for $\widehat{\Omega_1}(Z(S))$ (see Definition 3.1).

Our proofs will follow the following steps:

- Step 1: Find the Sylow p-subgroups and their centers.
- Step 2: Classify the irreducible representations of the Sylow p-subgroups using Wigner-Mackey theory.
- Step 3: Construct upper and lower bounds using the classification in step 2.

Remark 5. For some of the more detailed calculations, see the appendix.

2 Essential p-Dimension Background

Fix a field k. Let G be a finite group, p a prime.

Definition 2.1. Let T : Fields$/k \to$ Sets be a functor. Let F/k be a field extension, and $t \in T(F)$. The *essential dimension of* t is

$$\mathrm{ed}_k(t) = \min_{F' \subset F \text{ s.t. } t \in Im(T(F') \to T(F))} \mathrm{trdeg}_k(F').$$

Definition 2.2. Let T : Fields$/k \to$ Sets be a functor. The *essential dimension of* T is

$$\mathrm{ed}_k(T) = \sup_{t \in T(F),\ F/k \in \mathrm{Fields}/k} \mathrm{ed}_k(t).$$

Definition 2.3. For G be a finite group, let $H^1(-;G)$: Fields$/k \to$ Sets be defined by

$$H^1(-;G)(F/k) = \{\text{the isomorphism classes of } G\text{-torsors over } \mathrm{Spec}F\}.$$

Definition 2.4. The *essential dimension of* G is

$$\mathrm{ed}_k(G) = \mathrm{ed}_k(H^1(-;G)).$$

Definition 2.5. Let T : Fields$/k \to$ Sets be a functor. Let F/k be a field extension, and $t \in T(F)$. The *essential* p*-dimension of* t is

$$\mathrm{ed}_k(t,p) = \min \mathrm{trdeg}_k(F'')$$

where the minimum is taken over all

$$\begin{aligned} F'' \subset F' \text{ a finite extension, with } F \subset F' \\ [F':F] \text{ finite s.t. } p \nmid [F':F] \text{ and} \\ \text{the image of } t \text{ in } T(F') \text{ is in } \mathrm{Im}(T(F'') \to T(F')) \end{aligned}$$

Note. $\mathrm{ed}_k(t,p) = \min_{F \subset F',\ p \nmid [F':F]} \mathrm{ed}_k(t|_{F'})$.

Definition 2.6. Let T : Fields$/k \to$ Sets be a functor. The *essential* p*-dimension of* T is

$$\mathrm{ed}_k(T,p) = \sup_{t \in T(F),\ F/k \in \mathrm{Fields}/k} \mathrm{ed}_k(t,p).$$

Definition 2.7. The *essential* p*-dimension of* G is

$$\mathrm{ed}_k(G,p) = \mathrm{ed}_k(H^1(-;G),p).$$

The next lemma follows directly from the definitions:

Lemma 2.8. *If $H \subset G$, then* $\mathrm{ed}_k(H,p) \leq \mathrm{ed}_k(G,p)$.

The key to proving the above lemma is that given a Galois H-algebra E over F, we can extend to a Galois G-algebra over F. See the appendix for the proof.

Lemma 2.9. *Let $S \in \mathrm{Syl}_p(G)$. Then* $\mathrm{ed}_k(G,p) = \mathrm{ed}_k(S,p)$.

The key to proving the above lemma is that given a Galois G-algebra E over F there exists an extension of F, $F_0 = E^H$, such that E is a Galois H-algebra over E^H. See the appendix for the proof.

The following lemma allows us to extend the underlying field k when calculating essential p-dimension, so long as the extension is of degree prime to p. In particular, this allows us to assume our field k contains p-th roots of unity (Corollary 2.12).

Lemma 2.10 ([10], Remark 4.8)**.** *If k a field of characteristic $\neq p$, k_1/k a finite field extension of degree prime to p, then* $\mathrm{ed}_k(G,p) = \mathrm{ed}_{k_1}(G,p)$.

(The idea for the lemma above was brought to my attention by Federico Scavia and Zinovy Reichstein.) The key to proving Lemma 2.10 is the fact that given a field extension F/k and a finite field extension k_1/k, $\mathrm{trdeg}_k(Fk_1) = \mathrm{trdeg}_k(F)$. See the appendix for the proof. Putting Lemma 2.10 together with Lemma 2.9, we get

Corollary 2.11. *If k_1/k a finite field extension of degree prime to p, $S \in \mathrm{Syl}_p(G)$, then* $\mathrm{ed}_k(G,p) = \mathrm{ed}_k(S,p) = \mathrm{ed}_{k_1}(S,p)$.

Corollary 2.12. *If k a field of characteristic $\neq p$, $S \in \mathrm{Syl}_p(G)$, ζ a primitive p-th root of unity, then*

$$\mathrm{ed}_k(G,p) = \mathrm{ed}_{k(\zeta)}(S,p).$$

Proof. Since ζ is a primitive p-th root of unity, ζ is a root of the polynomial $x^p - 1 = (x-1)(1+\ldots+x^{p-1})$. Then the minimal polynomial over a field of characteristic prime to p divides $1+\ldots+x^{p-1}$ and so has degree prime to p. So we have that $p \nmid [k(\zeta):k]$. $\square$

Note. By the corollary above, when calculating the essential p-dimension over a field k of characteristic $\neq p$, we may assume that k contains a primitive p-th root of unity.

The following theorem and corollary from [10] will also be useful for our approach:

Theorem 2.13 (Karpenko-Merkurjev [10], Theorem 5.1)**.** *Let G_1 and G_2 be two p-groups, k a field with char $k \neq p$ containing a primitive p-th root of unity, then* $\mathrm{ed}_k(G_1 \times G_2) = \mathrm{ed}_k(G_1) + \mathrm{ed}_k(G_2)$.

Corollary 2.14. *Let G be a finite abelian p-group, k a field with char $k \neq p$ containing a primitive p-th root of unity. Then* $\mathrm{ed}_k(G) = rank(G)$.

3 Representation Theory Background

Definition 3.1. Let H be a p-group. Define $\Omega_1(Z(H))$ (also called the socle of H) to be the largest elementary abelian p-group contained in $Z(H)$, i.e. $\Omega_1(Z(H)) = \{z \in Z(H) : z^p = 1\}$.

Definition 3.2. For G an abelian group, k a field, let $\widehat{G}$ denote the group of characters of G (homomorphisms from G to $k^\times$). We will use the notation $\widehat{\Omega_1}(Z(H))$ for the character group of $\Omega_1(Z(H))$.

The next lemma is due to Meyer-Reichstein [15] and reproduced in [1].

Lemma 3.3 ([15], Lemma 2.3)**.** *Let k be a field with char $k \neq p$ containing p-th roots of unity. Let H be a finite p-group and let $(\rho_i : H \to GL(V_i))_{1\leq i\leq n}$ be a family of irreducible representations of H with central characters χ_i. Suppose that $\{\chi_i|_{\Omega_1(Z(H))} : 1 \leq i \leq n\}$ spans $\widehat{\Omega_1}(Z(H))$. Then $\bigoplus_i \rho_i$ is a faithful representation of H.*

Note. For each of the groups $S \in \mathrm{Syl}_p(G)$ in sections 4-6, $\Omega_1(Z(S)) = Z(S)$, so we can ignore the Ω_1 in those sections.

Let $\mathbb{F}_{p^r}^+ \cong (\mathbb{Z}/p\mathbb{Z})^r$ denote the additive group of $\mathbb{F}_{p^r}$.

Definition 3.4. For k containing a p-th root of unity, fix a nontrivial character ψ of $\mathbb{F}_{p^r}^+ \to k$. For $b \in \mathbb{F}_{p^r}$, define $\psi_b(x) = \psi(bx)$.

Remark 6. The map given by $b \mapsto \psi_b$ is an isomorphism between $\mathbb{F}_{p^r}^+$ and $\widehat{\mathbb{F}_{p^r}^+}$.

We will use boldface $\mathbf{b}$ to denote elements in $(\mathbb{F}_{p^r})^m$ and $b_1, b_2, \ldots, b_m \in \mathbb{F}_{p^r}$ to denote the components.

Definition 3.5. Fix a nontrivial character ψ of $\mathbb{F}_{p^r}^+ \to k$. Fix m. For $\mathbf{b} = (b_j) \in (\mathbb{F}_{p^r}^+)^m$, define

$$\psi_{\mathbf{b}}(\mathbf{d}) = \prod_j (\psi_{b_j}(d_j)) \in \widehat{(\mathbb{F}_{p^r}^+)^m},$$

where b_j, d_j are the components of $\mathbf{b}, \mathbf{d}$.

Lemma 3.6. *For k containing a p-th root of unity, fix a nontrivial character ψ of $\mathbb{F}_{p^r}^+ \to k$. Then $\mathbf{b} \mapsto \psi_{\mathbf{b}}$ gives an isomorphism $(\mathbb{F}_{p^r}^+)^m \cong \widehat{(\mathbb{F}_{p^r}^+)^m}$, and $\psi_{\mathbf{b}}(\mathbf{d}) = \psi(\mathbf{b}\mathbf{d}^T)$.*

The Wigner-Mackey Little Group Method

The following exposition of Wigner-Mackey Theory follows [23] Section 8.2 and is also reproduced in [1] page 7: Let G be a finite group such that we can write $G = \Delta \rtimes L$ with Δ abelian. Let k be a field with char $k \nmid |G|$ such that all irreducible representations of Δ over k have degree 1. Then the irreducible characters of Δ form a group $\widehat{\Delta} = \mathrm{Hom}(\Delta, k^\times)$. The group G acts on $\widehat{\Delta}$ by

$$(\chi^g)(a) = \chi(gag^{-1}), \text{ for } g \in G, \chi \in \widehat{\Delta}, a \in \Delta.$$

Let $(\psi_s)_{\psi_s \in \widehat{\Delta}/L}$ be a system of representatives for the orbits of L in $\widehat{\Delta}$. For each ψ_s, let L_s be the subgroup of L consisting of those elements such that $l\psi_s = \psi_s$, that is $L_s = \mathrm{Stab}_L(\psi_s)$. Let $G_s = \Delta \cdot L_s$ be the corresponding subgroup of G. Extend ψ_s to G_s by setting

$$\psi_s(al) = \psi_s(a), \text{ for } a \in \Delta, l \in L_s.$$

Then since $l\psi_s = \psi_s$ for all $l \in L_s$, we see that ψ_s is a one-dimensional representation of G_s. Now let λ be an irreducible representation of L_s; by composing λ with the canonical projection $G_s \to L_s$ we obtain an irreducible representation λ of G_s, i.e

$$\lambda(al) = \lambda(l), \text{ for } a \in \Delta, l \in L_s.$$

Finally, by taking the tensor product of χ_s and λ, we obtain an irreducible representation $\psi_s \otimes \lambda$ of G_s. Let $\theta_{s,\lambda}$ be the corresponding induced representation of G, i.e. $\theta_{s,\lambda} := \mathrm{Ind}_{G_s}^{G}(\psi_s \otimes \lambda)$. The following is an extension of Proposition 25 in Chapter 8 of [23], it is called "Wigner-Mackey theory" in [1] (Theorem 4.2):

Theorem 3.7 (Venkataraman [26], Theorem 4.1; Serre (for $k = \mathbb{C}$) [23], Proposition 25)**.** *Under the above assumptions,*

(i) $\theta_{s,\lambda}$ *is irreducible.*

(ii) Every irreducible representation of G *is isomorphic to one of the* $\theta_{s,\lambda}$.

Venkataraman also proves a uniqueness statement: If $\theta_{s,\lambda}$ and $\theta_{s',\lambda'}$ are isomorphic, then $\psi_s = \psi'_s$ and λ is isomorphic to λ'. But we do not care about the uniqueness of the irreducible representations. In what follows, we will consider characters ψ_s with $\psi_s \in \widehat{\Delta}$ rather than $\psi_s \in \widehat{\Delta}/L$. The two points above still hold.

Note that in the cases considered in sections 4-6, the conditions hold so long as char $k \neq p$. Since we are considering the Sylow p-subgroups, this takes care of the first condition that char $k \nmid |G|$. All of our Sylow p-subgroups have the form $\Delta \rtimes L$ with $\Delta \cong (\mathbb{Z}/p\mathbb{Z})^N$ for some $N > 0$. By the note following Lemma 2.10, we may assume that k contains a primitive p-th root of unity. Thus we can conclude that all irreducible representations of Δ over k have degree 1.

The dimension is given by $\dim(\theta_{s,\lambda}) = \frac{|L|}{|L_s|}\dim(\lambda)$. If we pick $\lambda = 1$, then this will minimize the dimension of the representation and we will have $\dim(\theta_{s,1}) = \frac{|L|}{|L_s|}$. So for our purposes, we will only consider when $\lambda = 1$. The dimension of the representation will be minimized when $|L_s|$ is maximized.

4 The Linear Groups at the Defining Prime

In this section, we will prove that

Theorem 4.1 ([1] $p \neq 2$, K. $p = 2$)**.** *For any prime* p, k *a field such that char* $k \neq p$,

$$\mathrm{ed}_k(PSL_n(\mathbb{F}_{p^r}), p) = \mathrm{ed}_k(GL_n(\mathbb{F}_{p^r}), p) = rp^{r(n-2)}.$$

In this case, we will actually identify a subgroup (the Heisenberg subgroup) of a Sylow p-subgroup, to which Wigner-Mackey theory can be applied. This will give a lower bound for the essential p-dimension. We will find an upper bound by constructing a specific faithful representation (we will extend the minimal dimensional representation of the Heisenberg subgroup to a representation of the same dimension).

Definition 4.2. Define $\mathrm{Up}_n(\mathbb{F}_{p^r})$ to be the unitriangular $n \times n$ matrices over $\mathbb{F}_{p^r}$ under multiplciation. (Unitriangular matrices are upper triangular matrices with 1's on the diagonal).

The kernel of the natural homomorphism $GL_n(\mathbb{F}_{p^r}) \to PSL_n(\mathbb{F}_{p^r})$ has order prime to p, so it maps the Sylow p-subgroups of $GL_n(\mathbb{F}_{p^r})$ isomorphically onto Sylow p-subgroups of $PSL_n(\mathbb{F}_{p^r})$, so it suffices to consider the Sylow p-subgroups of $GL_n(\mathbb{F}_{p^r})$. It is straightforward to show the following two lemmas.

Lemma 4.3. *For all $n \geq 2$ and all primes p, we have* $\mathrm{Up}_n(\mathbb{F}_{p^r}) \in \mathrm{Syl}_p(GL_n(\mathbb{F}_{p^r}))$.

Lemma 4.4. *For all $n \geq 2$ and all primes p, we have*

$$Z(\mathrm{Up}_n(\mathbb{F}_{p^r})) = \{ \begin{pmatrix} 1 & 0 & \dots & 0 & a_{1,n} \\ 0 & 1 & 0 & \dots & 0 \\ & & \ddots & & \vdots \\ 0 & 0 & \dots & 1 & 0 \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \} \cong \mathbb{F}_{p^r}^{+} \cong (\mathbb{Z}/p\mathbb{Z})^r$$

Definition 4.5. Define the Heisenberg subgroup to be

$$H_n(\mathbb{F}_{p^r}) = \{ \begin{pmatrix} 1 & \mathbf{a} & x \\ \mathbf{0} & \mathrm{Id}_{n-2} & \mathbf{b}^T \\ 0 & \mathbf{0} & 1 \end{pmatrix} : x \in \mathbb{F}_{p^r}, \mathbf{a}, \mathbf{b} \in (\mathbb{F}_{p^r})^{n-2} \}.$$

It is a straightforward calculation to find the center.

Lemma 4.6. $Z(H_n(\mathbb{F}_{p^r})) = \{ \begin{pmatrix} 1 & \mathbf{0} & x \\ \mathbf{0} & Id_{n-2} & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \} = Z(\mathrm{Up}_n(\mathbb{F}_{p^r}))$.

Using Wigner-Mackey theory, in [1] the essential dimension of the Heisenberg subgroup is calculated for all p :

Theorem 4.7 ([1], Theorem 1.1)**.** *Let k be a field with char $k \neq p$. Then*

$$\mathrm{ed}_k(H_n(\mathbb{F}_{p^r})) = rp^{r(n-2)}$$

[1] assumes that $k = \mathbb{C}$, but by using Venkataram's extension of Wigner-Mackey theory, their proofs carry over to the case where char $k \neq p$. Now we will show that $\mathrm{Up}_n(\mathbb{F}_{p^r})$ has the same essential p-dimension of $H_n(\mathbb{F}_{p^r})$.

Theorem 4.8. *Let k be a field with char $k \neq p$. Then*

$$\mathrm{ed}_k(\mathrm{Up}_n(\mathbb{F}_{p^r})) = \mathrm{ed}_k(H_n(\mathbb{F}_{p^r}))$$

For $p \neq 2, k = \mathbb{C}$, this is a theorem of [1] (Theorem 1.2). Since $H_n(\mathbb{F}_{p^r}) \subset \mathrm{Up}_n(\mathbb{F}_{p^r})$, by Lemma 2.8

$$\mathrm{ed}_k(H_n(\mathbb{F}_{p^r})) \leq \mathrm{ed}_k(\mathrm{Up}_n(\mathbb{F}_{p^r})).$$

So it suffices to prove

$$\mathrm{ed}_k(\mathrm{Up}_n(\mathbb{F}_{p^r})) \leq \mathrm{ed}_k(H_n(\mathbb{F}_{p^r})).$$

We will do this by constructing a faithful representation of $\mathrm{Up}_n(\mathbb{F}_{p^r})$ of dimension $rp^{r(n-2)}$. A straightforward calculation shows the following.

Proposition 4.9. $\mathrm{Up}_n(\mathbb{F}_{p^r})$ *is isomorphic to* $H_n(\mathbb{F}_{p^r}) \rtimes \mathrm{Up}_{n-2}(\mathbb{F}_{p^r})$, *where the action of* $\mathrm{Up}_{n-2}(\mathbb{F}_{p^r})$ *on* $H_n(\mathbb{F}_{p^r})$ *is given by*

$$A\begin{pmatrix} 1 & \mathbf{a} & x \\ \mathbf{0} & Id_{n-2} & \mathbf{b}^T \\ 0 & \mathbf{0} & 1 \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{a}A^{-1} & x \\ \mathbf{0} & Id_{n-2} & (\mathbf{b}A^T)^T \\ 0 & \mathbf{0} & 1 \end{pmatrix}$$

for

$$A \in \mathrm{Up}_{n-2}(\mathbb{F}_{p^r}), \begin{pmatrix} 1 & \mathbf{a} & x \\ \mathbf{0} & Id_{n-2} & \mathbf{b}^T \\ 0 & \mathbf{0} & 1 \end{pmatrix} \in H_n(\mathbb{F}_{p^r}).$$

Proof of Theorem 4.8. By Corollary 2.12, we may assume that our field k contains p-th roots of unity. We will construct a faithful representation of $\mathrm{Up}_n(\mathbb{F}_{p^r})$ of dimension $rp^{r(n-2)}$: By Problem 6.18 in [9], every faithful irreducible representation of $H_n(\mathbb{F}_{p^r})$ can be extended to $\mathrm{Up}_n(\mathbb{F}_{p^r})$.

Fix ψ a non-trivial character of $\mathbb{F}_{p^r}^+$. Then the characters of $Z(H_n(\mathbb{F}_{p^r})) \cong \mathbb{F}_{p^r}^+$ are given by ψ_b for $b \in \mathbb{F}_{p^r}$, where ψ_b is defined by $\psi_b(d) = \psi(bd)$. Let $\{e_i\}$ be a basis for $\mathbb{F}_{p^r}^+$ over $\mathbb{F}_p$. For each i, let ρ_i be an irreducible representation of $H_n(\mathbb{F}_{p^r})$ with central character ψ_{e_i}. Then extend ρ_i to $\mathrm{Up}_n(\mathbb{F}_{p^r})$. Let $\rho = \bigoplus_i \rho_{e_i}$. Then ρ is a representation of $\mathrm{Up}_n(\mathbb{F}_{p^r})$ of dimension $rp^{r(n-2)}$. Since the set of all $\{\rho_{e_i}|_{Z(\mathrm{Up}_n(\mathbb{F}_{p^r}))} = \psi_{e_i}\}$ form a basis for $\widehat{\mathbb{F}_{p^r}^+}$, ρ is a faithful representation of $\mathrm{Up}_n(\mathbb{F}_{p^r})$ by Lemma 3.3.

□

5 The Symplectic Groups at the Defining Prime

In this section, we will show that

Theorem 5.1. *For k a field such that char $k \neq p$,*

$$\mathrm{ed}_k(PSp(2n, p^r), p) = \mathrm{ed}_k(Sp(2n, p^r), p) = \begin{cases} rp^{r(n-1)}, & p \neq 2 \text{ or } n = 2 \\ r2^{r(n-1)-1}(2^{r(n-2)} + 1), & p = 2, n > 2 \end{cases}$$

We do not prove the case $p = 2, n = 2, r = 1$, since it is already known that $\mathrm{ed}_k(PSp(4, 2)', 2) = \mathrm{ed}_k(A_6, 2) = 2$. In any other case, $PSp(2n, p^r)' = PSp(2n, p^r)$, so we obtain a complete calculation of $\mathrm{ed}_k(PSp(2n, p^r)', p)$.

Definitions

Definition 5.2. Let $S = \begin{pmatrix} 0 & \mathrm{Id}_n \\ -\mathrm{Id}_n & 0 \end{pmatrix}$. The symplectic groups are defined by

$$Sp(2n, p^r) := \{M \in GL_{2n}(\mathbb{F}_{p^r}) : M^T S M = S\},$$

and the projective symplectic groups are defined by

$$PSp(2n, p^r) := Sp(2n, p^r)/Z(Sp(2n, p^r)).$$

Note: A matrix $M = \begin{pmatrix} A & B \\ C & D \end{pmatrix} \in GL_{2n}(\mathbb{F}_{p^r})$ is symplectic if and only if $A^T C$, $B^T D$ are symmetric and $A^T D - C^T B = \mathrm{Id}_n$.

The Sylow p-subgroups and their centers

The kernel of the natural homomorphism $Sp(2n, p^r) \to PSp(2n, p^r)$ has order prime to p, so it maps the Sylow p-subgroups of $Sp(2n, p^r)$ isomorphically onto Sylow p-subgroups of $PSp(2n, p^r)$, so it suffices to consider the Sylow p-subgroups of $Sp(2n, p^r)$.

Definition 5.3. For any prime p, define $Sym(n, p^r)$ as the group of $n \times n$ symmetric matrices under addition (with entries from $\mathbb{F}_{p^r}$).

It is straightforward to show the following results. See the appendix for the calculations.

Lemma 5.4. *[See [18], Lemma 1] For any prime p, let*

$$S(p,n) = \{ \begin{pmatrix} A & 0_n \\ 0_n & (A^{-1})^T \end{pmatrix} \begin{pmatrix} Id_n & B \\ 0_n & Id_n \end{pmatrix} : A \in \mathrm{Up}_n(\mathbb{F}_{p^r}), B \in Sym(n, p^r)\}.$$

Then $S(p,n) \in \mathrm{Syl}_p(Sp(2n, p^r))$.

Corollary 5.5. *[See [19]] For any prime p, $S(p,n)$ the Sylow p-subgroup of $Sp(2n, p^r)$ defined in Lemma 5.4,*

$$S(p,n) \cong Sym(n, p^r) \rtimes \mathrm{Up}_n(\mathbb{F}_{p^r}),$$

where the action is given by $A(B) = ABA^T$, *where* $B \in Sym(n, p^r), A \in \mathrm{Up}_n(\mathbb{F}_{p^r})$.

Lemma 5.6. *For* $p \neq 2$, $S(p, n)$ *the Sylow* p*-subgroup of* $Sp(2n, p^r)$ *defined in Lemma 5.4,*

$$Z(S(p,n)) = \{\begin{pmatrix} Id_n & D \\ 0_n & Id_n \end{pmatrix} : D = \begin{pmatrix} d & \mathbf{0} \\ \mathbf{0} & 0_{n-1} \end{pmatrix}\} \cong \mathbb{F}_{p^r}^+ \cong (\mathbb{Z}/p\mathbb{Z})^r$$

Lemma 5.7. *For* $S(2, n)$ *the Sylow* p*-subgroup of* $Sp(2n, 2^r)$ *defined in Lemma 5.4,*

$$Z(S(2,n))$$
$$= \{\begin{pmatrix} Id_n & D \\ 0_n & Id_n \end{pmatrix} : D_{i,j} = 0, \text{ for all } (i,j) \notin \{(1,1),(1,2),(2,1), D_{1,2} = D_{2,1}\} \cong (\mathbb{F}_{2^r}^+)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$$

See the appendix for the calculations of the centers.

Classifying the irreducible representations

By Corollary 2.12, we may assume that our field k contains p-th roots of unity. We will use Wigner-Mackey Theory with $S(p, n) \cong Sym(n, p^r) \rtimes \mathrm{Up}_n(\mathbb{F}_{p^r})$ to compute the minimum dimension of an irreducible representation with non-trivial central character. So

$$\Delta = Sym(n, p^r), L = \mathrm{Up}_n(\mathbb{F}_{p^r}).$$

For

$$B = \begin{pmatrix} b_1 & b_2 & \dots & & b_n \\ b_2 & b_{n+1} & \dots & & b_{2n-1} \\ \vdots & & \ddots & & \vdots \\ b_{n-1} & \dots & & b_{n(n+1)/2-2} & b_{n(n+1)/2-1} \\ b_n & \dots & & b_{n(n+1)/2-1} & b_{n(n+1)/2} \end{pmatrix} \in Sym(n, p^r),$$

let $\mathbf{b} = (b_1, \dots, b_{n(n+1)/2})$. Then the map map $B \mapsto \mathbf{b}$ gives an isomorphism $Sym(n, p^r) \cong (\mathbb{F}_{p^r}^+)^{n(n+1)/2}$.

Fix ψ a non-trivial character of $\mathbb{F}_{p^r}^+$. By Lemma 3.6, there is an isomorphism between $(\mathbb{F}_{p^r}^+)^{n(n+1)/2}$ and $\widehat{(\mathbb{F}_{p^r}^+)^{n(n+1)/2}}$ given by sending $\mathbf{b} \in (\mathbb{F}_{p^r}^+)^{n(n+1)/2}$ to the character $\psi_{\mathbf{b}}$ defined by

$\psi_{\mathbf{b}}(\mathbf{d}) = \psi(\mathbf{b}\mathbf{d}^T)$. A straightforward computation shows that for $p \neq 2$, the characters extending a non-trivial central character are $\psi_{\mathbf{b}}$ with $b_1 \neq 0$. Similarly, a straighforward computation shows that for $p = 2$, the characters extending a non-trivial central character are $\psi_{\mathbf{b}}$ with $(b_1, b_2) \neq (0, 0)$, that is $b_1 \neq 0$ or $b_2 \neq 0$. Note that $H \in L_{\mathbf{b}}$ if and only if $\psi(\mathbf{b}\cdot(\mathbf{hdh^T} - \mathbf{d})) = 1$ for all $\mathbf{d} \in (\mathbb{F}_{p^r})^{n(n+1)/2}$, where $\mathbf{hdh^T}$ is the vector corresponding to HDH^T under the isomorphism $Sym(n, p^r) \cong (\mathbb{F}_{p^r}^+)^{n(n+1)/2}$. See the appendix for the full details of the computation.

The case $p \neq 2$

Proposition 5.8. *For $p \neq 2$,*

$$\min_{\mathbf{b} \in (\mathbb{F}_{p^r}^+)^{n(n+1)/2},\, b_1 \neq 0} \dim(\theta_{\mathbf{b},1}) = p^{r(n-1)}.$$

This minimum is achieved when $\mathbf{b} = (b, 0, \ldots, 0)$ with $b \neq 0$.

Proof. Recall that $\mathbf{b}, \mathbf{d}$ are vectors corresponding to matrices $B, D \in Sym(n, p^r)$ via the isomorphism defined above for $Sym(n, p^r) \cong (\mathbb{F}_{p^r}^+)^{n(n+1)/2}$ and $\mathbf{hdh^T}$ is the vector in $(\mathbb{F}_{p^r}^+)^{n(n+1)/2}$ corresponding to $HDH^T \in Sym(n, p^r)$ under the isomorphism $Sym(n, p^r) \cong (\mathbb{F}_{p^r}^+)^{n(n+1)/2}$.

We prove this proposition by showing that for $\mathbf{b} = (b_1, \cdots, b_{n(n+1)/2})$ with $b_1 \neq 0$, $|L_{\mathbf{b}}| \leq |\operatorname{Up}_{n-1}(\mathbb{F}_{p^r})| = p^{r(n-1)(n-2)/2}$. Pick $j_0 \neq 1$ and choose D with $d_{i,j} = 0$ except for d_{1,j_0} and let $\mathbf{d}$ be the corresponding vector. Then

$$\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = d_{1,j_0} \left(2h_{1,j_0} B_{1,1} + \sum_{i=2}^{j_0 - 1} h_{i,j_0} B_{1,i} \right).$$

So since we need $\psi(\mathbf{b} \cdot (\mathbf{hdh}^T - \mathbf{d})) = 1$ for all choices of $\mathbf{d}$, we can conclude that

$$h_{1,j_0} = \frac{-1}{2B_{1,1}} \sum_{i=2}^{j_0 - 1} h_{i,j_0} B_{1,i}.$$

So

$$|L_{\mathbf{b}}| \leq |\{H : H_{1,j} \text{ fixed } \forall j \neq 1\}| = |\operatorname{Up}_{n-1}(\mathbb{F}_{p^r})| = p^{r(n-1)(n-2)/2}$$

It is straightforward to show that for $\mathbf{b} = (b, 0, \ldots, 0)$,

$$L_{\mathbf{b}} = \{(0_n, H^{-1}) : H_{1,j} = 0, \forall j \neq 1\} \cong \mathrm{Up}_{n-1}(\mathbb{F}_{p^r}).$$

Thus the minimum is achieved when $\mathbf{b} = (b, 0, \ldots, 0)$.

$\square$

The case $p = 2$

Case 1: $\mathbf{n = 2}$

Proposition 5.9. *For $p = 2$, $n = 2$,*

$$\min_{\mathbf{b} \in (\mathbb{F}_{p^r}^+)^3,\ b_1 \neq 0, b_2 \neq 0} \dim(\theta_{\mathbf{b},1}) = 2^{r-1}.$$

This minimum is achieved when $\mathbf{b} = (b_1, b_2, 0)$ with $b_1 \neq 0, b_2 \neq 0$.

If $\mathbf{b} = (b_1, b_2, 0)$ with $b_1 \neq 0, b_2 \neq 0$, then

$$\dim(\theta_{\mathbf{b},1}) = 2^r.$$

Proof. The proof is similar to that for $p \neq 2$. We refer the reader to the appendix for full details. $\square$

Case 2: $\mathbf{n > 2}$

Proposition 5.10. *For $p = 2$, $n > 2$,*

$$\min_{\mathbf{b} \in (\mathbb{F}_{p^r}^+)^{n(n+1)/2},\ b_2 \neq 0} \dim(\theta_{\mathbf{b},1}) = 2^{r(2n-3)-1}.$$

This minimum is achieved when $\mathbf{b} = (b_i) = (b_1, b_2, 0, \ldots, 0)$ with $b_1, b_2 \neq 0$.

$$\min_{\mathbf{b} \in (\mathbb{F}_{p^r}^+)^{n(n+1)/2},\ b_1 \neq 0} \dim(\theta_{\mathbf{b},1}) = 2^{r(n-1)-1}.$$

This minimum is achieved when $\mathbf{b} = (b_i) = (b_1, 0, b_3, \ldots, 0)$ with $b_1, b_3 \neq 0$.

Proof. The proof is again similar. We refer the reader to the appendix for this proof. □

Note: For any $n > 2$ and any r, $2^{r(2n-3)-1} > 2^{r(n-1)-1}$.

Proof of Theorem 5.1

Proof. By Corollary 2.12, we may assume that our field k contains p-th roots of unity. So by Lemma 1.5, faithful representations of $S(p,n)$ of minimal dimension will decompose as a direct sum of exactly $r = \text{rank}(Z(S(p,n)))$ irreducible representations.

Case 1: $\mathbf{p \neq 2}$

Since the center of $S(p,n)$ has rank r and the minimum dimension of an irreducible representation with non-trivial central character is $p^{r(n-1)}$,

$$\text{ed}_k(PSp(2n,p^r),p) \geq rp^{r(n-1)}.$$

Let $\{e_i\}$ be a basis for $\mathbb{F}_{p^r}^+$ over $\mathbb{F}_p$, and let $s_i = (e_i, 0, \ldots, 0)$. Let $\rho = \bigoplus_i \theta_{s_i,1}$. Then by Proposition 5.8,

$$\dim(\rho) = rp^{r(n-1)}.$$

By Lemma 3.3, ρ is a faithful representation of $S(p,n)$. Thus

$$\text{ed}_k(PSp(2n,p^r),p) = rp^{r(n-1)}.$$

Case 2: $\mathbf{p = 2}$

Step 1: Find the lower bound

Subcase 1: $\mathbf{n = 2}$: Since the center has rank $2r$ and by Proposition 5.9 the minimum dimension of an irreducible representation with non-trivial central character is 2^{r-1},

$$\text{ed}_k(PSp(4,2^r)) \geq 2r2^{r-1} = r2^r.$$

Subcase 2: $\mathbf{n > 2}$: Let $\rho = \rho_i$ be a minimal dimensional faithful representation. Since the set of all central characters $\{\chi_i\}$ must form a basis for $\widehat{(\mathbb{F}_{p^r}^+)^2}$, we can conclude that $b_2 \neq 0$

for at least r of the ρ_i. So for these ρ_i minimum dimension is $2^{r(2n-3)-1}$, by Proposition 5.10. The other r may have $b_2 = 0$, so their minimum dimension is $2^{r(n-1)-1}$, by Proposition 5.10. Thus we have

$$\mathrm{ed}_k\left(PSp(2n,2^r),2\right) \geq r2^{r(2n-3)-1} + r2^{r(n-1)-1} = r2^{r(n-1)-1}(2^{r(n-2)}+1).$$

Step 2: Construct the upper bound

Let $\{e_i\}_{i=1}^{2r}$ be a basis for $\mathbb{F}_{2^r}^{+}$ over $\mathbb{F}_2$. Let x be a nonzero element in $\mathbb{F}_{2^r}$. We will choose subsets S of $\Delta = Sym(n,p^r)$ such that the set of all central characters of $\{\theta_{\mathbf{b},1}\}_{\mathbf{b}\in S}$ form a basis for the characters of the center. For $n=2$, let $S = \{(e_i,e_i,0),(x,e_i,0)\}_{i=1}^{2r}$. For $n>2$, let

$$S = \{(e_i,e_i,0,\ldots,0),(e_i,0,x,0,\ldots,0)\}_{i=1}^{2r}.$$

Let $\rho = \bigoplus_{\mathbf{b}\in S}\theta_{\mathbf{b},1}$. Then by Propositions 5.9 and 5.10,

$$\dim(\rho) = \sum_{\mathbf{b}\in S}\dim(\theta_{\mathbf{b},1}) = \begin{cases} r2^r, & n=2, r>1 \\ r2^{r(n-1)-1}(2^{r(n-2)}+1), & n>2 \end{cases}.$$

By Lemma 3.3, ρ is a faithful representation of $S(2,n)$. Steps 1 and 2 together give us that

$$\mathrm{ed}_k\left(PSp(2n,2^r),2\right) = \begin{cases} r2^r, & n=2, r>1 \\ r2^{r(n-1)-1}(2^{r(n-2)}+1), & n>2 \end{cases}.$$

□

6 The Orthogonal Groups at the Defining Prime

In this section, we will show the following theorem:

Theorem 6.1. *For $\epsilon \in \{\pm\}$ in the notation of Subsection 6, k a field such that char $k \neq p$,*

$$\mathrm{ed}_k(P\Omega^\epsilon(n,p^r),p) = \mathrm{ed}_k(\Omega^\epsilon(n,p^r),p) = \begin{cases} r, & n=3, p\neq 2 \\ 2r, & n=4,\ \textit{any } p \\ rp^{2r(m-2)}, & n=2m,\ n>4,\ \textit{any } p \\ rp^{r(m-1)(m-2)} + rp^{r(m-1)}, & n=2m+1,\ n\geq 5,\ p\neq 2 \end{cases}$$

Furthermore, $\mathrm{ed}_k(O^\epsilon(2m,2^r),2) = 1 + \mathrm{ed}_k(\Omega^\epsilon(2m,2^r),2)$, *and for $p \neq 2$,* $\mathrm{ed}_k(O^\epsilon(n,p^r),p) = \mathrm{ed}_k(\Omega^\epsilon(n,p^r),p)$.

We do not need to consider the case $n = 2m+1, p = 2$ since $O^\epsilon(2m+1,2^r) \cong Sp(2m,2^r)$ ([8], Theorem 14.2), so this case is taken care of in the work on the symplectic groups.

Definitions

The case $n = 2m, p \neq 2$

Let

$$A^+ = \begin{pmatrix} 0_m & \mathrm{Id}_m \\ \mathrm{Id}_m & 0_m \end{pmatrix}.$$

Let $\eta \in \mathbb{F}_{p^r}^\times$ be a non-square and let Id_m^η be the $m \times m$ identity matrix with the first entry replaced by η. Let

$$A^- = \begin{pmatrix} 0_m & \mathrm{Id}_m \\ \mathrm{Id}_m^\eta & 0_m \end{pmatrix}.$$

Definition 6.2. The orthogonal groups associated with A^+ are defined by

$$O^+(2m,p^r) := \{M \in GL(2m,\mathbb{F}_{p^r}) : M^T A^+ M = A^+\}.$$

The orthogonal groups associated with A^- are defined by

$$O^-(2m,p^r) := \{M \in GL(2m,\mathbb{F}_{p^r}) : M^T A^- M = A^-\}.$$

The special orthogonal groups are defined by

$$SO^{\epsilon}(2m, p^r) := \{M \in O^{\epsilon}(2m, p^r) : \det(M) = 1\}.$$

We define

$$\Omega^{\epsilon}(2m, p^r) := SO^{\epsilon}(2m, p^r)' \text{ (the commutator subgroup).}$$

Lastly, we define

$$P\Omega^{\epsilon}(2m, p^r) := \Omega^{\epsilon}(2m, p^r)/(\Omega^{\epsilon}(2m, p^r) \cap \{\pm \mathrm{Id}\}).$$

The case $n = 2m, p = 2$

For $\mathbf{x} = (x_i) \in \mathbb{F}_{p^r}^n$, let $Q^+(\mathbf{x}) = \sum_{i=1}^m x_i x_{i+m}$, and let

$$A_m^+ = \begin{pmatrix} 0_m & \mathrm{Id}_m \\ 0_m & 0_m \end{pmatrix}.$$

Then $Q^+(\mathbf{x}) = \mathbf{x} A_m^+ \mathbf{x}^T$. By Artin-Schreier theory, there exists $\eta \in \mathbb{F}_{2^r}$ such that $z^2 + z + \eta$ is irreducible in $\mathbb{F}_{2^r}[z]$.

Let

$$Q_m^-(\mathbf{x}) = \sum_{i=1}^m x_i x_{i+m} + x_m^2 + x_m x_{2m} + \eta x_{2m}^2$$

and define A_m^- to be

$$A_m^- = \begin{pmatrix} 0_m^1 & \mathrm{Id}_m \\ 0_m & 0_m^{\eta} \end{pmatrix}, \qquad \text{where } 0_m^1 = \begin{pmatrix} 0_{m-1} & \mathbf{0} \\ \mathbf{0} & 1 \end{pmatrix} \text{ and } 0_m^{\eta} = \begin{pmatrix} 0_{m-1} & \mathbf{0} \\ \mathbf{0} & \eta \end{pmatrix}.$$

Then $Q_m^-(x) = \mathbf{x} A_m^- \mathbf{x}^T$. So if we write $\mathbf{x} = (\mathbf{a}, b, \mathbf{c}, e)$ where $\mathbf{a}, \mathbf{c} \in \mathbb{F}_{2^r}^{m-1}, b, e \in \mathbb{F}_{2^r}$, then

$$Q_m^-(\mathbf{x}) = Q_{m-1}^+(\mathbf{a}, \mathbf{c}) + b^2 + be + \eta e^2 = \mathbf{a}\mathbf{c}^T + b^2 + be + \eta e^2.$$

Or if we write $\mathbf{x} = (\mathbf{y}, \mathbf{z})$ where $\mathbf{y}, \mathbf{z} \in \mathbb{F}_{2^r}^m$, then

$$Q_m^-(\mathbf{x}) = \mathbf{y}\mathbf{z}^T + y_m^2 + \eta z_m^2.$$

Definition 6.3. Define $O^\epsilon(2m, 2^r)$ as

$$O^\epsilon(2m, 2^r) := \{M \in GL(2m, \mathbb{F}_{2^r}) : Q^\epsilon(Mx) = Q^\epsilon(x) \text{ for all } x \in \mathbb{F}_{2^r}^{2m}\}.$$

Definition 6.4. Define $B^\epsilon(x, y) = Q^\epsilon(x + y) + Q^\epsilon(x) + Q^\epsilon(y)$, the bilinear form corresponding to Q^ϵ.

Note that $B^+(x, y) = \sum_{i=1}^m x_i y_{i+m} + \sum_{i=1}^m y_i x_{i+m}$. So the corresponding matrix is

$$S = \begin{pmatrix} 0 & \mathrm{Id}_m \\ \mathrm{Id}_m & 0 \end{pmatrix}.$$

That is, $B^+(x, y) = xSy^T$, and $B^-(x, y) = \sum_{i=1}^{m-1} x_i y_{i+m} + y_i x_{i+m} + x_m y_{2m} + y_m x_{2m}$. So the corresponding matrix is also S. That is, we have $B^-(x, y) = xSy^T = B^+(x, y)$, the same bilinear form as for A^+. Note that this is a nondegenerate alternating form and we have

$$O^\epsilon(2m, 2^r) \subset Sp(2m, 2^r),$$

where $Sp(2m, 2^r)$ is the symplectic group corresponding to S.

Definition 6.5. Define $\Omega^\epsilon(2m, 2^r) := O^\epsilon(2m, 2^r)'$ (the commutator subgroup).

For consistency, we make the following definition:

Definition 6.6. Define $P\Omega^\epsilon(2m, 2^r) := \Omega^\epsilon(2m, 2^r)/(\Omega^\epsilon(2m, 2^r) \cap \{\pm\mathrm{Id}\}) = \Omega^\epsilon(2m, 2^r)$.

Definition 6.7. The *Dickson invariant*, $\delta_{2m,2^r}^\epsilon$, is a homomorphism from $O^\epsilon(2m, 2^r)$ to $\mathbb{Z}/2\mathbb{Z}$ given by $\delta_{2m,2^r}^\epsilon(M) = \mathrm{rank}(\mathrm{Id}_{2m} - M) \mod 2$. Define

$$SO^\epsilon(2m, 2^r) := \ker \delta_{2m,2^r}^\epsilon.$$

Definition 6.8. Given $\epsilon \in \{\pm\}$, the Witt index w_ϵ is defined to be the dimension of a maximal totally isotropic subspace of $\mathbb{F}_{2^r}$ with respect to the quadratic form Q^ϵ.

Grove shows ([8], Proposition 14.41) that for Witt index $w_\epsilon > 0$, and $n \geq 2$,

$$\Omega^\epsilon(2m, 2^r) = O^\epsilon(2m, 2^r)' = SO^\epsilon(2m, 2^r)'.$$

He also shows ([8], Theorem 14.43) that if $m \geq 2$ and $(m, w_\epsilon) \neq (2, 2)$, then $\Omega^\epsilon(2m, 2^r)$ is simple.

The case $n = 2m + 1$

Let

$$L = \begin{pmatrix} -1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & 0_m & \mathrm{Id}_m \\ \mathbf{0} & \mathrm{Id}_m & 0_m \end{pmatrix}.$$

Definition 6.9. The odd orthogonal groups are defined by

$$O(2m+1, p^r) := \{M \in GL(2m+1, \mathbb{F}_{p^r}) : M^T L M = L\}.$$

The special orthogonal groups are defined by

$$SO(2m+1, p^r) := \{M \in O(2m+1, p^r) : \det(M) = 1\}$$

Define

$$\Omega(2m+1, p^r) := SO(2m+1, p^r)' \text{ (the commutator subgroup).}$$

The Sylow p-subgroups

Definition 6.10. For any prime p, define $Antisym(m, p^r)$ as the group of $m \times m$ anti-symmetric matrices under addition (with entries from $\mathbb{F}_{p^r}$).

Definition 6.11. For $p = 2$, define $Antisym_0(m, 2^r) \subset Antisym(m, 2^r) = Sym(m, 2^r)$ as the subgroup of symmetric/antisymmetric matrices with 0's on the diagonal. That is,

$$Antisym_0(m, 2^r) = \{B \in Sym(m, 2^r) = Antisym(m, 2^r) : B_{i,i} = 0, \ \forall i\}.$$

The case $n = 2m$

For $p \neq 2$, the Sylow p-subgroups of $P\Omega^\epsilon(2m, p^r)$, $\Omega^\epsilon(2m, p^r)$, and $O^\epsilon(2m, p^r)$ are isomorphic, so it suffices to consider the Sylow p-subgroups of $\Omega^\epsilon(2m, p^r)$. (We do this for notational purposes so we can combine the arguments with the case $p = 2$.) A direct computation shows the following.

Lemma 6.12. *[See [18], [12]] For* $p \neq 2$, $\epsilon = +$, *let*

$$S^+(p, 2m) = \{\begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} Id_m & B \\ 0_m & Id_m \end{pmatrix} : A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), B \in Antisym(m, p^r)\}.$$

and for $p \neq 2, \epsilon = -$, *let*

$$S^-(p, 2m) = \{\begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} Id_m & 0_m \\ C & Id_m \end{pmatrix} : A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), C \in Antisym(m, p^r)\}.$$

Then $S^+(p, 2m)$ *is isomorphic to the elements in* $\mathrm{Syl}_p(\Omega^+(2m, p^r))$ *and* $S^-(p, 2m)$ *is isomorphic to the elements in* $\mathrm{Syl}_p(\Omega^-(2m, p^r))$.

Corollary 6.13. *For* $p \neq 2$, $S^\epsilon(p, 2m)$ *as defined in Lemma 6.12,* $\epsilon \in \{\pm\}$,

$$S^\epsilon(p, 2m) \cong Antisym(m, p^r) \rtimes \mathrm{Up}_m(\mathbb{F}_{p^r}),$$

where the action is given by $A(B) = ABA^T$.

Since $S^+(p, 2m) \cong S^-(p, 2m)$, it suffices to consider $S^+(p, 2m)$. For the sake of simplicity of notation, let $S(p, 2m) = S^+(p, 2m)$.

Lemma 6.14. *Let*

$$S(2,2m) = \{ \begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} Id_m & B \\ 0_m & Id_m \end{pmatrix} : A \in \mathrm{Up}_m(\mathbb{F}_{2^r}), B \in Antisym_0(m, 2^r)\}.$$

Then $S(2,2m) \in \mathrm{Syl}_2(\Omega^\epsilon(2m, 2^r))$ *for* $\epsilon \in \{\pm\}$*.*

Corollary 6.15. *For* $S(2,2m)$ *as defined in Lemma 6.14,*

$$S(2,2m) \cong Antisym_0(m, 2^r) \rtimes \mathrm{Up}_m(\mathbb{F}_{2^r}),$$

where the action is given by $A(B) = ABA^T$*.*

The above lemma is slightly more involved, see the appendix for the details.

The case $n = 2m+1, p \neq 2$

The kernel of the natural homomorphism $O(2m+1, p^r) \to \Omega(2m+1, p^r)$ has order prime to p, so it maps the Sylow p-subgroups of $O(2m+1, p^r)$ isomorphically onto Sylow p-subgroups of $\Omega(2m+1, p^r)$, so it suffices to consider the Sylow p-subgroups of $O(2m+1, p^r)$.

It is straightforward to show the following:

Lemma 6.16. *For* $p \neq 2$*, let*

$$S(p, 2m+1)$$
$$= \{ \begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & Id_m & 0_m \\ \mathbf{0} & 0_m & Id_n \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & A & 0_m \\ \mathbf{0} & 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & Id_m & B \\ \mathbf{0} & \mathbf{0} & Id_m \end{pmatrix} : \mathbf{x} \in \mathbb{F}_{p^r}^m, A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), B \in Antisym(m, p^r)\}.$$

Then $S(p, 2m+1) \in \mathrm{Syl}_p(O(2m+1, p^r))$*.*

Corollary 6.17. *For* $p \neq 2$*,*

$$S(p, 2m+1) \cong \big((\mathbb{F}_{p^r}^+)^m \times Antisym(m, p^r)\big) \rtimes \mathrm{Up}_m(\mathbb{F}_{p^r})),$$

where the action of $\mathrm{Up}_m(\mathbb{F}_{p^r})$ *on* $Antisym(m, p^r)$ *is given by* $A(B) = ABA^T$*. and the action of* $\mathrm{Up}_m(\mathbb{F}_{p^r})$ *on* $(\mathbb{F}_{p^r}^+)^m$ *is given by* $A(\mathbf{x}) = \mathbf{x}A^T$*.*

The centers

For $n=3$, $Antisym(1,p^r)$ and $\mathrm{Up}_1(\mathbb{F}_{p^r})$ are trivial, so we have $S(p,3)\cong\mathbb{F}_{p^r}^{+}$, which is abelian. For $n=4$, the action of $\mathrm{Up}_2(\mathbb{F}_{p^r})\cong\mathbb{F}_{p^r}$ on $Antisym(2,p^r)\cong\mathbb{F}_{p^r}$ is trivial and so $S(p,n)\cong\mathbb{F}_{p^r}\times\mathbb{F}_{p^r}$. Thus the Sylow p-subgroup is abelian.

Lemma 6.18. *For any prime p, $m>2$, let $S(p,2m)=S^{+}(p,2m)$ be defined as in Lemmas 6.12 and 6.14. Then*

$$Z(S(p,2m))=\{\begin{pmatrix} Id_m & D \\ 0_m & Id_m \end{pmatrix} : D=\begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix}\}\cong\mathbb{F}_{p^r}^{+}\cong(\mathbb{Z}/p\mathbb{Z})^r$$

Lemma 6.19. *For $p\neq 2$, $m\geq 2$, $S(p,2m+1)$ defined as in Lemma 6.16,*

$$Z(S(p,2m+1))=\{\begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & Id_m & D \\ \mathbf{0} & 0_m & Id_m \end{pmatrix} : \mathbf{x}=(x_1,0,\ldots,0), D=\begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix}\}\cong(\mathbb{F}_{p^r}^{+})^2$$

For the calculations of the centers, see the appendix.

Classifying the irreducible representations

By Corollary 2.12, we may assume that our field k contains p-th roots of unity.

The case $n=2m$

We will use Wigner-Mackey Theory with

$$S(p,2m)\cong\begin{cases} Antisym(m,p^r)\rtimes\mathrm{Up}_m(\mathbb{F}_{p^r}) & p\neq 2 \\ Antisym_0(m,2^r)\rtimes\mathrm{Up}_m(\mathbb{F}_{2^r}) & p=2 \end{cases}$$

to see what is the minimum dimension of an irreducible representation with non-trivial central character. So

$$\Delta = \begin{cases} Antisym(m, p^r) & p \neq 2 \\ Antisym_0(m, 2^r) & p = 2 \end{cases} \cong (\mathbb{F}_{p^r}^+)^{m(m-1)/2}, \qquad L = \mathrm{Up}_m(\mathbb{F}_{p^r}).$$

For

$$B = \begin{pmatrix} 0 & b_1 & \cdots & & b_{m-1} \\ -b_1 & 0 & b_m & \cdots & b_{2m-3} \\ \vdots & & \ddots & & \vdots \\ -b_{m-2} & \cdots & & 0 & b_{m(m-1)/2} \\ -b_{m-1} & \cdots & & -b_{m(m-1)/2} & 0 \end{pmatrix} \in \begin{cases} Antisym(m, p^r), & p \neq 2 \\ Antisym_0(m, p^r), & p = 2 \end{cases}$$

let $\mathbf{b} = (b_1, \cdots, b_{m(m-1)/2})$. (When $p = 2$, the negatives go away.) Then the map $B \mapsto \mathbf{b}$ gives an isomorphism $\begin{cases} Antisym(m, p^r), & p \neq 2 \\ Antisym_0(m, p^r), & p = 2 \end{cases} \cong (\mathbb{F}_{p^r}^+)^{m(m-1)/2}$.

Fix ψ a non-trivial character of $\mathbb{F}_{p^r}^+$. By Lemma 3.6, there is an isomorphism between $(\mathbb{F}_{p^r}^+)^{m(m-1)/2}$ and $\widehat{(\mathbb{F}_{p^r}^+)^{m(m-1)/2}}$ given by sending $\mathbf{b} \in (\mathbb{F}_{p^r}^+)^{m(m-1)/2}$ to the character $\psi_{\mathbf{b}}$ defined by $\psi_{\mathbf{b}}(\mathbf{d}) = \psi(\mathbf{b}\mathbf{d}^T)$. As for the symplectic groups, a straightforward computation shows that for any prime p, the characters extending a non-trivial central character are $\psi_{\mathbf{b}}$ with $b_1 \neq 0$. Note that $H \in L_{\mathbf{b}}$ if and only if $\psi(\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1$ for all $\mathbf{d} \in (\mathbb{F}_{p^r}^+)^{m(m-1)/2}$, where $\mathbf{hdh^T}$ is the vector in $(\mathbb{F}_{p^r}^+)^{m(m-1)/2}$ corresponding to $HDH^T \in Sym(m, p^r)$ under the isomorphsim $Sym(m, p^r) \cong (\mathbb{F}_{p^r}^+)^{m(m-1)/2}$. See the appendix for the full details of the computation.

Proposition 6.20. *For any prime p,*

$$\min_{\mathbf{b} \in (\mathbb{F}_{p^r}^+)^{m(m-1)/2},\ b_1 \neq 0} \dim(\theta_{\mathbf{b},1}) = p^{2r(m-2)}.$$

This minimum is achieved when $\mathbf{b} = (b, 0, \ldots, 0)$ with $b \neq 0$.

Proof. Recall that $\mathbf{b}, \mathbf{d}$ are vectors corresponding to matrices $B, D \in \Delta$ via the isomorphism

$\Delta \cong (\mathbb{F}_{p^r}^+)^{m(m-1)/2}$ and $\mathbf{hdh^T}$ is the vector in $(\mathbb{F}_{p^r}^+)^{m(m-1)/2}$ corresponding to $HDH^T \in Antisym(m,p^r)$ under the isomorphism $Antisym(m,p^r) \cong (\mathbb{F}_{p^r}^+)^{m(m-1)/2}$.

Calculation 1. For $j_0 > 2$, choosing $d_{i,j} = 0$ except for $d_{1,j_0} = -d_{j_0,1}$ and performing similar calculations to those for Propostion 5.8, we get that

$$\sum_{i=2}^{j_0-1} h_{i,j_0} B_{1,i} = 0.$$

For $2 \le k \le n$, if $B_{1,k} \neq 0$, we can solve for h_{k,j_0} in terms of h_{i,j_0} for $i \neq 1, k$. If particular, since $B_{1,2} = b_1 \neq 0$, we can solve for h_{2,j_0} in terms of h_{i,j_0} with $i > 2$.

Calculation 2. For $j_0 > 2$, choose $d_{i,j} = 0$ except for $d_{2,j_0} = -d_{j_0,2}$, and again performing similar calculations to those for Propostion 5.8, we get

$$-B_{1,2}h_{1,j_0} + \sum_{i=2}^{j_0} B_{1,i}h_{i,j_0}h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,i}h_{i,j_0} = 0.$$

Since $B_{1,2} = b_1 \neq 0$, we can solve for h_{1,j_0} in terms of $h_{1,2}$ and h_{i,j_0} with $i > 2$.

Putting these two calculations together, we can conclude that for all $\mathbf{b} = (b_i)$ with $b_1 \neq 0$,

$$|L_{\mathbf{b}}| \le |\{H : H_{2,j} \text{ fixed }, \forall j > 2, H_{1,j} \text{ fixed }, \forall j > 2\}| = |\mathbb{F}_{p^r}| \cdot |U_{m-2}(\mathbb{F}_{p^r})| = p^{r[(m-2)(m-3)/2+1]}.$$

We leave to the reader the verification that the minimum is achieved for $\mathbf{b} = (b, 0, \ldots, 0)$. □

For more details of the above proof, see the appendix.

The case $n = 2m+1$, $p \neq 2$

We will use Wigner-Mackey Theory with $S(p, 2m+1) \cong \big((\mathbb{F}_{p^r}^+)^m \times Antisym(m,p^r)\big) \rtimes \mathrm{Up}_m(\mathbb{F}_{p^r})$ to compute the minimum dimension of an irreducible representation with non-trivial central character. So we have

$$\Delta = \big((\mathbb{F}_{p^r}^+)^m \times Antisym(m,p^r)\big) \rtimes \{\mathrm{Id}_m\},$$

$$L = (\{\mathbf{0} \times \{0_m\}\}) \rtimes \mathrm{Up}_m(\mathbb{F}_{p^r}).$$

We obtain an isomorphism $(\mathbb{F}_{p^r}^+)^m \times Antisym(m,p^r) \cong (\mathbb{F}_{p^r}^+)^{m+m(m-1)/2}$ by sending $(\mathbf{a}, B)$ to $(\mathbf{a}, \mathbf{b})$, where $\mathbf{b}$ is the image of B under the isomorphism $Antisym(m,p^r) \cong (\mathbb{F}_{p^r}^+)^{m(m-1)/2}$ defined at the beginning of 6.

Fix ψ a non-trivial character of $\mathbb{F}_{p^r}^+$. By Lemma 3.6, there is an isomorphsim between $(\mathbb{F}_{p^r}^+)^{m+m(m-1)/2}$ and $(\mathbb{F}_{p^r}^+)^{\widehat{m+m(m-1)/2}}$ given by sending $(\mathbf{a},\mathbf{b}) \in (\mathbb{F}_{p^r}^+)^{m+m(m-1)/2}$ to the character $\psi_{\mathbf{a},\mathbf{b}}$ defined by $\psi_{\mathbf{a},\mathbf{b}}(\mathbf{c},\mathbf{d}) = \psi((\mathbf{a},\mathbf{b})(\mathbf{c},\mathbf{d})^T)$. As above, a straightforward computation shows that the characters of $(\mathbb{F}_{p^r})^{m+m(m-1)/2}$ extending a non-trivial central character of the Sylow p-subgroup are $\psi_{\mathbf{a},\mathbf{b}}$ with $(a_1, b_1) \neq (0,0)$. Note that $H \in L_{(\mathbf{a},\mathbf{b})}$ if and only if

$$\psi(\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x}) + \mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1$$

for all $(\mathbf{x},\mathbf{d}) \in (\mathbb{F}_{p^r})^{m+m(m-1)/2}$, where $\mathbf{hdh^T}$ is the vector in $(\mathbb{F}_{p^r}^+)^{m+m(m-1)/2}$ corresponding to $HDH^T \in (\mathbb{F}_{p^r}^+)^m \times Antisym(m,p^r)$ under the isomorphism $(\mathbb{F}_{p^r}^+)^m \times Antisym(m,p^r) \cong (\mathbb{F}_{p^r}^+)^{m+m(m-1)/2}$.

Proposition 6.21. *For $p \neq 2$,*

$$\min_{(\mathbf{a},\mathbf{b}) \in (\mathbb{F}_{p^r}^+)^{m+m(m-1)/2},\ b_1 \neq 0} \dim(\theta_{(\mathbf{a},\mathbf{b}),1}) = p^{r(m-1)(m-2)}.$$

This minimum is achieved when $\mathbf{a} = \mathbf{0}, \mathbf{b} = (b_1, 0, \ldots, 0)$ with $b_1 \neq 0$. Similarly,

$$\min_{(\mathbf{a},\mathbf{b}) \in (\mathbb{F}_{p^r}^+)^{m+m(m-1)/2},\ a_1 \neq 0} \dim(\theta_{(\mathbf{a},\mathbf{b}),1}) = p^{r(m-1)}.$$

This minimum is achieved when $\mathbf{a} = (a_1, 0, \ldots, 0), \mathbf{b} = \mathbf{0}$ with $a_1 \neq 0$.

Proof.

Case 1: $\mathbf{b_1 \neq 0}$

If we take $\mathbf{x} = 0$, then $\psi(\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x})) + \mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1$ reduces to the condition for $\Omega^+(2m, p^r)$. So $L_{(\mathbf{a},\mathbf{b})}$ must be a subset of the $L_{\mathbf{b}}$ calculated in Proposition 6.20. Thus

$$|L_{(\mathbf{a},\mathbf{b})}| \leq |\{H : H_{2,j} \text{ fixed } , \forall j > 2, H_{1,j} \text{ fixed } , \forall j > 2\}| = p^{r[(m-2)(m-3)/2+1]}.$$

It is straightforward to show that for $\mathbf{a} = \mathbf{0}$, $\mathbf{b} = (b_1, 0, \ldots, 0)$,

$$L_{(\mathbf{a},\mathbf{b})} = \{H \in \mathrm{Up}_m(\mathbb{F}_{p^r}) : H_{1,j} = 0, \forall j \neq 2, H_{2,j} = 0, \forall j > 2\}.$$

Hence the minimum is achieved for $\mathbf{a} = \mathbf{0}$, $\mathbf{b} = (b_1, 0, \ldots, 0)$.

Case 2: $\mathbf{a_1} \neq \mathbf{0}$

If we take $\mathbf{d} = \mathbf{0}$ then $\psi(\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x}) + \mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1$ reduces to $\psi(\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x})) = 1$. Note that

$$\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x}) = \sum_{k=1}^{m-1} a_k \cdot (\sum_{j=k+1}^{m} x_j h_{k,j})$$

For $j_0 > 1$, choose $x_i = 0$ except for x_{j_0}. Then we get that

$$\sum_{k=1}^{j_0-1} a_k h_{k,j_0} = 0.$$

So if $a_1 \neq 0$, we can solve for h_{1,j_0} in terms of $h_{i,j_0}, i \neq 1, k$. Hence

$$|L_{(\mathbf{a},\mathbf{b})}| \leq |\{H : H_{1,j} \text{ fixed } \forall j \neq 1\} = |\,\mathrm{Up}_{n-1}(\mathbb{F}_{p^r})| = p^{r(n-1)(n-2)/2}.$$

It is straightforward to show that for $\mathbf{a} = (a_1, 0, \ldots, 0)$, $\mathbf{b} = \mathbf{0}$,

$$L_{(\mathbf{a},\mathbf{b})} = \{H : H_{1,j} = 0, \forall j \neq 1\}.$$

Hence the minimum is the minimum is achieved for $\mathbf{a} = (a_1, 0, \ldots, 0)$, $\mathbf{b} = \mathbf{0}$.

□

Again, for more details see the appendix. For $O^\epsilon(2m, 2^r)$, note that $\langle -\mathrm{Id} \rangle \times S(2, 2m)$ is a

Sylow 2-subgroup of $O^\epsilon(2m, 2^r)$. Thus

$$\mathrm{ed}_k(O^\epsilon(2m, 2^r), 2) = 1 + \mathrm{ed}_k(\Omega^\epsilon(2, 2^r), 2).$$

Proof of Theorem 6.1

Proof. By Lemma 1.5, faithful representations of $S(p, n)$ of minimal dimension will decompose as a direct sum of exactly $r = \mathrm{rank}(Z(S(p, n)))$ irreducible representations. We will complete the proof for four separate cases.

Case 1: $\mathbf{n = 3, p \neq 2}$

For $n = 3, p \neq 2$, $S(p, 3) \cong \mathbb{F}_{p^r}^+$, and thus $\mathrm{ed}_k(S(p, 3)) = \mathrm{ed}_k(\mathbb{F}_{p^r}^+) = r$.

Case 2: $\mathbf{n = 4}$

For $p \neq 2$, the action of $\mathrm{Up}_2(\mathbb{F}_{p^r}) \cong \mathbb{F}_{p^r}$ on $Antisym(2, p^r) \cong \mathbb{F}_{p^r}^+$ is trivial, and so $S^+(p, 4) \cong \mathbb{F}_{p^r}^+ \times \mathbb{F}_{p^r}^+$. So $\mathrm{ed}_k(S^+(p, 4)) = \mathrm{ed}_k(\mathbb{F}_{p^r}^+ \times \mathbb{F}_{p^r}^+) = 2r$.

Similarly for $n = 4$, $p = 2$, $S^+(2, 4) \cong \mathbb{F}_{2^r} \times \mathbb{F}_{2^r}^+$. So $\mathrm{ed}_k(S^+(2, 4)) = \mathrm{ed}_k(\mathbb{F}_{2^r}^+ \times \mathbb{F}_{2^r}^+) = 2r$.

Note: The work in the previous section is valid, though unnecessary, for $n = 4$. It gives us that the minimum dimension of an irreducible representation is 1. Then since the center has rank $2r$, we will get an essential dimension of $2r$.

Case 3: $\mathbf{n = 2m, m > 2}$

Since the center has rank r and the minimum dimension of an irreducible representation with non-trivial central character is $p^{2r(m-2)}$,

$$\mathrm{ed}_k(\Omega^+(2m, p^r), p) \geq rp^{2r(m-2)},$$

Let $\{e_i\}$ be a basis for $\mathbb{F}_{p^r}^+$ over $\mathbb{F}_p$, and let $s_i = (e_i, 0, \ldots, 0)$. Let $\rho = \bigoplus_i \theta_{s_i,1}$. Then by Proposition 6.20,

$$\dim(\rho) = \sum_{i=1}^{r} \dim(\theta_{s_i,1}) = rp^{2r(m-2)}.$$

By Lemma 3.3, ρ is a faithful representation of $S^+(p, 2m)$. Therefore

$$ed_k(\Omega^\epsilon(2m, p^r), p) = rp^{2r(m-2)}.$$

Case 4: $\mathbf{n = 2m+1, p \neq 2}$

Let $\rho = \rho_i$ be a minimal dimensional faithful representation. Since the set of all central characters $\{\chi_i\}$ must form a basis for $Z(S(\widehat{p, 2m}+1))$, we can conclude that $b_1 \neq 0$ for at least r of the $\chi_i = \psi_{\mathbf{b}}$, and so the dimension is at least $p^{r(m-1)(m-2)}$. The other r may have $b_1 = 0$ but then we must have $a_1 \neq 0$, so their minimum dimension is $p^{r(m-1)}$. Thus

$$\mathrm{ed}_k\left(S(p, 2m+1)\right) \geq rp^{r(m-1)(m-2)} + rp^{r(m-1)}.$$

Let $\{e_i\}$ be a basis for $\mathbb{F}_{p^r}^{+}$ over $\mathbb{F}_p$, and let $S = \{(e_i, 0, \ldots, 0), (0, \ldots, 0, e_i, 0, \ldots, 0)\}$. Let $\rho = \bigoplus_{s \in S} \theta_{s,1}$. Then by Proposition 6.21,

$$\dim(\rho) = \sum_{s \in S} \dim(\theta_{s,1}) = rp^{r(m-1)(m-2)} + rp^{r(m-1)}.$$

By Lemma 3.3, ρ is a faithful representation of $S(p, 2m+1)$. Therefore

$$\mathrm{ed}_k(\Omega^{\epsilon}(2m, p^r), p) = rp^{r(m-1)(m-2)} + rp^{r(m-1)}.$$

□

7 The General Linear Groups at Non-defining Primes

In this section, we will prove the following theorem:

Theorem 7.1. *Let p be a prime, $q = p^r$, and l a prime with $l \neq p$. Let k be a field with char $k \neq l$. Let d be the smallest positive integer such that $l \mid q^d - 1$. Let $s = \nu_l(q^d - 1)$. Assume that k contains a primitive l^s-th root of unity. Let $n_0 = \lfloor \frac{n}{d} \rfloor$. If $l = 2$, assume that $q \equiv 1$* (mod 4)*. Then for all l,*

$$\mathrm{ed}_k(GL_n(\mathbb{F}_q), l) = \sum_{k=0}^{\mu_l(n_0)} \left(\lfloor \frac{n_0}{l^k} \rfloor - l \lfloor \frac{n_0}{l^{k+1}} \rfloor \right) l^k,$$

The p-Sylow and its center

Definition 7.2. Let $|G|_l = \nu_l(|G|)$; i.e. $|G|_l$ is the order of a Sylow l-subgroup of G.

By ([25], Lemma 3.1), for $l \neq 2$,

$$|GL_n(\mathbb{F}_q)|_l = l^{sn_0 + \lfloor \frac{n_0}{l} \rfloor + \lfloor \frac{n_0}{l^2} \rfloor + \cdots}.$$

And by ([25], Theorem 3.7),

$$|GL_n(\mathbb{F}_q)|_2 = (2^s)^n \cdot 2^{\nu_2(n!)}.$$

Note that in both these cases, we have for any l,

$$|GL_n(\mathbb{F}_q)|_l = l^{sn_0} \cdot |S_{n_0}|_l.$$

We first find a Sylow l-subgroup of S_n.

Lemma 7.3. *Let σ_i^j be the permutation which permutes the ith set of l blocks of size l^{j-1}. Then*

$$\langle \{\sigma_i^j\}_{1 \leq j \leq \mu_l(n), 1 \leq i \leq \lfloor \frac{n}{l^j} \rfloor} \rangle \in \mathrm{Syl}_l(S_n).$$

Let $P_l(S_n)$ denote this particular Sylow l-subgroup of S_n.

Proof. For the proof, see the Appendix. □

Lemma 7.4. *For $P \in \mathrm{Syl}_l(GL_n(\mathbb{F}_q))$,*

$$P \cong (\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0}).$$

Proof. [1]

Let ϵ be a primitive l^s-th root of unity in $\mathbb{F}_{q^d}$, and let E be the image of ϵ in $GL_d(\mathbb{F}_q)$. There

[1] This construction follows [25].

are n_0 copies of $\langle E \rangle$ in $GL_n(\mathbb{F}_q)$, given by $\langle E_1 \rangle, \ldots, \langle E_{n_0} \rangle$ where

$$E_1 = \begin{pmatrix} E & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}, \ldots, E_{n_0} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & E & \\ & & & & \mathrm{Id}_{n-n_0 d} \end{pmatrix}$$

The symmetric group on n_0 letters acts on $\langle E_1, \ldots, E_{n_0} \rangle$ by permuting the E_i, and it can be embedded into $GL_n(\mathbb{F}_q)$. Let

$$\begin{aligned} P &= \langle E_1, \ldots, E_{n_0} \rangle \rtimes P_l(S_{n_0}) \\ &\cong (\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0}) \end{aligned}$$

Then

$$\begin{aligned} |P| &= |(\mathbb{Z}/l^s\mathbb{Z})^{n_0}| \cdot |P_l(S_n)| \\ &= |GL_n(\mathbb{F}_q)|_l \end{aligned}$$

Therefore, $P \in \mathrm{Syl}_l(GL_n(\mathbb{F}_q))$.

□

Lemma 7.5. *For $P \in Syl_l(GL_n(\mathbb{F}_q))$,*

$$Z(P) \cong (\mathbb{Z}/l^s\mathbb{Z})^{\sum_{k=0}^{\mu_l(n_0)} \lfloor \frac{n_0}{l^k} \rfloor - l \lfloor \frac{n_0}{l^{k+1}} \rfloor}.$$

Proof.

Let $P = (\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0})$. By Lemma 7.4, P is isomorphic to a Sylow l-subgroup of $GL_n(\mathbb{F}_q)$.

For $\mu_{\mathbf{l}}(\mathbf{n_0}) = \mathbf{0}$: $P \cong (\mathbb{Z}/l^s\mathbb{Z})^{n_0}$, which is abelian.

For $\mu_\mathbf{l}(\mathbf{n_0}) > \mathbf{0}$: Fix

$$(\mathbf{b}', \tau') \in (\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0}),$$

and let

$$(\mathbf{b}, \tau) \in (\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0}).$$

Then

$$(\mathbf{b}', \tau')(\mathbf{b}, \tau) = (\mathbf{b}' + \tau'(\mathbf{b}), \tau'\tau) \text{ and } (\mathbf{b}, \tau)(\mathbf{b}', \tau') = (\mathbf{b} + \tau(\mathbf{b}'), \tau\tau').$$

Thus $(\mathbf{b}', \tau')$ is in the center if and only if $\tau' \in Z(P_l(S_{n_0}))$ and

$$\mathbf{b}' + \tau'(\mathbf{b}) = \mathbf{b} + \tau(\mathbf{b}')$$

for all $\mathbf{b}, \tau$. Choosing $\tau = \text{Id}$, we see we must have $\mathbf{b}' + \tau'(\mathbf{b}) = \mathbf{b} + \mathbf{b}'$. Thus we must have $\tau'(\mathbf{b}) = \mathbf{b}$ for all $\mathbf{b}$. Therefore, $\tau' = \text{Id}$. We also need $\tau(\mathbf{b}') = \mathbf{b}'$ for all $\tau \in P_l(S_{n_0})$. Write $\mathbf{b}' = \prod_i E_i^{b_i}$.

Note that $\langle \sigma_1^1, \ldots, \sigma^1_{\lfloor \frac{n_0}{l} \rfloor} \rangle$ acts transitively on $\{E_1, \ldots, E_l\}, \{E_{l+1}, \ldots E_{2l}\}, \ldots \{E_{(l-1)\lfloor \frac{n_0}{l} \rfloor}, \ldots, E_{l\lfloor \frac{n_0}{l} \rfloor}\}$ and acts trivially on the remaining E_i, if there are more. Thus we can conclude that

$$b_1 = \cdots = b_l, \; b_{l+1} = \cdots = b_{2l}, \; \ldots, \; b_{l\lfloor \frac{n_0}{l} \rfloor - l} = \cdots = b_{l\lfloor \frac{n_0}{l} \rfloor},$$

and the remaining $n_0 - l\lfloor \frac{n_0}{l} \rfloor$ choices of b_i can be anything.

$\langle \sigma_1^2, \ldots, \sigma^2_{\lfloor \frac{n_0}{l^2} \rfloor} \rangle$ acts transitively on each group of l of the sets above through the $l\lfloor \frac{n_0}{l^2} \rfloor$-th set and trivially on the rest. Thus we can conclude that

$$b_1 = \cdots = b_{l^2}, \; b_{l^2+1} = \cdots = b_{2l^2}, \; \ldots, \; b_{l^2(\lfloor \frac{n_0}{l^2} \rfloor - 1)} = \cdots = b_{l^2\lfloor \frac{n_0}{l^2} \rfloor},$$

and of the remaining b_i, from the previous paragraph, we must have $\frac{l\lfloor \frac{n_0}{l} \rfloor - l^2\lfloor \frac{n_0}{l^2} \rfloor}{l} = \lfloor \frac{n_0}{l} \rfloor - l\lfloor \frac{n_0}{l^2} \rfloor$ sets of l b_i which are equal, while we still have the last $n_0 - l\lfloor \frac{n_0}{l} \rfloor$ allowed to be anything.

Continuing this logic until we get to $\langle \sigma_1^{\mu_l(n_0)}, \sigma^{\mu_l(n_0)}_{\lfloor \frac{n_0}{l^{\mu_l(n_0)}} \rfloor} \rangle$, where $\mu_l(n_0)$ is the highest power of

l such that $\lfloor \frac{n_0}{l^{\mu_l(n_0)}} \rfloor > 0$, and we can conclude that

$$b_1 = \cdots = b_{l^{\mu_l(n_0)}}, \;\; \cdots, \;\; b_{l^{\mu_l(n_0)}(\lfloor \frac{n_0}{l^{\mu_l(n_0)}} \rfloor - 1)} = \cdots = b_{l^{\mu_l(n_0)}\lfloor \frac{n_0}{l^{\mu_l(n_0)}} \rfloor},$$

and we have

$$\frac{l^{\mu_l(n_0)-1}\lfloor \frac{n_0}{l^{\mu_l(n_0)-1}} \rfloor - l^{\mu_l(n_0)}\lfloor \frac{n_0}{l^{\mu_l(n_0)}} \rfloor}{l^{\mu_l(n_0)-1}} = \lfloor \frac{n_0}{l^{\mu_l(n_0)-1}} \rfloor - l\lfloor \frac{n_0}{l^{\mu_l(n_0)}} \rfloor$$

sets of $l^{\mu_l(n_0)-1}$ b_i which are equal, and in general for $1 \leq k \leq \mu_l(n_0)$, we have

$$\lfloor \frac{n_0}{l^k} \rfloor - l\lfloor \frac{n_0}{l^{k+1}} \rfloor$$

sets of l^k b_i which are equal. So we are allowed to choose

$$\sum_{k=0}^{\mu_l(n_0)} \lfloor \frac{n_0}{l^k} \rfloor - l\lfloor \frac{n_0}{l^{k+1}} \rfloor$$

different entries. Thus

$$Z(P) = (\mathbb{Z}/l^s\mathbb{Z})^{\sum_{k=0}^{\mu_l(n_0)} \lfloor \frac{n_0}{l^k} \rfloor - l\lfloor \frac{n_0}{l^{k+1}} \rfloor}.$$

□

Definition 7.6. Let $s_{l,n_0} = \sum_{k=0}^{\mu_l(n_0)} \lfloor \frac{n_0}{l^k} \rfloor - l\lfloor \frac{n_0}{l^{k+1}} \rfloor$. In Lemma 7.5, we showed that in $(\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0})$, we can choose s_{l,n_0} components of $\mathbf{b}$ while making $(\mathbf{b}, \tau)$ to be in the center. Call the indices of these components i_ι. For $1 \leq \iota \leq s_{l,n_0} - 1$, we have that in the center the entries b_i for $i_\iota \leq i < i_{\iota+1}$ are equal. And we have that the entries b_i are equal for $i_{s_{l,n_0}} \leq i \leq n_0$. Let I_ι denote

$$I_\iota = \begin{cases} \{i : i_\iota \leq i < i_{\iota+1}\}, & \iota < s_{l,0n} \\ \{i : i_{s_{l,n_0}} \leq i \leq n\}, & \iota = s_{l,n} \end{cases}.$$

For each ι, note that $|I_\iota| = l^k$ for some k. Let k_ι be such that $|I_\iota| = l^{k_\iota}$.

Classifying the irreducible representations

We will use Wigner-Mackey Theory with $(\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0})$ to compute the minimum dimension of an irreducible faithful representation with non-trivial central character. So

$$\Delta = (\mathbb{Z}/l^s\mathbb{Z})^{n_0},\ L = P_l(S_{n_0}).$$

Recall that we are assuming that k contains a primitive l^s-th root of unity. Define $\psi : \mathbb{Z}/l^s\mathbb{Z} \to S^1$ by $\psi(k) = e^{\frac{2\pi i k}{l^s}}$. Then the characters of $(\mathbb{Z}/l^s\mathbb{Z})^{n_0}$ are given by $\psi_{\mathbf{b}}$ for $\mathbf{b} \in (\mathbb{Z}/l^s\mathbb{Z})^{n_0}$, where $\psi_{\mathbf{b}}(\mathbf{d}) = \psi(\mathbf{b} \cdot \mathbf{d})$.

Note. Since $\Delta \cong (\mathbb{Z}/l^s\mathbb{Z})^{n_0}$, we now need to assume that k contains a primitive l^s-th root of unity in order to apply Venkataram's extension of Wigner-Mackey Theory.

Recall

$$L_{\mathbf{b}} = \mathrm{stab}_L \psi_{\mathbf{b}} = \{\tau : \psi(\mathbf{b} \cdot (\tau(\mathbf{a}) - \mathbf{a})) = 1,\ \forall \mathbf{a} \in (\mathbb{Z}/l^s\mathbb{Z})^{n_0}\}.$$

Recall that the dimension of the irreducible representation $\theta_{\mathbf{b},1}$ will be minimized when $|L_{\mathbf{b}}|$ is maximized, and the dimension is given by $\frac{|L|}{|L_{\mathbf{b}}|}$.

Proposition 7.7. *Fix ι. Then*

$$\min_{b_i \neq 0 \text{ for some } i \in I_\iota} \dim(\theta_{\mathbf{b},1}) = l^{k_\iota}.$$

This minimum is achieved when $\mathbf{b} = (b_i)$ with $b_{i_\iota} = 1$ and all other entries 0.

Proof.

Let $\tau \in L_{\mathbf{b}}$. Note that $\mathbf{b} \cdot (\tau(\mathbf{a}) - \mathbf{a}) = \sum_i a_i(b_{\tau(i)} - b_i)$. For $i_0 \leq n$, let $\mathbf{a} = x e_{i_0}$. Then

$$\mathbf{b} \cdot (\tau(\mathbf{a}) - \mathbf{a}) = x(b_{\tau(i_0)} - b_{i_0}).$$

If $b_{\tau(i_0)} - b_{i_0} \neq 0$, then $x b_{\tau(i_0)} - x b_{i_0}$ will be non-zero for some value of $x \in \mathbb{Z}/l^s\mathbb{Z}$. But then $\psi(x b_{\tau(i_0)} - x b_{i_0})$ would not equal 1. This contradicts the assumption that $\tau \in L_{\mathbf{b}}$. Therefore, for all i, we must have $b_{\tau(i)} = b_i$. If this condition is satisfied, then $\mathbf{b} \cdot (\tau(\mathbf{a}) - \mathbf{a}) = 0$ for all

$\mathbf{a} \in (\mathbb{Z}/l^s\mathbb{Z})^{n_0}$. Thus

$$L_{\mathbf{b}} = \{\tau : b_{\tau(i)} = b_i, \ \forall i\}.$$

If $|I_\iota| = 1$, then all $\tau \in L$ act trivially on I_ι. Thus for $\mathbf{b} = (b_i)$ with $b_{i_\iota} = 1$ and all other entries 0, we will have $L_{\mathbf{b}} = L$, and thus $\dim(\theta_{\mathbf{b},1}) = 1$.

If $l \mid |I_\iota|$, then if we choose $\mathbf{b}$ with $b_i = b$ for $i \in I_\iota$ and all other entries 0, then for $\mathbf{d} = (d_i)$ with $d_i = xl^{s-1}$ for $i \in I_\iota$ and all other entries 0, we get that

$$\psi_{\mathbf{b}}(\mathbf{d}) = e^{\frac{2\pi i l b x l^{s-1}}{l^s}} = e^{2\pi i b x} = 1.$$

Thus in terms of forming a basis for $\Omega_1(Z(\widehat{(\mathbb{Z}/l^s\mathbb{Z})^{n_0}} \rtimes P_l(S_{n_0})))$, this is no different than having $b_i = b_j = 0$ for $i \in I_\iota$. So we must have $b_{i_0} \neq b_{j_0}$ for some $i_0, j_0 \in I_\iota$ or we can assume that $b_i = b_j = 0$ for all $i, j \in I_\iota$. Hence for

$$\tau = \prod_{1 \leq \mu \leq \mu_l(n_0), 1 \leq \nu \leq \lfloor \frac{n_0}{l^\mu} \rfloor} (\sigma_\nu^\mu)^{a_{\mu,\nu}} \in L_{\mathbf{b}},$$

we must have $b_i = b_j = 0$ for all $i, j \in I_\iota$ or $b_{i_0} \neq b_{j_0}$ for some $i_0, j_0 \in I_\iota$ and $a_{\mu,\nu} = 0$ for all σ_ν^μ which act non-trivially on I_ι. Recall $|I_\iota| = l^{k_\iota}$. For $i \in I_\iota$, for each $\kappa \leq k_\iota$, there will be one σ_ν^κ which acts on b_i, each of order l. Thus $|L_{\mathbf{b}}| \leq \frac{|L|}{l^{k_\iota}}$. So

$$\dim(\theta_{\mathbf{b},\lambda}) \geq l^{k_\iota}.$$

For $\mathbf{b} = (b_i)$ with $b_{i_\iota} = 1$ and all other entries 0, this minimum will be achieved.

□

Proof

Proof. Let $P = (\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0})$. By Lemma 1.5, faithful representations of P of minimal dimension will decompose as a direct sum of exactly $r = \text{rank}(Z(P))$ irreducible representations. Since the center has rank $s_{l,n_0} = \sum_{k=0}^{\mu_l(n_0)} \lfloor \frac{n_0}{l^k} \rfloor - l \lfloor \frac{n_0}{l^{k+1}} \rfloor$, a faithful representation ρ of minimal dimension decomposes as a direct sum

$$\rho = \rho_1 \oplus \ldots \oplus \rho_{s_{l,n_0}}$$

of exactly s_{l,n_0} irreducibles, and if χ_i are the central characters of ρ_i, then $\{\chi_i|_{\Omega_1(Z(P))}\}$ form a basis for $\Omega_1\widehat{(Z(P))} \cong \widehat{(\mathbb{Z}/l\mathbb{Z})}^{s_{l,n_0}}$.

Since we must have $\chi_i|_{\Omega_1(Z(P))}$ generating $\Omega_1\widehat{(Z(P))}$, for each $1 \leq \iota \leq s_{l,n_0}$, we will need at least one of the χ_i to have $b_i \neq 0$ for some $i \in I_\iota$, and so by Proposition 7.7, the minimum dimension of that ρ_i in the decomposition into irreducibles will be

$$\min_{b_i \neq 0 \text{ for some } i \in I_\iota} \dim(\theta_{\mathbf{b},\lambda}) = l^{k_\iota},$$

where $|I_\iota| = l^{k_\iota}$.

Moreover, by choosing $\mathbf{b}^\iota = (b_i)$, with $b_{i_\iota} = 1$ and all other entries 0, λ trivial, we get that $\rho = \oplus_{\iota=1}^{s_{l,n_0}} \theta_{\mathbf{b}^\iota,1}$ is a faithful representation of dimension $\sum_{\iota=1}^{s_{l,n_0}} l^{k_\iota}$.

In the sum $s_{l,n_0} = \sum_{k=0}^{\mu_l(n_0)} \lfloor \frac{n_0}{l^k} \rfloor - l \lfloor \frac{n_0}{l^{k+1}} \rfloor$ calculated in the proof of Lemma 7.5, for each k, we get $\lfloor \frac{n_0}{l^k} \rfloor - l \lfloor \frac{n_0}{l^{k+1}} \rfloor$ different values of i_ι with $|I_\iota| = l^k$, i.e. $k_\iota = k$. Thus

$$\mathrm{ed}_k(GL_n(\mathbb{F}_q), l) = \sum_{\iota=1}^{s_{l,n_0}} l^{k_\iota} = \sum_{k=0}^{\mu_l(n_0)} \left(\lfloor \frac{n_0}{l^k} \rfloor - l \lfloor \frac{n_0}{l^{k+1}} \rfloor \right) l^k$$

□

8 The Special Linear Groups at Non-defining Primes

Theorem 8.1. *Let p be a prime, $q = p^r$, and l a prime with $l \neq p$. Let k be a field with char $k \neq l$. Let d be the smallest positive integer such that $l \mid q^d - 1$. Let $s = \nu_l(q^d - 1)$. Assume that k contains a primitive l^s-th root of unity. Let $\mu_l(n)'$ denote the smallest k such that $\lfloor \frac{n}{l^k} \rfloor - l \lfloor \frac{n}{l^{k+1}} \rfloor > 0$. If $l = 2$, assume that $q \equiv 1 \pmod 4$. Then for all l,*

$$\mathrm{ed}_k(SL_n(\mathbb{F}_q), l) = \begin{cases} \mathrm{ed}_k(GL_n(\mathbb{F}_q), l), & l \nmid q-1 \\ \mathrm{ed}_k(GL_n(\mathbb{F}_q), l) - l^{\mu_l(n)'}, & l \mid q-1 \end{cases}$$

Note: In the notation of the previous section, when $l \mid q-1$, we have $d = 1$ and $n_0 = n$.

If $l \nmid q-1$, then the Sylow l-subgroups of $SL_n(\mathbb{F}_q)$ are isomorphic to the Sylow l-subgroups of $\mathrm{GL}_n(\mathbb{F}_q)$. So we need only prove the case when $l \mid q-1$. Thus in this section, we will assume $l \mid q-1$.

The p-Sylow and its center

By ([8], Proposition 1.1),

$$|SL_n(\mathbb{F}_q)| = \frac{|GL_n(\mathbb{F}_q)|}{q-1}.$$

So

$$|SL_n(\mathbb{F}_q)|_l = \frac{|GL_n(\mathbb{F}_q)|_l}{l^{\nu_l(q-1)}} = l^{s(n-1)} \cdot |S_n|_l$$

Lemma 8.2. *For* $P \in \mathrm{Syl}_l(SL_n(\mathbb{F}_q))$,

$$P \cong (\mathbb{Z}/l^s\mathbb{Z})^{n-1} \rtimes P_l(S_n).$$

Proof.

Let ϵ be a primitive l^s-th root of unity in $\mathbb{F}_q$, and let

$$E_1 = \begin{pmatrix} \epsilon & & & & \\ & \frac{1}{\epsilon} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \ldots, E_{n-1} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \epsilon & \\ & & & & 1/\epsilon \end{pmatrix}, E_n = \begin{pmatrix} \frac{1}{\epsilon} & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \epsilon \end{pmatrix}$$

Note that in $SL_n(\mathbb{F}_q)$, these all generate distinct cyclic subgroups except E_n, and $E_n = \prod_{i=1}^{n-1} E_i^{l^s-1}$. The symmetric group on n letters acts on $\langle E_1, \ldots, E_n\rangle$ by permuting the E_i. So it acts on

$$\langle E_1, \ldots, E_{n-1}\rangle = \langle E_1, \ldots E_n\rangle/(E_n = \prod_{i=1}^{n-1} E_i^{l^s-1}).$$

And $P_l(S_n)$ can be embedded into $SL_n(\mathbb{F}_q)$. Let

$$\begin{aligned} P &= \langle E_1, \ldots, E_{n-1}\rangle \rtimes P_l(S_n) \\ &\cong (\mathbb{Z}/l^s\mathbb{Z})^{n-1} \rtimes P_l(S_n) \end{aligned}$$

Then $P \in \mathrm{Syl}_l(SL_n(\mathbb{F}_q))$.

□

Lemma 8.3. *For $P \in \mathrm{Syl}_l(SL_n(\mathbb{F}_q))$,*

$$Z(P) \cong (\mathbb{Z}/l^s\mathbb{Z})^{(\sum_{k=0}^{\mu_l(n)} \lfloor \frac{n}{l^k} \rfloor - l \lfloor \frac{n}{l^{k+1}} \rfloor) - 1}.$$

Proof.

Let $P = (\mathbb{Z}/l^s\mathbb{Z})^{n-1} \rtimes P_l(S_{n_0})$. By Lemma 7.4, P is isomorphic to a Sylow l-subgroup of $SL_n(\mathbb{F}_q)$.

For $\mu_\mathbf{l}(\mathbf{n}) = \mathbf{0}$: $P \cong (\mathbb{Z}/l^s\mathbb{Z})^{n-1}$, which is abelian.

For $\mu_\mathbf{l}(\mathbf{n}) > \mathbf{0}$: Just as for $GL_n(\mathbb{F}_q)$, $(\mathbf{b}', \tau')$ is in the center if and only if $\tau' = \mathrm{Id}$ and $\tau(\mathbf{b}') = \mathbf{b}'$ for all $\tau \in P_l(S_n)$. Write $\mathbf{b}' = \prod_{i=1}^{n-1} E_i^{b_i}$. Recall that $E_n = \prod_{i=1}^{n-1} E_i^{l^s-1}$,. If E_i can be sent to E_n via some $\tau \in P_l(S_n)$, then we will have $\tau(\mathbf{b}') = \prod_{i=1}^{n-1} E_i^{l^s} \neq \mathbf{b}'$. Thus for i such that E_i can be sent to E_n via some $\tau \in P_l(S_n)$ (that is for $i \in I_{s_{l,n}}$, we must have $b_i = 0$.

So not only do we have to have the b_i equal for E_i that can be mapped to E_n, we must have those $b_i = 0$ (if $l \nmid n$, then this is just $b_n = 0$). Thus we have one less different entry that we can choose than we could choose in the case of $GL_n(\mathbb{F}_q)$). Thus in either case,

$$Z(P) \cong (\mathbb{Z}/l^s\mathbb{Z})^{(\sum_{k=0}^{\mu_l(n)} \lfloor \frac{n}{l^k} \rfloor - l \lfloor \frac{n}{l^{k+1}} \rfloor) - 1}.$$

□

Classifying the irreducible representations

We will use Wigner-Mackey Theory with $(\mathbb{Z}/l^s\mathbb{Z})^n \rtimes P_l(S_n)$ to compute the minimum dimension of an irreducible faithful representation with non-trivial central character. So

$$\Delta = (\mathbb{Z}/l^s\mathbb{Z})^{n-1},\ L = P_l(S_n).$$

Recall that we are assuming that k contains a primitive l^s-th root of unity. Define $\psi : \mathbb{Z}/l^s\mathbb{Z} \to S^1$ by $\psi(k) = e^{\frac{2\pi ik}{l^s}}$. Then the characters of $(\mathbb{Z}/l^s\mathbb{Z})^{n-1}$ are given by $\psi_{\mathbf{b}}$ for $\mathbf{b} \in (\mathbb{Z}/l^s\mathbb{Z})^{n-1}$, where $\psi_{\mathbf{b}}(\mathbf{d}) = \psi(\mathbf{b} \cdot \mathbf{d})$. Recall

$$L_{\mathbf{b}} = \mathrm{stab}_L \psi_{\mathbf{b}} = \{\tau : \psi(\mathbf{b} \cdot (\tau(\mathbf{a}) - \mathbf{a})) = 1,\ \forall \mathbf{a} \in (\mathbb{Z}/l^s\mathbb{Z})^{n-1}\}.$$

Recall that the dimension of the irreducible representation $\theta_{\mathbf{b},1}$ will be minimized when $|L_{\mathbf{b}}|$ is maximized, and the dimension is given by $\frac{|L|}{|L_{\mathbf{b}}|}$.

Proposition 8.4. *Fix $\iota \neq s_{l,n}$. For $\mathbf{b} = (b_i)$*

$$\min_{b_i \neq 0 \textit{ for some } i \in I_\iota} \dim(\theta_{\mathbf{b},\lambda}) = l^{k_\iota}$$

This minimum is achieved when $\mathbf{b} = (b_i)$ with $b_{i_\iota} = 1$ and all other entries 0, λ trivial.

Proof.

Note that since $i \in I_\iota$ and $\iota \neq s_{l,n}$, e_i cannot be mapped to e_n, thus we will have $\tau(e_i) = e_j$ for some $j < n$, and we can write $\tau(e_i) = e_{\tau(i)}$.

By the exact same reasoning as for $GL_n(\mathbb{F}_q)$,

$$\dim(\theta_{\mathbf{b},\lambda}) \geq l^{k_\iota},$$

and this minimum will be achieved for $\mathbf{b} = (b_i)$ with $b_{i_\iota} = 1$ and all other entries 0.

□

Proof

Let $P = (\mathbb{Z}/l^s\mathbb{Z})^{n-1} \rtimes P_l(S_n)$. By Lemma 1.5, faithful representations of P of minimal dimension will decompose as a direct sum of exactly $r = \mathrm{rank}(Z(P))$ irreducible representations. Since the center has rank $s_{l,n_0} - 1$, a faithful representation ρ of minimal dimension decomposes as a direct sum

$$\rho = \rho_1 \oplus \cdots \oplus \rho_{s_{l,n_0}-1}$$

of exactly $s_{l,n_0} - 1$ irreducibles, and if χ_i are the central characters of ρ_i, then $\{\chi_i|_{\Omega_1(Z(P))}\}$ form a basis for $\widehat{\Omega_1(Z(P))} \cong \widehat{(\mathbb{Z}/l\mathbb{Z})^{s_{l,n_0}-1}}$.

Since we must have $\chi_i|_{\Omega_1(Z(P))}$ generating $\widehat{\Omega_1(Z(P))}$, for each $1 \leq \iota < s_{l,n_0} - 1$, we will need at least one of the χ_i to have $b_i \neq 0$ for some $i \in I_\iota$, and so by Proposition 8.4, the minimum dimension of that ρ_i in the decomposition into irreducibles will be

$$\min_{b_i \neq 0 \text{ for some } i \in I_\iota} \dim(\theta_{\mathbf{b},\lambda}) = l^{k_\iota},$$

where $|I_\iota| = l^{k_\iota}$.

Moreover, by choosing $\mathbf{b}^\iota = (b_i)$, with $b_{i_\iota} = 1$ and all other entries 0, we get that $\rho = \oplus_{\iota=1}^{s_{l,n}-1} \theta_{\mathbf{b}^\iota,1}$ is a faithful representation of dimension $\sum_{\iota=1}^{s_{l,n}-1} l^{k_\iota}$.

Let $\mu_l(n)'$ be the smallest value of k such that $\lfloor \frac{n}{l^k} \rfloor - l\lfloor \frac{n}{l^{k+1}} \rfloor > 0$. In the sum $\sum_{k=0}^{\mu_l(n_0)} \lfloor \frac{n_0}{l^k} \rfloor - l\lfloor \frac{n_0}{l^{k+1}} \rfloor - 1$ calculated in the proof of Lemma 8.3, for each $k > \mu_l(n)'$, we get $\lfloor \frac{n_0}{l^k} \rfloor - l\lfloor \frac{n_0}{l^{k+1}} \rfloor$ different values of i_ι with $|I_\iota| = l^k$, i.e. $k_\iota = k$. For $k = \mu_l(n)'$, we get $\lfloor \frac{n}{l^{\mu_l(n)'}} \rfloor - l\lfloor \frac{n}{l^{\mu_l(n)'+1}} \rfloor - 1$ different values of i_ι with $k_\iota = \mu_l(n)'$. Thus

$$\begin{aligned}
\mathrm{ed}_k(SL_n(\mathbb{F}_q), l) &= \sum_{\iota=1}^{s_{l,n}-1} l^{k_\iota} \\
&= \left(\sum_{k=\mu_l(n)'+1}^{\mu_l(n)} \left(\lfloor \frac{n}{l^k} \rfloor - l\lfloor \frac{n}{l^{k+1}} \rfloor \right) l^{k_\iota} \right) + \left(\lfloor \frac{n}{l^{\mu_l(n)'}} \rfloor - l\lfloor \frac{n}{l^{\mu_l(n)'+1}} \rfloor - 1 \right) l^{\mu_l(n)'} \\
&= \left(\sum_{k=\mu_l(n)'}^{\mu_l(n)} \left(\lfloor \frac{n}{l^k} \rfloor - l\lfloor \frac{n}{l^{k+1}} \rfloor \right) l^k \right) - l^{\mu_l(n)'}
\end{aligned}$$

$$= \left(\sum_{k=0}^{\mu_l(n)} \left(\lfloor \frac{n}{l^k} \rfloor - l \lfloor \frac{n}{l^{k+1}} \rfloor \right) l^k \right) - l^{\mu_l(n)'}$$

$$= \mathrm{ed}_k(GL_n(\mathbb{F}_q), l) - l^{\mu_l(n)'}$$

9 The Projective Special Linear Groups at Non-defining Primes

Theorem 9.1. *Let p be a prime, $q = p^r$, and l a prime with $l \neq p$. Let k be a field with char $k \neq l$. Let d be the smallest positive integer such that $l \mid q^d - 1$. Let $s = \nu_l(q^d - 1)$. Assume that k contains a primitive l^s-th root of unity. If $l = 2$, assume that $q \equiv 1 \pmod 4$. Then for all l,*

$$\mathrm{ed}_k(PSL_n(\mathbb{F}_q), l) = \mathrm{ed}_k(SL_n(\mathbb{F}_q), l))$$

If $l \nmid n$, then the Sylow l-subgroups of $PSL_n(\mathbb{F}_q)$ are isomorphic to the Sylow l-subgroups of $SL_n(\mathbb{F}_q)$. So we need only prove the theorem when $l \mid n$. Thus in this section, we will assume $l \mid n$. Let $t = \nu_l(n)$.

The p-Sylow and its center

By ([8], Proposition 1.1),

$$|PSL_n(\mathbb{F}_q)| = \frac{|SL_n(\mathbb{F}_q)|}{(n, q-1)}.$$

So

$$|PSL_n(\mathbb{F}_q)|_l = \frac{|SL_n(\mathbb{F}_q)|_l)}{\nu_l(gcd(n, q-1))} = l^{s(n-1)-\min(s,t)} \cdot |S_n|_l,$$

where $s = \nu_l(q-1)$ and $t = \nu_l(n)$.

Lemma 9.2. *For $P \in \mathrm{Syl}_l(PSL_n(\mathbb{F}_q))$,*

$$P \cong \begin{cases} (\mathbb{Z}/l^s\mathbb{Z})^{n-2} \rtimes P_l(S_n), & s \leq t \\ ((\mathbb{Z}/l^s\mathbb{Z})^{n-2} \times \mathbb{Z}/l^{s-t}\mathbb{Z}) \rtimes P_l(S_n), & s > t \end{cases}$$

Proof.

Let ϵ be a primitive l^s-th root of unity in $\mathbb{F}_q$. Let

$$E_1 = \begin{pmatrix} \epsilon & & & & \\ & \frac{1}{\epsilon} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \ldots, E_{n-1} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \epsilon & \\ & & & & 1/\epsilon \end{pmatrix}, E_n = \begin{pmatrix} \frac{1}{\epsilon} & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \epsilon \end{pmatrix}$$

Note that in $PSL_n(\mathbb{F}_q)$, these all generate distinct cyclic subgroups except E_n and E_{n-1}. Just as in $SL_n(\mathbb{F}_q)$, $E_n = \prod_{i=1}^{n-1} E_i^{l^s-1}$.

Case 1: $\mathbf{s \leq t}$

If $s \leq t$, then $\min(s,t) = s$, so

$$|PSL_n(\mathbb{F}_q)|_l = l^{s(n-2)} \cdot |S_n|_l.$$

Note that $Z(SL_n(\mathbb{F}_q)) = \{a\mathrm{Id} : a \in F_q^\times, a^n = 1\}$. Since $l^s \bigm| n$, $\epsilon^n = 1$. Thus $\epsilon\mathrm{Id} \in Z(SL_n(\mathbb{F}_q))$. Note $E_{n-1} = \frac{1}{\epsilon}(E_1)E_2^2 \cdots E_{n-2}^{n-2}$. Thus

$$\langle E_1, \ldots, E_{n-1}\rangle = \langle E_1, \ldots, E_{n-2}\rangle \cong (\mathbb{Z}/l\mathbb{Z})^{n-2}.$$

As before, S_n acts on $\langle E_1, \ldots, E_n\rangle$ by permuting the E_i. So it acts on

$$\langle E_1, \ldots, E_{n-2}\rangle = \langle E_1, \ldots E_n\rangle / (E_n = \prod_{i=1}^{n-1} E_i^{l^s-1}, E_{n-1} = \prod_{i=1}^{n-2} E_i^i).$$

$P_l(S_n)$ can be embedded into $PSL_n(\mathbb{F}_q)$. Let

$$\begin{aligned} P &= \langle E_1, \ldots, E_{n-2}\rangle \rtimes P_l(S_n) \\ &\cong (\mathbb{Z}/l^s\mathbb{Z})^{n-2} \rtimes P_l(S_n). \end{aligned}$$

Then $P \in \mathrm{Syl}_l(PSL_n(\mathbb{F}_q))$.

Case 2: $\mathbf{s > t}$

If $s > t$, then $\min(s,t) = t$, so

$$|PSL_n(\mathbb{F}_q)|_l = l^{s(n-1)-t} \cdot |S_n|_l.$$

Note that $Z(SL_n(\mathbb{F}_q)) = \{a\mathrm{Id} : a \in F_q^\times, a^n = 1\}$. So since $(\epsilon^{l^{s-t}})^n = 1$, $\epsilon^{l^{s-t}}\mathrm{Id} \in Z(SL_n(\mathbb{F}_q))$. Note $(E_{n-1})^{l^{s-t}} = \frac{1}{\epsilon^{l^{s-t}}} \prod_{i=1}^{n-2} E_i^{il^{s-t}}$. So in $PSL_n(\mathbb{F}_q)$, $E_{n-1}^{l^{s-t}} = \prod_{i=1}^{n-2} E_i^{il^{s-t}}$. As before, S_n acts on

$$\langle E_1, \ldots, E_{n-2}\rangle = \langle E_1, \ldots E_n\rangle / (E_n = \prod_{i=1}^{n-1} E_i^{l^s-1}, E_{n-1}^{l^{s-t}} = \prod_{i=1}^{n-2} E_i^{il^{s-t}}).$$

$P_l(S_n)$ can be embedded into $PSL_n(\mathbb{F}_q)$. Let

$$\begin{aligned} P &= \langle E_1, \ldots, E_{n-1}\rangle \rtimes P_l(S_n) \\ &\cong ((\mathbb{Z}/l^s\mathbb{Z})^{n-2} \times \mathbb{Z}/l^{s-t}\mathbb{Z}) \rtimes P_l(S_n). \end{aligned}$$

Then $P \in \mathrm{Syl}_l(PSL_n(\mathbb{F}_q))$. □

Lemma 9.3. *For $P \in \mathrm{Syl}_l(PSL_n(\mathbb{F}_q))$,*

$$Z(P) \cong (\mathbb{Z}/l^s\mathbb{Z})^{(\sum_{k=0}^{\mu_l(n)} \lfloor \frac{n}{l^k} \rfloor - l \lfloor \frac{n}{l^{k+1}} \rfloor)-1}.$$

Proof.

Note that since $l \mid n$, $\mu_\mathbf{l}(\mathbf{n}) > \mathbf{0}$. Just as for $GL_n(\mathbb{F}_q)$ and $SL_n(\mathbb{F}_q)$, $(\mathbf{b}', \tau')$ is in the center if and only if $\tau' = \mathrm{Id}$ and $\tau(\mathbf{b}') = \mathbf{b}'$ for all $\tau \in P_l(S_n)$. Write $\mathbf{b}' = \prod_{i=1}^{n-1} E_i^{b_i}$. Just as for $SL_n(\mathbb{F}_q)$, we must have $b_i = 0$ for i such that E_i can be sent to E_n via some $\tau \in P_l(S_n)$. Similarly, we will need $b_i = 0$ for i such that E_i can be sent to E_{n-1}. But since $l \mid n$, the E_i which get mapped to E_{n-1} are the same as those which get mapped to E_n. So we get no added conditions to those which we had for $SL_n(\mathbb{F}_q)$. □

Classifying the irreducible representations

We will use Wigner-Mackey Thoery with

$$\begin{cases} (\mathbb{Z}/l^s\mathbb{Z})^{n-2} \rtimes P_l(S_n), & s \le t \\ ((\mathbb{Z}/l^s\mathbb{Z})^{n-2} \times \mathbb{Z}/l^{s-t}\mathbb{Z}) \rtimes P_l(S_n), & s > t \end{cases}$$

to compute the minimum dimension of a fiathiful representation with non-trivial central character.

Recall that we are assuming that k contains a primitive l^s-th root of unity. Define $\psi : \mathbb{Z}/l^s\mathbb{Z} \to S^1$ by $\psi(k) = e^{\frac{2\pi i k}{l^s}}$.

Recall that for $1 \le \iota \le s_{l,n_0} - 1$, i_ι correspond to the components of $\mathbf{b}$ that are allowed to be chosen arbitrarily while making $(\mathbf{b}, \tau)$ to be in the center, where $s_{l,n_0} = \sum_{k=0}^{\mu_l(n_0)} \lfloor \frac{n_0}{l^k} \rfloor - l \lfloor \frac{n_0}{l^{k+1}} \rfloor$. I_ι is

$$I_\iota = \begin{cases} \{i : i_\iota \le i < i_{\iota+1}\}, & \iota < s_{l,n_0} \\ \{i : i_{s_{l,n_0}} \le i \le n\}, & \iota = s_0 \end{cases}.$$

k_ι is such that $|I_\iota| = l^{k_\iota}$.

For $s \le t$, the characters of $(\mathbb{Z}/l^s\mathbb{Z})^{n-2}$ are given by $\psi_{\mathbf{b}}$ for $\mathbf{b} \in (\mathbb{Z}/l^s\mathbb{Z})^{n-2}$, where $\psi_{\mathbf{b}}(\mathbf{d}) = \psi(\mathbf{b} \cdot \mathbf{d})$. Recall

$$L_{\mathbf{b}} = \mathrm{stab}_L \psi_{\mathbf{b}} = \{\tau : \psi(\mathbf{b} \cdot (\tau(\mathbf{a}) - \mathbf{a})) = 1,\ \forall \mathbf{a} \in (\mathbb{Z}/l^s\mathbb{Z})^{n-2}\}.$$

For $s > t$, the characters of $(\mathbb{Z}/l^s\mathbb{Z})^{n-2} \times \mathbb{Z}/l^{s-t}\mathbb{Z}$ are given by $\psi_{\mathbf{b},x}$ for $\mathbf{b} \in (\mathbb{Z}/l^s\mathbb{Z})^{n-2}, x \in Z/l^{s-t}\mathbb{Z}$, where

$$\psi_{\mathbf{b},x}(\mathbf{d}, y) = \psi(\mathbf{b} \cdot \mathbf{d} + l^t(xy)).$$

Recall

$$\begin{aligned} L_{\mathbf{b},x} &= \mathrm{stab}_L \psi_{\mathbf{b},x} \\ &= \{\tau : \psi(\mathbf{b} \cdot (\tau(\mathbf{a}, y)|_{(\mathbb{Z}/l^s\mathbb{Z})^{n-2}} - \mathbf{a}) + l^t x(\tau(\mathbf{a}, y)|_{\mathbb{Z}/l^{s-t}\mathbb{Z}} - y)),\ \forall (\mathbf{a}, y) \in (\mathbb{Z}/l^s\mathbb{Z})^{n-2} \times (\mathbb{Z}/l^{s-t}\mathbb{Z})\}, \end{aligned}$$

Note that for $(\mathbf{b}, x)$ in the center, we will have $x = 0$, thus since we only care about non-trivial central characters, we can assume that $x = 0$, and so we have the exact same situation as that for $s \leq t$.

Proposition 9.4. *Fix $\iota \neq s_{l,n}$. For $\mathbf{b} = (b_i)$*

$$\min_{b_i \neq 0 \text{ for some } i \in I_\iota} \dim(\theta_{\mathbf{b},\lambda}) = l^{k_\iota}$$

This minimum is achieved when $\mathbf{b} = (b_i)$ with $b_{i_\iota} = 1$ and all other entries 0, λ trivial.

Proof.

Note that since $i \in I_\iota$ and $\iota \neq s_{l,n}$, e_i cannot be mapped to e_n. And since $l \mid n$, we also have $n-1 \in I_{s_{l,n}}$; thus e_i cannot be mapped to e_{n-1} either. Hence we will have $\tau(e_i) = e_j$ for some $j < n-1$, and we can write $\tau(e_i) = e_{\tau(i)}$.

By the exact same reasoning as for $GL_n(\mathbb{F}_q)$,

$$\dim(\theta_{\mathbf{b},\lambda}) \geq l^{k_\iota},$$

and this minimum will be achieved for $\mathbf{b} = (b_i)$ with $b_{i_\iota} = 1$ and all other entries 0.

□

Proof

Let

$$P = \begin{cases} (\mathbb{Z}/l^s\mathbb{Z})^{n-2} \rtimes P_l(S_n), & s \leq t \\ ((\mathbb{Z}/l^s\mathbb{Z})^{n-2} \times \mathbb{Z}/l^{s-t}\mathbb{Z}) \rtimes P_l(S_n), & s > t \end{cases}.$$

By Lemma 1.5, faithful representations of P of minimal dimension will decompose as a direct sum of exactly $r = \text{rank}(Z(P))$ irreducible representations. Since the center has rank $s_{l,n_0} - 1$, a faithful representation ρ of minimal dimension decomposes as a direct sum

$$\rho = \rho_1 \oplus \cdots \oplus \rho_{s_{l,n_0}-1}$$

of exactly $s_{l,n_0}-1$ irreducibles, and if χ_i are the central characters of ρ_i, then $\{\chi_i|_{\Omega_1(Z(P))}\}$ form a basis for $\Omega_1\widehat{(Z(P))} \cong \widehat{(\mathbb{Z}/l\mathbb{Z})^{s_{l,n_0}-1}}$.

Since we must have $\chi_i|_{\Omega_1(Z(P))}$ generating $\Omega_1\widehat{(Z(P))}$, for each $1 \le \iota < s_{l,n}-1$, we will need at least one of the χ_i to have $b_i \ne 0$ for some $i \in I_\iota$, and so by Proposition 9.4, the minimum dimension of that ρ_i in the decomposition into irreducibles will be

$$\min_{b_i \ne 0 \text{ for some } i \in I_\iota} \dim(\theta_{\mathbf{b},1}) = l^{k_\iota},$$

where $|I_\iota| = l^{k_\iota}$.

Moreover, by choosing $\mathbf{b}^\iota = (b_i)$, with $b_{i_\iota} = 1$ and all other entries 0, we get that $\rho = \oplus_{\iota=1}^{s_0} \theta_{\mathbf{b}^\iota,\mathrm{triv}}$ is a faithful representation of dimension

$$\sum_{\iota=1}^{s_{l,n}-1} l^{k_\iota}.$$

Thus

$$\mathrm{ed}_k(PSL_n(\mathbb{F}_q), l) = \sum_{\iota=1}^{s_{l,n}-1} l^{k_\iota} = \mathrm{ed}_k(SL_n(\mathbb{F}_q), l)$$

10 Quotients of $SL_n(\mathbb{F}_q)$ by cyclic subgroups of the center at Non-defining Primes

Note the for $n'|n$, we obtain a subgroup of $SL_n(\mathbb{F}_q)$ containing $PSL_n(\mathbb{F}_q)$ of order $\frac{|SL_n(\mathbb{F}_q)|}{(n',q-1)}$ by taking the quotient of $SL_n(\mathbb{F}_q)$ by the cyclic subgroup of order n' given by $\{aI : a \in \mathbb{F}_q^\times, a^{n'} = 1\}$. The order of the p-Sylow subgroup will be given by

$$l^{s(n-1)-\min(s,t')+\lfloor \frac{n}{l} \rfloor + \lfloor \frac{n}{l^2} + \ldots + \lfloor \frac{n}{l^t} \rfloor},$$

for $s = \nu_l(q-1), t = \nu_l(n)$.

Theorem 10.1. *Let $n'|n$, and let $s = \nu_l(q-1)$. Assume that k contains an l^s-th root of unity.*

If $l = 2$, assume that $q \equiv 1 \pmod 4$. Then for all l,

$$\mathrm{ed}_k(SL_n(\mathbb{F}_q)/\{aI : a \in \mathbb{F}_q^\times, a^{n'} = 1\}, l) = \mathrm{ed}_k(PSL_n(\mathbb{F}_q), l).$$

Proof. Let $s = \nu_l(q-1), t = \nu_l(n), t' = \nu_l(n')$. For $l \nmid n$ or $s \leq t'$, we will get that the l-Sylow is the same as that for $PSL_n(\mathbb{F}_q)$.

So let us consider the case $l \mid n, s > t'$. All the arguments that we used for $PSL_n(\mathbb{F}_q)$ apply directly here as well. By identical arguments to those for $PSL_n(\mathbb{F}_q)$, we can show that for $E_1, \ldots E_n$ defined as before, the p-Sylow is given by

$$\langle E_1, \ldots, E_{n-1}\rangle \rtimes P_l(S_n) \cong ((\mathbb{Z}/l^s\mathbb{Z})^{n-2} \times \mathbb{Z}/l^{s-t'}\mathbb{Z}) \rtimes P_l(S_n).$$

The fact that we have $\mathbb{Z}/l^{s-t'}\mathbb{Z}$ instead of $\mathbb{Z}/l^{s-t}\mathbb{Z}$ does not affect the argements used before. By the exact same arguments, we obtain the same essential l-dimension.

□

11 The Symplectic Groups at Non-defining Primes

Theorem 11.1. *Let p be a prime, $q = p^r$, and l a prime with $l \neq 2, p$. Let k be a field with char $k \neq l$. Let d be the smallest positive integer such that $l \mid q^d - 1$. Then*

$$\mathrm{ed}_k(PSp(2n,q), l) = \mathrm{ed}_k(Sp(2n,q), l) = \begin{cases} \mathrm{ed}_k(GL_{2n}(\mathbb{F}_q), l), & d \text{ even} \\ \mathrm{ed}_k(GL_n(\mathbb{F}_q), l), & d \text{ odd} \end{cases}$$

Proof. By Grove ([8], Theorem 3.12),

$$|PSp(2n,q)| = \frac{|Sp(2n,q)|}{(2, q-1)}.$$

So since $l \neq 2$, $|l, PSp(2n,q)|_l = |Sp(2n,q)|_l$. Hence since $PSp(2n,q)$ is a quotient of $Sp(2n,q)$, we can conclude that their Sylow l-subgroups are isomorphic. Let d be the smallest positive integer such that $l \mid q^d - 1$ and let $s = \nu_l(q^d - 1)$.

If **d is even**: Then by Stather ([25]), $|Sp(2n,q)|_l = |GL_{2n}(\mathbb{F}_q)|_l$. Hence since $Sp(2n,q)$ is a subgroup of $GL_{2n}(\mathbb{F}_q)$, we can conclude that their Sylow l-subgroups are isomorphic.

If **d is odd**: Then by Stather ([25]), letting $n_0 = \lfloor \frac{n}{d} \rfloor$, we have

$$|Sp(2n,q)|_l = |GL_n(\mathbb{F}_q)|_l = l^{sn_0} \cdot |S_{n_0}|_l$$

Let ϵ be primitive l^s-th root in $\mathbb{F}_{q^d}$, and let E be the image of ϵ in $GL_d(\mathbb{F}_q)$. Let

$$E_1 = \begin{pmatrix} E & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & (E^{-1})^T & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix},$$

$$\vdots$$

$$E_{n_0} = \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & E & & & & & & & \\ & & & & \mathrm{Id}_{n-n_0 d} & & & & & & \\ & & & & & 1 & & & & & \\ & & & & & & \ddots & & & & \\ & & & & & & & 1 & & & \\ & & & & & & & & (E^{-1})^T & & \\ & & & & & & & & & \mathrm{Id}_{n-n_0 d} \end{pmatrix}$$

Then for all i, $E_i \in Sp(2n, p^r)$. Note we can embed $P_l(S_{n_0})$ into $Sp(2n, q)$. Let

$$P = \langle E_1, \ldots, E_{n_0} \rangle \rtimes L = (\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{n_0})$$

Then $P \in \mathrm{Syl}_l(Sp(2n, q))$, and P is isomorphic to a Sylow l-subgroup of $GL_n(\mathbb{F}_q)$. □

12 The Orthogonal Groups at Non-defining Primes, $l \neq 2$

Theorem 12.1. *Let p be a prime, $q = p^r$, and l a prime with $l \neq 2, p$. Let k be a field with char $k \neq l$. Let d be the smallest positive integer such that $l \mid q^d - 1$, and let $n_0 = \lfloor \frac{n}{d} \rfloor$.*

$$\mathrm{ed}_k(P\Omega^\epsilon(n,q), l) = \mathrm{ed}_k(O^\epsilon(n,q), l) = \begin{cases} \mathrm{ed}_k(GL_m(\mathbb{F}_q), l), & n = 2m+1,\ d \text{ odd} \\ & \text{or } n = 2m, d \text{ odd}, \epsilon = + \\ \mathrm{ed}_k(GL_{m-1}(\mathbb{F}_q), l), & n = 2m, d \text{ odd}, \epsilon = - \\ \mathrm{ed}_k(GL_{2m}(\mathbb{F}_q), l), & n = 2m+1,\ d \text{ even} \\ & \text{or } n = 2m,\ d \text{ even}, n_0 \text{ even}, \epsilon = + \\ & \text{or } n = 2m, d \text{ even}, n_0 \text{ odd}, \epsilon = - \\ ed_k(GL_{2m-2}(\mathbb{F}_q), l), & n = 2m, d \text{ even}, n_0 \text{ odd}, \epsilon = + \\ & \text{or } n = 2m, d \text{ even}, n_0 \text{ even}, \epsilon = - \end{cases}$$

Remark 7. We do not need to prove the case $n = 2m+1, p = 2$ since $O^\epsilon(2m+1, 2^r) \cong Sp(2m, p^r)$ ([8], Theorem 14.2), so this case is taken care of in the work on the symplectic groups.

Proof. By Grove, for $p \neq 2$ ([8], Theorem 9.11 and Corollary 9.12),

$$|P\Omega(2m+1, q)| = \frac{|O(2m+1, q)|}{4} \qquad \text{and} \qquad |P\Omega^\epsilon(2m, q)| = \frac{|O^\epsilon(2m, q)|}{2(4, q^m - \epsilon 1)}.$$

For $p = 2$ ([8], Theorem 14.48 and Corollary 14.49),

$$|P\Omega^\epsilon(2m, q)| = \frac{|O^\epsilon(2m, q)|}{2}.$$

So in all cases, since $l \neq 2$, we have that $|P\Omega^\epsilon(n,q)|_l = |O^\epsilon(n,q)|_l$. Hence since $P\Omega^\epsilon(n,q)$ is a quotient of $O^\epsilon(n,q)$, we can conclude that their Sylow l-subgroups are congruent. Let d be the smallest positive integer such that $l \mid q^d - 1$ and let $s = \nu_l(q^d - 1)$.

The case $n = 2m+1$

If **d is even**: Then $|O(2m+1,q)|_l = |GL_{2m+1}(\mathbb{F}_q)|_l = |GL_{2m}(\mathbb{F}_q)|_l$. Hence since $O(2m+1,q)$ embeds in $GL_{2m+1}(\mathbb{F}_q)$ and $GL_{2m}(\mathbb{F}_q)$ embeds in $GL_{2m+1}(\mathbb{F}_q)$, we can conclude that the Sylow l-subgroups of $O(2m+1,q)$, $GL_{2m+1}(\mathbb{F}_q)$, $GL_{2m}(\mathbb{F}_q)$ are isomorphic.

If **d is odd**: Then by Stather ([25]), letting $m_0 = \lfloor \frac{m}{d} \rfloor$, we have

$$|O(2m+1,q)|_l = |GL_m(\mathbb{F}_q)|_l = l^{sm_0} \cdot P_l(S_{m_0})$$

Let ϵ be primitive l^s-th root in $\mathbb{F}_{q^d}$, and let E be the image of ϵ in $GL_d(\mathbb{F}_q)$. Let

$$E_1 = \begin{pmatrix} 1 &&&&&&&& \\ & E &&&&&&& \\ && 1 &&&&&& \\ &&& \ddots &&&&& \\ &&&& 1 &&&& \\ &&&&& (E^{-1})^T &&& \\ &&&&&& 1 && \\ &&&&&&& \ddots & \\ &&&&&&&& 1 \end{pmatrix}$$

$$\vdots$$

$$E_{m_0} = \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & E & & & & & & & \\ & & & & \mathrm{Id}_{m-m_0 d} & & & & & & \\ & & & & & 1 & & & & & \\ & & & & & & \ddots & & & & \\ & & & & & & & 1 & & & \\ & & & & & & & & (E^{-1})^T & & \\ & & & & & & & & & \mathrm{Id}_{m-m_0 d} \end{pmatrix}$$

Then for all i, $E_i \in O(2m+1, p^r)$. Note we can embed $P_l(S_{m_0})$ into $O(2m+1, q)$. Let

$$P = \langle E_1, \ldots, E_{n_0} \rangle \rtimes L = (\mathbb{Z}/l^s\mathbb{Z})^{n_0} \rtimes P_l(S_{m_0})$$

Then $P \in \mathrm{Syl}_l(O(2m+1, q))$, and P is isomorphic to a Sylow l-subgroup of $GL_m(\mathbb{F}_q)$.

The case $n = 2m$

Note that $O^\epsilon(n, q)$ embeds into $O^\epsilon(n+1, q)$ via

$$X \mapsto \begin{pmatrix} 1 & 0 \\ 0 & X \end{pmatrix}.$$

By Grove ([8], Theorem 9.11 and Corollary 9.12),

$$|O^+(2m, q)| = 2q^{m(m-1)}(q^m - 1) \prod_{i=1}^{m-1} (q^{2i} - 1).$$

$$|O^-(2m, q)| = 2q^{m(m-1)}(q^m + 1) \prod_{i=1}^{m-1} (q^{2i} - 1).$$

and

$$|O(2m+1,1)| = 2q^{m^2}\prod_{i=1}^{m}(q^{2i}-1).$$

Thus

$$\begin{aligned}
[O(2m+1,q) : O^+(2m,q)] &= q^m(q^m+1)\\
[O^+(2m,q) : O(2m-1,q)] &= q^{m-1}(q^m-1)\\
[O(2m+1,q) : O^-(2m,q)] &= q^m(q^m-1)\\
[O^-(2m,q) : O(2m-1,q)] &= q^{m-1}(q^m+1)
\end{aligned}$$

Note that since $l \neq 2$, either q^m+1 or q^m-1 is prime to l.

If q^m+1 is prime to l, then

$$\begin{aligned}
|O^+(2m,q)|_l &= |O(2m+1,q)|_l\\
|O^-(2m,q)|_l &= |O(2m-1,q)|_l
\end{aligned}$$

Thus when q^m+1 is prime to l, the Sylow l-subgroups of $O^+(2m,q)$ are isomorphic to those of $O(2m+1,q)$, and the Sylow l-subgroups of $O^-(2m,q)$ are isomorphic to those of $O(2m-1,q)$. If q^m-1 is prime to l, then

$$\begin{aligned}
|O^+(2m,q)|_l &= |O(2m-1,q)|_l\\
|O^-(2m,q)|_l &= |O(2m+1,q)|_l
\end{aligned}$$

Thus when q^m-1 is prime to l, the Sylow l-subgroups of $O^+(2m,q)$ are isomorphic to those of $O(2m-1,q)$, and the Sylow l-subgroups of $O^-(2m,q)$ are isomorphic to those of $O(2m+1,q)$.

We showed in the section on odd orthogonal groups that when d is even, the Sylow l-subgroups of $O(2m+1,q)$ are isomorphic to those of $GL_{2m}(\mathbb{F}_q)$, and when d is odd, the Sylow l-subgroups of $O(2m+1,q)$ are isomorphic to those of $GL_m(\mathbb{F}_q)$.

Recall that we defined $n_0 = \lfloor \frac{2m}{d} \rfloor$. By Stather [25],

$$|O^+(2m,q)|_l = \begin{cases} |GL_m(\mathbb{F}_q)|_l, & d \text{ odd} \\ |GL_{2m-2}(\mathbb{F}_q)|_l, & d \text{ even}, n_0 \text{ odd} \\ |GL_{2m}(\mathbb{F}_q)|_l, & d \text{ even}, n_0 \text{ even} \end{cases}$$

and

$$|O^-(2m,q)|_l = \begin{cases} |GL_{m-1}(\mathbb{F}_q)|_l, & d \text{ odd} \\ |GL_{2m}(\mathbb{F}_q)|_l, & d \text{ even}, n_0 \text{ odd} \\ |GL_{2m-2}(\mathbb{F}_q)|_l, & d \text{ even}, n_0 \text{ even} \end{cases}.$$

In order for this to match up with the isomorphisms to the odd orthogonal groups, we must have that when d is odd or d is even with n_0 even, then $q^m + 1$ is prime to l. When d is even with n_0 odd, then $q^m - 1$ is prime to l.

Case 1: d odd

For d odd, the Sylow l-subgroups of $O^+(2m,q)$ are isomorphic to those of $O(2m+1,q)$, which are isomorphic to those of $GL_m(\mathbb{F}_q)$ and the Sylow l-subgroups of $O^-(2m,q)$ are isomorphic to those of $O(2m-1,q)$, which are isomorphic to those of $GL_{m-1}(\mathbb{F}_q)$.

Case 2: d even, $\mathbf{n_0}$ odd

For d even, n_0 odd, the Sylow l-subgroups of $O^+(2m,q)$ are isomorphic to those of $O(2m-1,q)$, which are isomorphic to those of $GL_{2m-2}(\mathbb{F}_q)$ and the Sylow l-subgroups of $O^+(2m,q)$ are isomorphic to those of $O(2m+1,q)$, which are isomorphic to those of $GL_{2m}(\mathbb{F}_q)$.

Case 3: d even, $\mathbf{n_0}$ even

For d even, n_0 even, the Sylow l-subgroups of $O^+(2m,q)$ are isomorphic to those of $O(2m+1,q)$, which are isomorphic to those of $GL_{2m}(\mathbb{F}_q)$ and the Sylow l-subgroups of $O^-(2m,q)$ are isomorphic to those of $O(2m-1,q)$, which are isomorphic to those of $GL_{2m-2}(\mathbb{F}_q)$.

Putting the above results together, we get Theorem 12.1. □

13 The Unitary Groups at Non-defining Primes, $l \neq 2$

Theorem 13.1. *Let p be a prime, $q = p^r$, and l a prime with $l \neq 2, p$. Let k be a field with char $k \neq l$. Let d be the smallest positive integer such that $l \mid q^d - 1$. Then*

$$\mathrm{ed}_k(U(n,q^2),l) = \begin{cases} \mathrm{ed}_k(GL_n(\mathbb{F}_{q^2}),l), & d = 2 \pmod 4 \\ \mathrm{ed}_k(GL_{\lfloor \frac{n}{2} \rfloor}(\mathbb{F}_{q^2}),l), & d \neq 2 \pmod 4 \end{cases}$$

Proof. By Stather [25]

$$|U(n,q^2)|_l = \begin{cases} |GL_n(\mathbb{F}_{q^2})|_l, & d = 2 \pmod 4 \\ |GL_{\lfloor \frac{n}{2} \rfloor}(\mathbb{F}_{q^2})|_l, & d \neq 2 \pmod 4 \end{cases}$$

Case 1: $\mathbf{d = 2} \pmod{\mathbf{4}}$.

Since $U(n,q^2) \subset GL_n(\mathbb{F}_{q^2})$ and $|U(n,q^2)|_l = |GL_n(\mathbb{F}_{q^2})|_l$ in this case, we can immediately conclude that for $d = 2 \pmod 4$, the Sylow l-subgroups of $U(n,q^2)$ and $GL_n(\mathbb{F}_{q^2})$ are isomorphic.

Case 2: $\mathbf{d \neq 2} \pmod{\mathbf{4}}$

Let $s = \nu_l(q^d - 1)$. let ϵ be a primitive l^s-root of unity in $\mathbb{F}_{q^{2d}}$. Let E be the image of ϵ in $GL_d(\mathbb{F}_q)$.

For $n = 2m$, let

$$E_1 = \begin{pmatrix} E & & & & & & & \\ & 1 & & & & & & \\ & & \ddots & & & & & \\ & & & 1 & & & & \\ & & & & (\overline{E^{-1}})^T & & & \\ & & & & & 1 & & \\ & & & & & & \ddots & \\ & & & & & & & 1 \end{pmatrix}$$

$\vdots$

$$E_{\lfloor \frac{m}{d} \rfloor} = \begin{pmatrix} 1 & & & & & & & & & & \\ & \ddots & & & & & & & & & \\ & & 1 & & & & & & & & \\ & & & E & & & & & & & \\ & & & & \mathrm{Id}_{m-\lfloor \frac{m}{d} \rfloor d} & & & & & & \\ & & & & & 1 & & & & & \\ & & & & & & \ddots & & & & \\ & & & & & & & 1 & & & \\ & & & & & & & & (\overline{E^{-1}})^T & & \\ & & & & & & & & & \mathrm{Id}_{m-\lfloor \frac{m}{d} \rfloor d} \end{pmatrix}$$

For $n = 2m + 1$, let

$$E_1' = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & E_1 \end{pmatrix}, \ldots, E_{\lfloor \frac{m}{d} \rfloor} = \begin{pmatrix} 1 & \mathbf{0} \\ \mathbf{0} & E_{\lfloor \frac{m}{d} \rfloor} \end{pmatrix}$$

$P_l(S_{\lfloor \frac{m}{d} \rfloor})$ acts on $\langle E_1, \ldots, E_{\lfloor \frac{m}{d} \rfloor} \rangle \cong \langle E_1', \ldots, E'_{\lfloor \frac{m}{d} \rfloor} \rangle$. We can embed $P_l(S_{\lfloor \frac{m}{d} \rfloor})$ into $U(n, q^2)$. Let

$$P = \langle E_1, \ldots, E_{\lfloor \frac{m}{d} \rfloor} \rangle \rtimes P_l S_{\lfloor \frac{m}{d} \rfloor})$$

Then $P \in \mathrm{Syl}_l(U(n, q^2))$, and P is isomorphic to a Sylow l-subgroup of $GL_m(\mathbb{F}_{q^2})$, which is isomorphic to a Sylow l-subgroup of $GL_{\lfloor \frac{n}{2} \rfloor}(\mathbb{F}_{q^2})$. □

14 The Special Unitary Groups at Non-defining Primes, $l \neq 2$

Theorem 14.1. *Let p be a prime, $q = p^r$, and l a prime with $l \neq 2, p$. Let k be a field with char $k \neq l$. Then*

$$\mathrm{ed}_k(SU(n, q^2), l) = \begin{cases} \mathrm{ed}_k(U(n, q^2), l), & l \nmid q + 1 \\ \mathrm{ed}_k(SL_n(\mathbb{F}_{q^2}), l), & l \mid q + 1 \end{cases}$$

Proof. By Grove ([8], Theorem 11.28 and Corollary 11.29),

$$|SU(n,q^2)| = \frac{|U(n,q^2)|}{q+1}$$

If $l \nmid q+1$, then the Sylow l-subgroups of $SU(n,q^2)$ are isomorphic to the Sylow l-subgroups of $U(n,q^2)$. So we need only prove the case when $l \mid q+1$. Thus in this section, we will assume $l \mid q+1$. Then since $l \neq 2$, this implies that $l \nmid q-1$. Also, since $q^2-1 = (q+1)(q-1)$, we must have $l \mid q^2-1$. Let d' be the smallest positive integer such that $l \mid q^d - 1$. Then $d' = 2$. Let $s = \nu_l(q^2-1)$. Then since $l \nmid q-1$, we have that $s = \nu_l(q+1)$.

Note that when finding the Sylow l-subgroup of $GL_n(\mathbb{F}_{q^2})$, we would have d the smallest power of q^2 such that $l \mid (q^2)^d - 1$. So in this case, we would have $d = 1$. Then we would set $s = \nu_l((q^2)^d - 1) = \nu_l(q^2-1)$, so the s is still the same even though the d is different. We would have $n_0 = \lfloor \frac{n}{d} \rfloor = \lfloor \frac{n}{1} \rfloor = n$. Thus in the present case,

$$|GL_n(\mathbb{F}_{q^2})|_l = l^{sn} \cdot |S_n|_l.$$

So

$$|SU(n,q^2)|_l = \frac{|GL_n(\mathbb{F}_{q^2})|_l}{l^{\nu_l(q+1)}} = l^{s(n-1)} \cdot |S_n|_l = |SL_n(\mathbb{F}_{q^2})|_l|$$

Recall that $SU(n,q^2) = \{M \in U(n,q^2) : \det(M) = 1\}$ and $SL_n(\mathbb{F}_{q^2}) = \{M \in GL_n(\mathbb{F}_{q^2}) : \det(M) = 1\}$. Therefore, since the Sylow l-subgroups of $U(n,q^2)$ and $GL_n(\mathbb{F}_{q^2})$ are isomorphic, we can conclude that the Sylow l-subgroups of $SU(n,q^2)$ and $SL_n(\mathbb{F}_{q^2})$ are isomorphic. □

15 The Projective Special Unitary Groups at Non-defining Primes, $l \neq 2$

Theorem 15.1. *Let p be a prime, $q = p^r$, and l a prime with $l \neq 2, p$. Let k be a field with char $k \neq l$. Then*

$$\mathrm{ed}_k(PSU(n,q^2),l) = \begin{cases} \mathrm{ed}_k(SU(n,q^2),l), & l \nmid n \text{ or } l \nmid q+1 \\ \mathrm{ed}_k(PSL_n(\mathbb{F}_{q^2}),l), & l \mid n,\ l \mid q+1 \end{cases}$$

Proof. By Grove (Corollary 11.29),

$$|PSU(n,q^2)| = \frac{|SU(n,q^2)|}{(n,q+1)}.$$

If $l \nmid n$ or $l \nmid q+1$, then the Sylow l-subgroups of $PSU(n,q^2)$ are isomorphic to the Sylow l-subgroups of $SU(n,q^2)$. So we need only prove the case when $l \mid n,\ l \mid q+1$. Thus in this section, we will assume $l \mid n,\ l \mid q+1$. As before, this implies that $l \nmid q-1$ and $l \mid q^2-1$. Let $s = \nu_l(q^2-1)$. Then since $l \nmid q-1$, we have that $s = \nu_l(q+1)$.

By the same reasoning as in the section on the special unitary groups, we can conclude that the s here is the same as the s found for the special linear groups. Thus we have

$$|SL_n(\mathbb{F}_{q^2})| = l^{s(n-1)} \cdot |S_n|_l.$$

Let $t = \nu_l(n)$. Then

$$|PSU(n,q^2)|_l = \frac{|SL_n(\mathbb{F}_{q^2})|_l}{l^{min(\nu_l(n),\nu_l(q+1))}} = l^{s(n-1)-min(s,t)} \cdot |S_n|_l = |PSL_n(\mathbb{F}_{q^2})|_l$$

Since $PSU(n,q^2)$ and $PSL_n(\mathbb{F}_{q^2}))$ are obtained from $SU(n,q^2)$ and $SL_n(\mathbb{F}_{q^2})$ respectively by modding out by a cyclic group of order $l^{\min(s,t)}$ and the Sylow l-subgroups of $SU(n,q^2)$ and $GL_n(\mathbb{F}_{q^2})$ are isomorphic, we can conclude that the Sylow l-subgroups of $PSU(n,q^2)$ and $PSL_n(\mathbb{F}_{q^2})$ are isomorphic. □

16 The Unitary Groups, $l = 2$ and $q \equiv 3 \pmod 4$

The Unitary Groups

Theorem 16.1. *Let $p \neq 2$ be a prime, $q = p^r$, k a field with char $k \neq 2$. Assume that $q \equiv 3 \pmod 4$, and let $s' = \nu_2(q+1)$. Assume that k contains a primitive $2^{s'}$-th root of unity.*

$$\mathrm{ed}_k(U(n,q^2),2) = \sum_{k=0}^{\mu_2(n)} (\lfloor \frac{n}{2^k} \rfloor - 2\lfloor \frac{n}{2^{k+1}} \rfloor) 2^k$$

Proof. By Stather [25]

$$|U(n,q^2)|_2 = 2^{\nu_2(n!)} 2^{s'n}$$

Note that

$$|\{a \in \mathbb{F}_{q^2} : a\overline{a} = 1\}| = q+1.$$

Let ϵ be an element of order $2^{s'}$ in $\{a \in \mathbb{F}_{q^2} : a\overline{a} = 1\}$. Then let

$$E_1 = \begin{pmatrix} \epsilon & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{pmatrix}, \ldots, E_n = \begin{pmatrix} 1 & & & \\ & \ddots & & \\ & & 1 & \\ & & & \epsilon \end{pmatrix}$$

Let

$$\begin{aligned} P &= \langle E_1, \ldots, E_n \rangle \rtimes P_2(S_n) \\ &\cong (\mathbb{Z}/2^{s'}\mathbb{Z})^n \rtimes P_2(S_n) \end{aligned}$$

Then $P \in \mathrm{Syl}_2(U(n,q^2))$. By the same reasoning as for $GL_n(\mathbb{F}_q)$,

$$\mathrm{ed}_k(U(n,q^2),2) = \sum_{k=0}^{\mu_2(n)} (\lfloor \frac{n}{2^k} \rfloor - 2\lfloor \frac{n}{2^{k+1}} \rfloor) 2^k.$$

$\square$

The Special Unitary Groups and Projective Special Unitary Groups

Theorem 16.2. *Let $p \neq 2$ be a prime, $q = p^r$, k a field with char $k \neq 2$. Assume that $q \equiv 3 \pmod 4$, and let $s' = \nu_2(q+1)$. Assume that k contains a primitive $2^{s'}$-th root of unity. Let $\mu_2(n)'$ denote the smallest k such that $\lfloor \frac{n}{2^k} \rfloor - \lfloor \frac{n}{2^{k+1}} \rfloor > 0$. Then*

$$\mathrm{ed}_k(SU_n(\mathbb{F}_q), 2) = \left(\sum_{k=\mu_l(n)'}^{\mu_l(n)} \left(\lfloor \frac{n}{2^k} \rfloor - 2 \lfloor \frac{n}{2^{k+1}} \rfloor \right) l^k \right) - 2^{\mu_2(n)'}$$

Proof. Note that

$$|\{a \in \mathbb{F}_{q^2} : a\overline{a} = 1\}| = q + 1.$$

Let ϵ be an element of order $2^{s'}$ in $\{a \in \mathbb{F}_{q^2} : a\overline{a} = 1\}$. Then let

$$E_1 = \begin{pmatrix} \epsilon & & & & \\ & \frac{1}{\epsilon} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}, \ldots, E_{n-1} = \begin{pmatrix} 1 & & & & \\ & \ddots & & & \\ & & 1 & & \\ & & & \epsilon & \\ & & & & 1/\epsilon \end{pmatrix}, E_n = \begin{pmatrix} \frac{1}{\epsilon} & & & & \\ & 1 & & & \\ & & \ddots & & \\ & & & 1 & \\ & & & & \epsilon \end{pmatrix}$$

Then in $SU(n, q^2)$ these all generate distinct cyclic subgroups except E_n and $E_n = \prod_{i=1}^{n-1} E_i^{2^{s'}-1}$. Let

$$\begin{aligned} P &= \langle E_1, \ldots, E_n \rangle \rtimes P_2(S_n) \\ &\cong (\mathbb{Z}/2^{s'}\mathbb{Z})^{n-1} \rtimes P_2(S_n) \end{aligned}$$

Then $P \in \mathrm{Syl}_2(SU(n, q^2))$. By the same reasoning as for $SL_n(\mathbb{F}_q)$,

$$\mathrm{ed}_k(SU(n, q^2), 2) = \left(\sum_{k=\mu_l(n)'}^{\mu_l(n)} \left(\lfloor \frac{n}{2^k} \rfloor - 2 \lfloor \frac{n}{2^{k+1}} \rfloor \right) l^k \right) - 2^{\mu_2(n)'}.$$

□

Theorem 16.3. *Let $p \neq 2$ be a prime, $q = p^r$, k a field with char $k \neq 2$. Assume that $q \equiv 3 \pmod 4$, and let $s' = \nu_2(q+1)$. Assume that k contains a primitive $2^{s'}$-th root of unity.*

$$\mathrm{ed}_k(PSU(n, q^2), 2) = \mathrm{ed}_k(SU(n, q^2), 2).$$

Proof. By Grove ([8], Theorem 11.28 and Corollary 11.29),

$$|PSU(n, q^2)| = \frac{|SU(n, q^2)|}{(n, q+1)}.$$

Thus if n is odd, the 2-Sylow subgroups are isomorphic. So we need only consider the case $n = 2m$. The proof is almost identical to that for $PSL_n(\mathbb{F}_q)$.

□

References

[1] M Bardestani, K. Mallahi-Karai, and H. Salmasian. Minimal dimension of faithful representations for p-groups. *Journal of Group Theory*, 19(4):589–608, 2016. https://arxiv.org/abs/1505.00626.

[2] G. Berhuy and G. Favi. Essential dimension: A functorial point of view (after A. Merkurjev). *Doc. Math.*, 8:279–330, 2003. https://www.math.uni-bielefeld.de/documenta/vol-08/11.pdf.

[3] P. Brosnan and N. Fakhruddin. Fixed points, local monodromy, and incompressibility of congruence covers, 2020. https://arxiv.org/abs/2007.01752.

[4] J. Buhler and Z. Reichstein. On the essential dimension of a finite group. *Composito Mathematica*, 106:159–179, 1997. https://www.cambridge.org/core/journals/compositio-mathematica/article/on-the-essential-dimension-of-a-finite-group/61533FF3CA007959ED6B36C1002C1C3A.

[5] A. Duncan. Essential dimensions of A_7 and S_7. *Math. Res. Lett.*, 17(2):263–266, 2010. https://arxiv.org/abs/0908.3220v1.

[6] A. Duncan and Z. Reichstein. Pseudo-reflection groups and essential dimension. *J. Lond. Math. Soc., II. Ser.*, 90(3):879–902, 2014. https://arxiv.org/abs/1307.5724.

[7] B. Farb, M. Kisin, and J. Wolfson. Modular functions and resolvent problems. https://arxiv.org/abs/1912.12536, 2018.

[8] L. Grove. *Classical Groups and Geometric Algebra.* American Mathematical Society, 2000. Graduate Studies in Mathematics Volume 39.

[9] I. M. Isaacs. *Character Theory of Finite Groups.* Academic Press, 1976.

[10] N. Karpenko and A. Merkurjev. Essential dimension of finite p-groups. *Inventiones mathematicae*, 172:491–508, 2008. https://www.math.ucla.edu/~merkurev/papers/esdim-final.pdf.

[11] S. Lang. *Algebra*, volume 211 in Graduate Texts in Mathematics. Springer, 2002.

[12] M. Marjoram. Irreducible characters of a Sylow p-subgroup of the orthogonal group. *Commun. Algebra*, 27(3):1171–1195, 1999. https://www.researchgate.net/publication/28238784_Irreducible_characters_of_a_Sylow_p-subgroup_of_the_orthogonal_group.

[13] A. Merkurjev. Essential dimension. In *Séminaire Bourbaki. Volume 2014/2015. Exposés 1089–1103*, pages 423–448, ex. Paris: Société Mathématique de France (SMF), 2016. https://www.math.ucla.edu/~merkurev/papers/Exp1102.A.Merkurjev.2.pdf.

[14] A. Meyer and Z. Reichstein. The essential dimension of the normalizer of a maximal torus in the projective linear group. *Algebra Number Theory*, 3(4):467–487, 2009. https://arxiv.org/abs/0809.1688.

[15] A. Meyer and Z. Reichstein. Some consequences of the Karpenko-Merkurjev theorem. *Doc. Math.*, Extra Vol: Andrei A. Suslin sixtieth birthday:445–457, 2010. https://arxiv.org/abs/0811.2517.

[16] A. Moretó. On the minimal dimension of a faithful linear representation of a finite group, 2021. https://arxiv.org/abs/2102.01463.

[17] K. Pommerening. Quadratic equations in finite fields of characteristic 2. *unpublished manuscript*, 2000, English version 2012. https://www.staff.uni-mainz.de/pommeren/MathMisc/QuGlChar2.pdf.

[18] A. Previtali. On a conjecture concerning character degrees of some p-groups. *Arch. Math.*, 65(5):375–378, 1995. https://www.researchgate.net/publication/226465705_On_a_conjecture_concerning_character_degrees_of_somep-groups.

[19] A. Previtali. Orbit lengths and character degrees in p-Sylow subgroups of some classical Lie groups. *Journal of Algebra*, 177(3):658–675, 1995. https://www.sciencedirect.com/science/article/pii/S0021869385713221.

[20] Z. Reichstein. Essential dimension. *Proceedings of the International Congress of Mathematicians*, II:162–188, 2010. Hackensack, NJ: World Scientific; New Delhi: Hindustan Book Agency.

[21] Z. Reichstein and A. Shukla. Essential dimension of double covers of symmetric and alternating groups. *J. Ramanujan Math. Soc.*, 35(4):357–372, 2020. https://arxiv.org/abs/1906.03698.

[22] Z. Reichstein and A. Vistoli. Dimension essentielle des groupes finis en caractéristique positive. *C. R., Math., Acad. Sci. Paris*, 356(5):463–467, 2018.

[23] J.P. Serre. *Linear Representations of Finite Groups*. Springer, 1977. Translated from the French by Leonard L. Scott.

[24] G.C. Shephard and J.A. Todd. Finite unitary reflection groups. *Canadian J. Math.*, 6:274–304, 1954. http://www.math.ucsd.edu/~nwallach/shephard-todd.pdf.

[25] M. Stather. Constructive sylow theorems for the classical groups. *Journal of Algebra*, 316(2):536–559. https://www.sciencedirect.com/science/article/pii/S0021869307001780.

[26] G. Venkataraman. On irreducibility of induced modules and an adaptation of the Wigner-Mackey method of little groups. *J. Korean Math. Soc.*, 50(6):1213–1222, 2013. https://arxiv.org/abs/0908.0026.

Appendix

In this appendix, we provide some details for the computations in this thesis.

Remark 4

Remark 4: Duncan and Reichstein calculated the essential p-dimension of the pseudo-reflection groups: For G a pseudo-reflection group with $k[V]^G = k[f_1, \cdots, f_n]$, $d_i = \deg(f_i)$, $\mathrm{ed}_k(G, p) = a(p) = |\{i : d_i \text{ is divisible by } p\}|$ ([6], Theorem 1.1). These groups overlap with the groups above in a few small cases (The values of d_i are in [24], Table VII):

(i) Group 12 in the Shephard-Todd classification, $Z_2.O \cong GL_2(\mathbb{F}_3)$: d_1, d_2 are $6, 8$; so

$$\mathrm{ed}_k(Z_2.O, 3) = 1 = \mathrm{ed}_k(GL_2(\mathbb{F}_3), 3).$$

(ii) Group 23 in the Shephard-Todd classification, $W(H_3) \cong \mathbb{Z}/2\mathbb{Z} \times PSL_2(\mathbb{F}_5)$: $d_1, \cdots d_3$ are $2, 6, 10$; so

$$\mathrm{ed}_k(W(H_3), 5) = 1 = \mathrm{ed}_k(PSL_2(\mathbb{F}_5), 5),$$

and

$$\mathrm{ed}_k(W(H_3), 3) = 1 = \mathrm{ed}_k(PSL_2(\mathbb{F}_5), 3).$$

(iii) Group 24 in the Shephard-Todd classification, $W(J_3(4)) \cong \mathbb{Z}/2\mathbb{Z} \times PSL_2(5)$: $d_1, \ldots, d_3$ are $4, 6, 14$; so

$$\mathrm{ed}_k(W(J_3(4)), 3) = 1 = \mathrm{ed}_k(PSL_2(5), 3)$$

and

$$\mathrm{ed}_k(W(J_3(4)), 7) = 1 = \mathrm{ed}_k(PSL_2(5), 7).$$

(iv) Group 32 in the Shephard-Todd classification, $W(L_4) \cong \mathbb{Z}/3\mathbb{Z} \times Sp(4, 3)$: $d_1, \cdots d_4$ are $12, 18, 24, 30$; so

$$\mathrm{ed}_k(W(L_4), 3) = 4 = 1 + \mathrm{ed}_k(Sp(4, 3), 3),$$

and

$$\text{ed}_k(W(L_4), 5) = 1 = \text{ed}_k(Sp(4,3), 5).$$

(v) Group 33 in the Shephard-Todd classification, $W(K_5) \cong \mathbb{Z}/2\mathbb{Z} \times PSp(4,3) \cong \mathbb{Z}/2\mathbb{Z} \times PSU(4,2)$: $d_1, \cdots d_5$ are $4, 6, 10, 12, 18$; so

$$\text{ed}_k(W(K_5), 3) = 3 = \text{ed}_k(PSp(4,3), 3),$$

$$\text{ed}_k(W(K_5), 2) = 5 = 1 + \text{ed}_k(PSU(4,2)),$$

$$\text{ed}_k(W(K_5), 5) = 1 = \text{ed}_k(PSp(4,3), 5) = \text{ed}_k(PSU(4,2^2), 5)$$

and

$$\text{ed}_k(W(K_5), 3) = 3 = \text{ed}_k(PSU(4,2^2), 3).$$

(vi) Group 35 in the Shephard-Todd classification, $W(E_6) \cong O^-(6,2)$: $d_1, \cdots, d_6$ are $2, 5, 6, 8, 9, 12$; so

$$\text{ed}_k(W(E_6), 2) = 4 = \text{ed}_k(O^-(6,2), 2),$$

$$\text{ed}_k(W(E_6), 5) = 1 = \text{ed}_k(O^-(6,2), 5),$$

and

$$\text{ed}_k(W(E_6), 3) = 3 = \text{ed}_k(O^-(6,2), 3).$$

(vii) Group 36 in the Shephard-Todd classification, $W(E_7) \cong \mathbb{Z}/2\mathbb{Z} \times Sp(6,2)$: $d_1, \cdots, d_7$ are $2, 6, 8, 10, 12, 14, 18$; so

$$\text{ed}_k(W(E_7), 2) = 7 = 1 + \text{ed}_k(Sp(6,2), 2),$$

$$\text{ed}_k(W(E_7), 5) = 1 = \text{ed}_k(Sp(6,2), 5),$$

$$\text{ed}_k(W(E_7), 3) = 3 = \text{ed}_k(Sp(6,2), 3),$$

and

$$\mathrm{ed}_k(W(E_7), 7) = 1 = \mathrm{ed}_k(Sp(6,2), 7).$$

(viii) Group 37 in the Shephard-Todd classification, $W(E_8)$ contains $O^+(8,2)$ as in index 2 subgroup: $d_1, \ldots, d_8$ are $2, 8, 12, 14, 18, 20, 24, 30$; so

$$\mathrm{ed}_k(W(E_8), 3) = 4 = \mathrm{ed}_k(O^+(8,2), 3),$$

$$\mathrm{ed}_k(W(E_8), 5) = 2 = \mathrm{ed}_k(O^+(8,2), 5),$$

and

$$\mathrm{ed}_k(W(E_8), 7) = 1 = \mathrm{ed}_k(O^+(8,2), 3).$$

Lemma 2.8

Lemma (2.8)**.** If $H \subset G$, then $\mathrm{ed}_k(H,p) \leq \mathrm{ed}_k(G,p)$.

Proof.

$$\begin{aligned}\mathrm{ed}_k(G,p) &= \mathrm{ed}_k(H^1(-;G)) \\ &= \sup_{E \text{ Galois } G\text{-algebra over } F,\ F/k \in \text{Fields}/k} \mathrm{ed}_k(E)\end{aligned}$$

And

$$\begin{aligned}\mathrm{ed}_k(G,p) &= \mathrm{ed}_k(H^1(-;G),p) \\ &= \sup_{E \text{ Galois } G\text{-algebra over } F,\ F/k \in \text{Fields}/k} \mathrm{ed}_k(E,p) \\ &= \sup_{E \text{ Galois } G\text{-algebra over } F} \big(\min \operatorname{trdeg}_k(F''))\big)\end{aligned}$$

where the minimum is taken over all

$$F'' \subset F' \text{ a finite extension, with } F \subset F'$$

$$[F' : F] \text{ finite s.t. } p \nmid [F' : F] \text{ and}$$

$$EF' = E'F'' \text{ for some } E' \text{ Galois } G\text{-algebra over } F''$$

Thus

$$\mathrm{ed}_k(G,p) = \sup_{E \text{ Galois } G\text{-algebra over } F} \min_{F\subset F' \text{ a finite extension and } p\nmid[F':F]} \min_{F'' \text{ s.t. } EF'=E'F'' \text{ for some } E' \text{ Galois } G\text{-algebra over } F''} \mathrm{trdeg}_k(F''))$$

And similarly,

$$\mathrm{ed}_k(H,p) = \sup_{E \text{ Galois } H\text{-algebra over } F} \min_{F\subset F' \text{ a finite extension and } p\nmid[F':F]} \min_{F'' \text{ s.t. } EF'=E'F'' \text{ for some } E' \text{ Galois } H\text{-algebra over } F''} \mathrm{trdeg}_k(F''))$$

Since H is a subgroup of G, we have that given a Galois H-algebra E over F, we can extend to a Galois G-algebra over F. Thus it suffices to show that for $E \subset E_1$ with E a Galois H-algebra over F and E_1 a Galois G-algebra over F, if $F \subset F'$ is a finite extension with $p \nmid [F' : F]$, then

$$\min_{F'' \text{ s.t. } EF'=E'F'' \text{ for some } E' \text{ Galois } H\text{-algebra over } F''} \mathrm{trdeg}_k(F''))$$
$$\leq \min_{F'' \text{ s.t. } E_1F'=E_1'F'' \text{ for some } E_1' \text{ Galois } G\text{-algebra over } F''} \mathrm{trdeg}_k(F''))$$

Let $F \subset F'$ be a finite extension with $p \nmid [F' : F]$. If F'' is such that there exists E_1' with $E_1F' = E_1'F''$, then there exists a Galois G algebra E' over F'' contained in $E_1'F'$ such that $E_0F'' = E'F'$. Let $E' = E_0 \cap E$. Then E' is a Galois H-algebra over F''. Hence F'' is considered in the min for $\mathrm{ed}_{\mathbb{C}}(H,p)$. Thus the desired inequality holds. Therefore,

$$\mathrm{ed}_k(H,p) \leq \mathrm{ed}_k(G,p).$$

□

Lemma 2.9

Lemma (2.9)**.** Let $S \in \mathrm{Syl}_p(G)$. Then $\mathrm{ed}_k(G,p) = \mathrm{ed}_k(S,p)$.

Proof. By Lemma 2.8, we already have $\mathrm{ed}_k(S,p) \leq \mathrm{ed}_k(G,p)$. So we only need to show that $\mathrm{ed}_k(G,p) \leq \mathrm{ed}_k(S,p)$. Since S is a subgroup of G, we have that given a Galois G-algebra E over F there exists an extension of F, $F_0 = E^S$, such that E is a Galois S-algebra over E^S. Thus it suffices to show that for E a Galois G-algebra over F, which is also a Galois S-algebra over $F_0 = E^S$,

$$\begin{aligned}
&\mathrm{ed}_k(G,p) \\
&\min_{F\subset F' \text{ a finite extension } \text{ and } p\nmid[F':F]} \\
&\qquad \min_{F'' \text{ s.t. } EF'=E'F'' \text{ for some } E' \text{ Galois } G\text{-algebra over } F''} \mathrm{trdeg}_k(F'')) \\
\leq &\min_{F_0\subset F' \text{ a finite extension } \text{ and } p\nmid[F':F_0]} \\
&\qquad \min_{F'' \text{ s.t. } EF'=E'F'' \text{ for some } E' \text{ Galois } S\text{-algebra over } F''} \mathrm{trdeg}_k(F''))
\end{aligned}$$

Note that since S is a subgroup of G of index prime to p and $[F_0 : F] = [E^S : F] = [G : S]$, we get that $p \nmid [F_0 : F]$. Given $F_0 \subset F'$ a finite extension and $p \nmid [F' : F_0]$, then

$$p \nmid [F' : F] = [F' : F_0][F_0 : F].$$

Thus F' is also considered in the minimum for $\mathrm{ed}_k(G,p)$, and so the desired inequality holds. Therefore,

$$\mathrm{ed}_k(G,p) \leq \mathrm{ed}_k(H,p).$$

□

Lemma 2.10

Lemma (2.10; [10], Remark 4.8)**.** If k a field of characteristic $\neq p$, k_1/k a finite field extension of degree prime to p, then $\mathrm{ed}_k(G,p) = \mathrm{ed}_{k_1}(G,p)$.

Proof. T : Fields$/k \to$ Sets be defined by $T(F/k) =$ the isomorphism class of G-torsors over Spec$F$. Recall that

$$\begin{aligned}
&\mathrm{ed}_k(G,p)\\
&= \sup_{t\in T(F), F/k\in \mathrm{Fields}/k} \mathrm{ed}_k(t,p)\\
&= \sup_{t\in T(F), F/k\in \mathrm{Fields}/k} \left(\min_{F''\subset F' \text{ s.t. } p\nmid [F':F''] \text{ and the image of } t \text{ in } T(F') \text{ is in } \mathrm{Im}(T(F'')\to T(F'))} \mathrm{trdeg}_k(F'') \right)
\end{aligned}$$

First we will show that $\mathrm{ed}_{\mathbf{k_1}}(\mathbf{G},\mathbf{p}) \leq \mathrm{ed}_{\mathbf{k}}(\mathbf{G},\mathbf{p})$:

Let F_1/k_1, $t_1 \in T(F)$. We want to show that there exist F/k, $t \in T(F)$ such that

$$\mathrm{ed}_{k_1}(t_1,p) \leq \mathrm{ed}_k(t,p).$$

In other words, if we are given $F'' \subset F'$ such that $p \nmid [F' : F'']$, the image of t in $T(F')$ is in $\mathrm{Im}(T(F'') \to T(F'))$, we need to be able to show that there exists $F_1'' \subset F_1'$ such that $p \nmid [F_1' : F_1'']$ and the image of t_1 in $T(F_1')$ is in $\mathrm{Im}(T(F_1'') \to T(F_1'))$ and

$$\mathrm{trdeg}_{k_1}(F_1'') \leq \mathrm{trdeg}_k(F'').$$

So, let $F = F_1$ and $t = t_1$. Suppose we are given $F'' \subset F'$ such that $p \nmid [F' : F'']$ and the image of t in $T(F')$ is in $\mathrm{Im}(T(F'') \to T(F'))$. In other words, there exists $t_2 \in T(F'')$, $t_3 \in T(F')$. such that t_2 and t_1 both map to t_3. Then let $F_1'' = F''k_1, F_1' = F'k_1$. Then since $p \nmid [k_1 : k]$ and G is a p-group, $t_2k_1 \in T(F_1''), t_3k_1 \in T(F_1')$, and t_1 and t_2k_1 both map to t_3k_1 in $T(F_1')$. Since $[F_1' : F_1''] \mid [F' : F'']$ and $p \nmid [F' : F'']$, we have that $p \nmid [F_1' : F_1'']$. Also the image of

t in $T(F_1')$ is in $\mathrm{Im}(T(F_1'') \to T(F_1'))$. Moreover, $\mathrm{trdeg}_{k_1} F_1'' = \mathrm{trdeg}_k F''$.

Therefore, we can conclude that $\mathrm{ed}_{\mathbf{k_1}}(\mathbf{T},\mathbf{p}) \leq \mathrm{ed}_{\mathbf{k}}(\mathbf{T},\mathbf{p})$.

Now we will show that $\mathrm{ed}_{\mathbf{k}}(\mathbf{G},\mathbf{p}) \leq \mathrm{ed}_{\mathbf{k_1}}(\mathbf{G},\mathbf{p})$:

Let F/k, $t \in T(F)$. We want to show that there exist F_1/k_1, $t_1 \in T(F')$ such that

$$\mathrm{ed}_k(t,p) \leq \mathrm{ed}_{k_1}(t_1,p).$$

In other words, if we are given $F_1'' \subset F_1'$ such that $p \nmid [F_1' : F_1'']$ and the image of t_1 in $T(F_1')$ is in $\mathrm{Im}(T(F_1'') \to T(F_1'))$, we need to be able to show that there exists $F'' \subset F'$ such that $p \nmid [F' : F'']$, the image of t in $T(F')$ is in $\mathrm{Im}(T(F'') \to T(F'))$ and

$$\mathrm{trdeg}_k(F'') \leq \mathrm{trdeg}_{k_1}(F_1'').$$

So, let $F_1 = Fk_1$ and let t_1 be the image of t in $T(F_1)$. Suppose we are given $F_1'' \subset F_1'$ such that $p \nmid [F_1' : F_1'']$ and the image of t_1 in $T(F_1')$ is in $\mathrm{Im}(T(F_1'') \to T(F_1'))$. Then let $F'' = F_1'', F' = F_1'$. Then $p \nmid [F' : F''] = [F_1' : F_1'']$, and the image of t in $T(F')$ is the image of t_1 in $T(F_1')$ (from $T(F_1)$), which is in $\mathrm{Im}(T(F'') \to T(F'))$. Moreover $\mathrm{trdeg}_k F'' = \mathrm{trdeg}_k F_1'' = \mathrm{trdeg}_{k_1} F_1''$, since k_1/k is a finite extension.

Therefore, we can conclude that $\mathrm{ed}_{\mathbf{k}}(\mathbf{T},\mathbf{p}) \leq \mathrm{ed}_{\mathbf{k_1}}(\mathbf{T},\mathbf{p})$.

$\square$

Lemmas 5.6 and 5.7

For any prime p, we define

$$S(p,n) = \{ \begin{pmatrix} A & 0_n \\ 0_n & (A^{-1})^T \end{pmatrix} \begin{pmatrix} \mathrm{Id}_n & B \\ 0_n & \mathrm{Id}_n \end{pmatrix} : A \in \mathrm{Up}_n(\mathbb{F}_{p^r}), B \in Sym(n,p^r)\}.$$

And it is easy to show that $S(p,n) \in \mathrm{Syl}_p(Sp(2n,p^r))$ and that

$$S(p,n) \cong Sym(n,p^r) \rtimes \mathrm{Up}_n(\mathbb{F}_{p^r}),$$

where the action is given by $A(B) = ABA^T$, where $B \in Sym(n, p^r), A \in \mathrm{Up}_n(\mathbb{F}_{p^r})$.

Lemma (5.6)**.** For $p \neq 2$, $S(p, n)$ the Sylow p-subgroup of $Sp(2n, p^r)$ defined above,

$$Z(S(p,n)) = \{\begin{pmatrix} \mathrm{Id}_n & D \\ 0_n & \mathrm{Id}_n \end{pmatrix} : D = \begin{pmatrix} d & \mathbf{0} \\ \mathbf{0} & 0_{n-1} \end{pmatrix}\} \cong \mathbb{F}_{p^r}^+ \cong (\mathbb{Z}/p\mathbb{Z})^r$$

For the proof of of this Lemma, we need the following lemma:

Lemma 16.4. *For $p \neq 2$, $D \in Sym(n, p^r)$, $AD = D(A^{-1})^T$ for all $A \in \mathrm{Up}_n(\mathbb{F}_{p^r})$ if and only if* $D = \begin{pmatrix} d & \mathbf{0} \\ \mathbf{0} & 0_{n-1} \end{pmatrix}$.

Granting this lemma, we can calculate the center:

Proof.

$$\begin{aligned} S(p,n) &= \{\begin{pmatrix} A & 0_n \\ 0_n & (A^{-1})^T \end{pmatrix} \begin{pmatrix} \mathrm{Id}_n & B \\ 0_n & \mathrm{Id}_n \end{pmatrix} : A \in \mathrm{Up}_n(\mathbb{F}_{p^r}), B \in Sym(n,p^r)\} \\ &= \{\begin{pmatrix} A & AB \\ 0_n & (A^{-1})^T \end{pmatrix} : A \in \mathrm{Up}_n(\mathbb{F}_{p^r}), B \in Sym(n,p^r)\}. \end{aligned}$$

Note that

$$\begin{pmatrix} A & AB \\ 0_n & (A^{-1})^T \end{pmatrix}^{-1} \begin{pmatrix} C & CD \\ 0_n & (C^{-1})^T \end{pmatrix} \begin{pmatrix} A & AB \\ 0_n & (A^{-1})^T \end{pmatrix} = \begin{pmatrix} A^{-1}CA & A^{-1}CAB + A^{-1}CD(A^{-1})^T - B((A^{-1}CA)^{-1})^T \\ 0_n & ((A^{-1}CA)^{-1})^T \end{pmatrix}$$

So $\begin{pmatrix} C & CD \\ 0_n & (C^{-1})^T \end{pmatrix} \in Z(S(p,n))$ if and only if $C \in Z(\mathrm{Up}_n(\mathbb{F}_{p^r}))$ and

$$CD = CB + CA^{-1}D(A^{-1})^T - B(C^{-1})^T, \qquad \text{for all } A \in \mathrm{Up}_n(\mathbb{F}_{p^r}), B \in Sym(n,p^r).$$

Choosing $A, B = \mathrm{Id}_n$, we need $CD = C + CD - (C^{-1})^T$. So $C = (C^{-1})^T$ and thus $C = \mathrm{Id}_n$. So the other requirement above becomes

$$D = A^{-1}D(A^{-1})^T \Leftrightarrow AD = D(A^{-1})^T, \qquad \text{for all } A \in \mathrm{Up}_n(\mathbb{F}_{p^r}).$$

By Lemma 16.4, we get that

$$Z(S(p,n)) = \{ \begin{pmatrix} \mathrm{Id}_n & D \\ 0_n & \mathrm{Id}_n \end{pmatrix} : D = \begin{pmatrix} d & \mathbf{0} \\ \mathbf{0} & 0_{n-1} \end{pmatrix} \}$$

□

Proof of Lemma 16.4.

$\Leftarrow$: This is a straightforward calculation.

$\Rightarrow$: We will prove this by induction.

Base Case: When $n = 2$, we can write $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $D = \begin{pmatrix} x & y \\ y & z \end{pmatrix}$.

$$AD = \begin{pmatrix} x + ay & y + az \\ y & z \end{pmatrix},$$

and

$$D(A^{-1})^T = \begin{pmatrix} x - ay & y - az \\ y & z \end{pmatrix}.$$

So the condition that $AD = D(A^{-1})^T$ for all A implies that $y = 0$ and $z = 0$.

Induction Step: Write

$$D = \begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & \cdots & d_{1,n} \\ d_{1,2} & d_{2,2} & d_{2,3} & \cdots & d_{2,n} \\ \vdots & & \ddots & & \vdots \\ d_{1,n-1} & d_{2,n-1} & \cdots & d_{n-1,n-1} & d_{n-1,n} \\ d_{1,n} & d_{2,n} & \cdots & d_{n-1,n} & d_{n,n} \end{pmatrix}, \qquad A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1,n} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Then

$$AD = \begin{pmatrix} d_{1,1} & \cdots & d_{1,n-1} & d_{1,n} \\ d_{2,2} & \cdots & d_{2,n-1} & d_{2,n} \\ \vdots & \ddots & & \vdots \\ d_{1,n-1} + a_{n-1,n} d_{1,n} & \cdots & d_{n-1,n-1} + a_{n-1,n} d_{n-1,n} & d_{n-1,n} + a_{n-1,n} d_{n,n} \\ d_{1,n} & \cdots & d_{n-1,n} & d_{n,n} \end{pmatrix}$$

and

$$D(A^{-1})^T = \begin{pmatrix} d_{1,1} & \cdots & d_{1,n-2} & d_{1,n-1} - a_{n-1,n} d_{1,n} & d_{1,n} \\ d_{1,2} & \cdots & d_{2,n-2} & d_{2,n-1} - a_{n-1,n} d_{2,n} & d_{2,n} \\ \vdots & \ddots & & \vdots & \\ d_{1,n-1} & \cdots & d_{n-1,n-2} & d_{n-1,n-1} - a_{n-1,n} d_{n-1,n} & d_{n-1,n} \\ d_{1,n} & \cdots & d_{n,n-2} & d_{n-1,n} - a_{n-1,n} d_{n,n} & d_{n,n} \end{pmatrix}$$

In order for these to be equal for all $a_{n-1,n}$, we must have $d_{k,n} = 0$ for all k. So the matrix

$$D' = \begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & \cdots & d_{1,n-1} \\ d_{1,2} & d_{2,2} & d_{2,3} & \cdots & d_{2,n-1} \\ \vdots & & \ddots & & \vdots \\ d_{1,n-2} & d_{2,n-2} & \cdots & d_{n-2,n-2} & d_{n-2,n} \\ d_{1,n-1} & d_{2,n-1} & \cdots & d_{n-2,n-1} & d_{n-1,n-1} \end{pmatrix}$$

satisfies the condition $A'D' = D'(A'^{-1})^T$ for all $A' \in \mathrm{Up}_{n-1}(\mathbb{F}_{p^r})$. By induction, we conclude that

$$D' = \begin{pmatrix} d & \mathbf{0} \\ \mathbf{0} & 0_{n-2} \end{pmatrix},$$

and hence

$$D = \begin{pmatrix} d & \mathbf{0} \\ \mathbf{0} & 0_{n-1} \end{pmatrix}.$$

□

Lemma (5.7)**.** For $S(2,n)$ the Sylow p-subgroup of $Sp(2n,2^r)$ defined above,

$$Z(S(2,n)) = \{ \begin{pmatrix} \mathrm{Id}_n & D \\ 0_n & \mathrm{Id}_n \end{pmatrix} : D_{i,j} = 0, \text{ for all } (i,j) \notin \{(1,1),(1,2),(2,1), D_{1,2} = D_{2,1}\}$$

$$\cong (\mathbb{F}_{2^r}^+)^2 \cong (\mathbb{Z}/2\mathbb{Z})^{2r}$$

For the proof, we need the following lemma:

Lemma 16.5. *For $p = 2$, $D \in Sym(n, 2^r)$, $AD = D(A^{-1})^T$ for all $A \in \mathrm{Up}_n(\mathbb{F}_{2^r})$ if and only if $D_{i,j} = 0$, for all $(i,j) \notin \{(1,1),(1,2),(2,1)\}$.*

Granting this lemma, we can calculate the center:

Proof.

$$\mathrm{Syl}_2(S(2,n)) = \{ \begin{pmatrix} A & AB \\ 0_n & (A^{-1})^T \end{pmatrix} : A \in \mathrm{Up}_n(\mathbb{F}_{2^r}), B \in Sym(n, 2^r)\}.$$

Just as for $p \neq 2$, $\begin{pmatrix} C & CD \\ 0_n & (C^{-1})^T \end{pmatrix} \in Z(\mathrm{Syl}_p(PSp(n,2^r)))$ if and only if $C = \mathrm{Id}_n$ and

$$D = A^{-1}D(A^{-1})^T \Leftrightarrow AD = D(A^{-1})^T, \qquad \text{for all } A \in \mathrm{Up}_n(\mathbb{F}_{p^r}).$$

By Lemma 16.5, then we have that

$$Z(S(2,n)) = \{ \begin{pmatrix} \mathrm{Id}_n & D \\ 0_n & \mathrm{Id}_n \end{pmatrix} : D_{i,j} = 0, \text{ for all } (i,j) \notin \{(1,1),(1,2),(2,1)\}\}$$

□

Proof of Lemma 16.5.

$\Leftarrow$: This is a straightforward calculation.

$\Rightarrow$: We will prove this by induction.

Base Case: When $n = 2$, we can write $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $D = \begin{pmatrix} x & y \\ y & z \end{pmatrix}$.

$$AD = \begin{pmatrix} x+ay & y+az \\ y & z \end{pmatrix},$$

and

$$D(A^{-1})^T = \begin{pmatrix} x+ay & y \\ y+az & z \end{pmatrix}.$$

So the condition that $AD = D(A^{-1})^T$ for all A implies that $z = 0$.

Remark 8. This calculation is the key difference between odd and even characteristic.

Induction Step: Assume that $n > 2$. Write

$$D = \begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & \cdots & d_{1,n} \\ d_{1,2} & d_{2,2} & d_{2,3} & \cdots & d_{2,n} \\ \vdots & & \ddots & & \vdots \\ d_{1,n-1} & d_{2,n-1} & \cdots & d_{n-1,n-1} & d_{n-1,n} \\ d_{1,n} & d_{2,n} & \cdots & d_{n-1,n} & d_{n,n} \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{n-1,n} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Then

$$AD = \begin{pmatrix} d_{1,1} & \cdots & d_{1,n-1} & d_{1,n} \\ d_{1,2} & \cdots & d_{2,n-1} & d_{2,n} \\ \vdots & \ddots & & \vdots \\ d_{1,n-1} + a_{n-1,n}d_{1,n} & \cdots & d_{n-1,n-1} + a_{n-1,n}d_{n-1,n} & d_{n-1,n} + a_{n-1,n}d_{n,n} \\ d_{1,n} & \cdots & d_{n-1,n} & d_{n,n} \end{pmatrix}$$

and

$$D(A^{-1})^T = \begin{pmatrix} d_{1,1} & \cdots & d_{1,n-2} & d_{1,n-1} + a_{n-1,n} d_{1,n} & d_{1,n} \\ d_{1,2} & \cdots & d_{2,n-2} & d_{2,n-1} + a_{n-1,n} d_{2,n} & d_{2,n} \\ \vdots & \ddots & & \vdots & \\ d_{1,n-1} & \cdots & d_{n-1,n-2} & d_{n-1,n-1} + a_{n-1,n} d_{n-1,n} & d_{n-1,n} \\ d_{1,n} & \cdots & d_{n,n-2} & d_{n-1,n} + a_{n-1,n} d_{n,n} & d_{n,n} \end{pmatrix}$$

In order for these to be equal for all $a_{n-1,n}$, we must have $d_{k,n} = 0$ for all k except $k = n-1$. Since $n > 2$, we can pick

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ & & \ddots & & \vdots \\ 0 & \cdots & 1 & a_{n-2,n-1} & 0 \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

By comparing the entries of AD and $D(A^{-1})^T$, we see that in order to have $AD = D(A^{-1})^T$ for all $a_{n-2,n-1}$, we must have $d_{k,n-1} = 0$ for all k except $k = n-2$. In particular, we get that $d_{n,n-1} = d_{n-1,n} = 0$. Thus $d_{k,n} = 0$ for all k. So the matrix

$$D' = \begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & \cdots & d_{1,n-1} \\ d_{1,2} & d_{2,2} & d_{2,3} & \cdots & d_{2,n-1} \\ \vdots & & \ddots & & \vdots \\ d_{1,n-2} & d_{2,n-2} & \cdots & d_{n-2,n-2} & d_{n-2,n} \\ d_{1,n-1} & d_{2,n-1} & \cdots & d_{n-2,n-1} & d_{n-1,n-1} \end{pmatrix}$$

satisfies the condition $A'D' = D'(A'^{-1})^T$ for all $A' \in \mathrm{Up}_{n-1}(\mathbb{F}_{p^r})$. By induction, we conclude that

$$D_{i,j} = 0, \text{ for all } (i,j) \notin \{(1,1),(1,2),(2,1)\}.$$

$\square$

Section 5.3 Calculation

The calculation that $H \in L_{\mathbf{b}}$ if and only if $\psi(\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1$ for all $\mathbf{d} \in (\mathbb{F}_{p^r})^{n(n+1)/2}$, where $\mathbf{hdh^T}$ is the vector corresponding to HDH^T under the isomorphism $Sym(n, p^r) \cong (\mathbb{F}_{p^r}^+)^{n(n+1)/2}$:

Remark 9. In all of the following, we view $\psi_{(b_j)}$ as a map on $\Delta \cong Sym(n, p^r) \cong \mathbb{F}_{p^r}^{n(n+1)/2}$. So $\psi_{(b_j)}(D, \mathrm{Id}) = \psi_{(b_j)}(D) = \psi(\mathbf{b} \cdot \mathbf{d})$, where $\mathbf{b} = (b_j)$ and $\mathbf{d}$ is the vector corresponding to the matrix D.

Note that $(0_n, H^{-1}) \in L_s$ if and only if for all $\mathbf{d} \in (\mathbb{F}_{p^r})^{n(n+1)/2} = D \in Sym(n, p^r)$,

$$\psi_{(b_j)}((0_n, H)(D, \mathrm{Id}_n)(0_n, H^{-1})) = \psi_{(b_j)}(D, \mathrm{Id}_n).$$

Let $\mathbf{hdh^T}$ denote the vector corresponding to HDH^T. Then since

$$\psi_{(b_j)}((0_n, H)(D, \mathrm{Id}_n)(0_n, H^{-1})) = \psi(\mathbf{b} \cdot \mathbf{hdh^T}),$$

and

$$\psi_{(b_j)}(D, \mathrm{Id}_n) = \psi(\mathbf{b} \cdot \mathbf{d}),$$

we get that $(0_n, H^{-1}) \in L_s$ if and only if for all $\mathbf{d} \in (\mathbb{F}_{p^r})^{n(n+1)/2} = D \in Sym(n, p^r)$,

$$\psi(\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1.$$

Proposition 5.8

Proposition (5.8)**.** For $p \neq 2$,

$$\min_{\mathbf{b} \in (\mathbb{F}_{p^r}^+)^{n(n+1)/2},\ b_1 \neq 0} \dim(\theta_{\mathbf{b},1}) = p^{r(n-1)}.$$

This minimum is achieved when $\mathbf{b} = (b, 0, \ldots, 0)$ with $b \neq 0$.

Write

$$H = \begin{pmatrix} 1 & h_{1,2} & h_{1,3} & \cdots & h_{1,n} \\ 0 & 1 & h_{2,3} & \cdots & h_{2,n} \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & h_{n-1,n} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \qquad D = \begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & \cdots & d_{1,n} \\ d_{1,2} & d_{2,2} & d_{2,3} & \cdots & d_{2,n} \\ \vdots & & \ddots & & \vdots \\ d_{1,n-1} & d_{2,n-1} & \cdots & d_{n-1,n-1} & d_{n-1,n} \\ d_{1,n} & d_{2,n} & \cdots & d_{n-1,n} & d_{n,n} \end{pmatrix}.$$

Then

$$\begin{aligned} &HDH^T - D \\ &= \begin{pmatrix} [\sum_{l=1}^n (h_{1,l} \sum_{k=1}^n d_{l,k} h_{1,k})] - d_{1,1} & [\sum_{l=2}^n (h_{2,l} \sum_{k=1}^n d_{l,k} h_{1,k})] - d_{1,2} & \cdots & (\sum_{k=1}^n d_{k,n} h_{1,k}) - d_{1,n} \\ [\sum_{l=1}^n (h_{1,l} \sum_{k=2}^n d_{l,k} h_{2,k})] - d_{1,2} & [\sum_{l=2}^n (h_{2,l} \sum_{k=2}^n d_{l,k} h_{2,k})] - d_{2,2} & \cdots & (\sum_{k=2}^n d_{k,n} h_{2,k}) - d_{2,n} \\ \vdots & & \ddots & \vdots \\ (\sum_{l=1}^n h_{1,l} d_{l,n}) - d_{1,n} & (\sum_{l=2}^n h_{2,l} d_{l,n}) - d_{2,n} & \cdots & 0 \end{pmatrix} \end{aligned}$$

We will prove the proposition in two steps:

Claim 16.6. For $p \neq 2$, for $s = (b_i)$, $b_1 \neq 0$, $|L_s| \leq |\operatorname{Up}_{n-1}(\mathbb{F}_{p^r})| = p^{r(n-1)(n-2)/2}$.

Claim 16.7. For $p \neq 2$, $s = (b, 0, \cdots, 0)$ with $b \neq 0$,

$$L_s = \operatorname{Stab}_L(\psi_s) = \{H : H_{1,j} = 0, \forall j \neq 1\} \cong \operatorname{Up}_{n-1}(\mathbb{F}_{p^r})$$

Proof of Claim 16.6. Pick $j_0 \neq 1$ and choose D with $d_{i,j} = 0$ except for $d_{1,j_0} = d_{j_0,1}$. Then we get that

$$HDH^T - D = \begin{pmatrix} 2d_{1,j_0}h_{1,j_0} & h_{2,j_0}d_{1,j_0} & \cdots & h_{j_0-1,j_0}d_{1,j_0} & 0 & \cdots & 0 \\ h_{2,j_0}d_{1,j_0} & 0 & & & \cdots & & 0 \\ \vdots & & & \ddots & & & \vdots \\ h_{j_0-1,j_0}d_{1,j_0} & 0 & & & \cdots & & 0 \\ 0 & & & & \cdots & & 0 \\ \vdots & & & \ddots & & & \vdots \\ 0 & 0 & & & \cdots & & 0 \end{pmatrix}$$

Thus we have

$$\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = 2d_{1,j_0}h_{1,j_0}B_{1,1} + \sum_{i=2}^{j_0-1} h_{i,j_0}d_{1,j_0}B_{1,i} = d_{1,j_0}\left(2h_{1,j_0}B_{1,1} + \sum_{i=2}^{j_0-1} h_{i,j_0}B_{1,i}\right)$$

If $\left(2h_{1,j_0}B_{1,1} + \sum_{i=2}^{j_0-1} h_{i,j_0}B_{1,i}\right) \neq 0$, then as we run through all the values for d_{1,j_0}, we will get that $\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})$ runs through all the values of $\mathbb{F}_{p^r}$. And since ψ is non-trivial, this means that $\psi(\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}))$ cannot always equal 1. This is a contradiction. So we must have

$$2h_{1,j_0}B_{1,1} + \sum_{i=2}^{j_0-1} h_{i,j_0}B_{1,i} = 0$$

for all choices of $j_0 \neq 1$. Recall that $B_{1,1} = b_1 \neq 0$. So, for all j_0, given h_{i,j_0} for $i > 1$, the above dictates h_{1,j_0}:

$$h_{1,j_0} = \frac{-1}{2B_{1,1}} \sum_{i=2}^{j_0-1} h_{i,j_0}B_{1,i}.$$

Thus we can conclude that for all $s = (b_i)$ with $b_1 \neq 0$,

$$|L_s| \leq |\{H : H_{1,j} \text{ fixed } \forall j \neq 1\}| = |\operatorname{Up}_{n-1}(\mathbb{F}_{p^r})| = p^{r(n-1)(n-2)/2}$$

□

Proof of Claim 16.7. Let B be the matrix corresponding to $s = (b, 0, \cdots, 0)$. Since the only nonzero entry of B is $B_{1,1} = b$, we have that

$$\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = b(\mathbf{hdh^T} - \mathbf{d})_1 = b\left([\sum_{l=1}^{n} (h_{1,l} \sum_{k=1}^{n} d_{l,k} h_{1,k})] - d_{1,1} \right).$$

By the proof of Claim 16.6, if $H \in L_s$, then $\forall j_0 \neq 1$, we must have

$$h_{1,j_0} = \frac{-1}{2B_{1,1}} \sum_{i=2}^{j_0-1} h_{i,j_0} B_{1,i} = 0.$$

And if $h_{1,j_0} = 0 \ \forall j \neq 1$, then we have

$$\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = b(h_{1,1} d_{1,1} h_{1,1} - d_{1,1}) = 0, \text{ since } h_{1,1} = 1$$

Thus we have shown that $(0_n, H^{-1}) \in L_s$ if and only if $h_{1,j} = 0, \forall j \neq 1$. Therefore,

$$L_s = \{(0_n, H^{-1}) : H_{1,j} = 0, \forall j \neq 1\} \cong \mathrm{Up}_{n-1}(\mathbb{F}_{p^r}).$$

□

Proposition 5.9

Proposition (5.9)**.** For $p = 2$, $n = 2$,

$$\min_{\mathbf{b} \in (\mathbb{F}_{p^r}^+)^3,\ b_1 \neq 0, b_2 \neq 0} \dim(\theta_{\mathbf{b},1}) = 2^{r-1}.$$

This minimum is achieved when $\mathbf{b} = (b_1, b_2, 0)$ with $b_1 \neq 0, b_2 \neq 0$.

If $\mathbf{b} = (b_1, b_2, 0)$ with $b_1 \neq 0, b_2 \neq 0$, then

$$\dim(\theta_{\mathbf{b},1}) = 2^r.$$

Proof. We will prove the proposition in two steps:

Step 1: Proving that for $\mathbf{p = 2, n = 2, s = (b_i), (b_1, b_2) \neq (0, 0)}$ **: if** $\mathbf{b_1, b_2 \neq 0}$**, then** $\mathbf{|L_s| \leq 2}$**, and otherwise** $\mathbf{|L_s| = 1}$.

$$HDH^T - D = \begin{pmatrix} [\sum_{l=1}^{2}(h_{1,l}\sum_{k=1}^{2} d_{l,k}h_{1,k})] - d_{1,1} & (\sum_{k=1}^{2} d_{k,2}h_{1,k}) - d_{1,2} \\ (\sum_{l=1}^{2} h_{1,l}d_{l,2}) - d_{1,2} & 0 \end{pmatrix}$$

Let $p = 2$, $s = (b_i)$ with $(b_1, b_2) \neq (0, 0)$.

Calculation 1. Choose $d_{i,j} = 0$ except for $d_{2,2}$.

Then we get that

$$HDH^T - D = \begin{pmatrix} h_{1,2}^2 d_{2,2} & h_{1,2}d_{2,2} \\ h_{1,2}d_{2,2} & 0 \end{pmatrix}$$

Thus we have

$$\begin{aligned} \mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) &= B_{1,1}h_{1,2}^2 d_{2,2} + B_{1,2}h_{1,2}d_{2,2} \\ &= d_{2,2}h_{1,2}(B_{1,1}h_{1,2} + B_{1,2}) \end{aligned}$$

Then since ψ is non-trivial, we must have $h_{1,2}(B_{1,1}h_{1,2} + B_{1,2}) = 0$. Thus either $h_{1,2} = 0$ or $B_{1,1}h_{1,2} + B_{1,2} = 0$. If $B_{1,1} \neq 0$, $B_{1,2} \neq 0$, then either $h_{1,2} = 0$ or $h_{1,2} = \frac{B_{1,2}}{B_{1,1}}$. If $B_{1,1} \neq 0$, $B_{1,2} = 0$ or $B_{1,1} = 0$, $B_{1,2} \neq 0$, then $h_{1,2} = 0$. Our findings can be summarized in a chart as follows (we only care when $(B_{1,1}, B_{1,2}) \neq (0, 0)$):

Case:	result	options
$B_{1,1} \neq 0, B_{1,2} \neq 0$	$h_{1,2} = 0$ or $h_{1,2} = \frac{B_{1,2}}{B_{1,1}}$	2
$B_{1,1} \neq 0, B_{1,2} = 0$	$h_{1,2} = 0$	1
$B_{1,1} = 0, B_{1,2} \neq 0$	$h_{1,2} = 0$	1

Thus we can conclude that for all $s = (b_i)$ with $(b_1, b_2) \neq (0, 0)$, then for $b_1, b_2 \neq 0$, $|L_s| \leq 2$ and otherwise $|L_s| = 1$.

Step 2: Showing that when $\mathbf{s} = (\mathbf{b_1}, \mathbf{b_2}, \mathbf{0})$ with $\mathbf{b_1} \neq \mathbf{0}, \mathbf{b_2} \neq \mathbf{0}, |\mathbf{L_s}| = \mathbf{2}$.

For $s = (b_1, b_2, b_3)$,

$$\mathbf{b}\cdot(\mathbf{hdh^T}-\mathbf{d}) = b_1\left([\sum_{l=1}^{2}(h_{1,l}\sum_{k=1}^{2}d_{l,k}h_{1,k})]-d_{1,1}\right)+b_2\left([\sum_{k=1}^{2}d_{k,2}h_{1,k}]-d_{1,2}\right)$$
$$= b_1h_{1,2}^2d_{2,2}+b_2d_{2,2}h_{1,2} \qquad \text{since we are working in char 2}$$
$$= d_{2,2}h_{1,2}(b_1h_1+b_2)$$

If $b_1 \neq 0, b_2 \neq 0$, then either $h_{1,2}=0$ or $h_1=\frac{b_2}{b_1}$. In either case, the above is identically zero. Thus $|L_s|=2$.

□

Proposition 5.10

Proposition (5.10)**.** For $p=2$, $n>2$,

$$\min_{\mathbf{b}\in(\mathbb{F}_{p^r}^+)^{n(n+1)/2},\ b_2\neq 0}\dim(\theta_{\mathbf{b},1}) = 2^{r(2n-3)-1}.$$

This minimum is achieved when $\mathbf{b}=(b_i)=(b_1,b_2,0,\ldots,0)$ with $b_1,b_2\neq 0$.

$$\min_{\mathbf{b}\in(\mathbb{F}_{p^r}^+)^{n(n+1)/2},\ b_1\neq 0}\dim(\theta_{\mathbf{b},1}) = 2^{r(n-1)-1}.$$

This minimum is achieved when $\mathbf{b}=(b_i)=(b_1,0,b_3,\ldots,0)$ with $b_1,b_3\neq 0$.

Proof. Again, we will prove this in two steps:

Step 1: Proving that for $\mathbf{p=2,n>2,s=(b_i),(b_1,b_2)\neq(0,0)}$: If $\mathbf{b_2\neq 0}$, then $\mathbf{|L_s|\leq 2^{r(n-2)(n-3)/2+1}}$, and if $\mathbf{b_2=0(\Rightarrow b_1\neq 0)}$, then $\mathbf{|L_s|\leq 2^{r(n-1)(n-2)/2+1}}$.

Calculation 1. For $j_0>2$, choose $d_{i,j}=0$ except for $d_{1,j_0}=d_{j_0,1}$.

Then
$$\mathbf{b}\cdot(\mathbf{hdh^T}-\mathbf{d}) = \sum_{i=2}^{j_0-1}h_{i,j_0}d_{1,j_0}B_{1,i} = d_{1,j_0}\sum_{i=2}^{j_0-1}h_{i,j_0}B_{1,i}$$

So for all $j_0>2$, we must have
$$\sum_{i=2}^{j_0-1}h_{i,j_0}B_{1,i}=0.$$

For $j_0 = 3$, this gives $h_{2,j_0} B_{1,2} = 0$, and thus if $B_{1,2} \neq 0$, we must have $h_{2,j_0} = 0$. For $2 \leq k \leq n$, if $B_{1,k} \neq 0$, then for all $j_0 > 3$, given h_{i,j_0} for $i \neq 1, k$, the above dictates h_{k,j_0}:

$$h_{k,j_0} = \frac{-1}{B_{1,k}} \sum_{i=2, i \neq k}^{j_0 - 1} h_{i,j_0} B_{1,i}.$$

Calculation 2. Now for $j_0 > 1$, choose $d_{i,j} = 0$ except for d_{j_0,j_0}.

Then

$$\mathbf{b} \cdot (\mathbf{h} \mathbf{d} \mathbf{h}^{\mathbf{T}} - \mathbf{d}) = d_{j_0,j_0} \left(\sum_{l=1}^{j_0-1} \sum_{k=l}^{j_0} B_{l,k} h_{l,j_0} h_{k,j_0} \right)$$

So for all $j_0 \neq 1$, we must have

$$\sum_{l=1}^{j_0-1} \sum_{k=l}^{j_0} B_{l,k} h_{l,j_0} h_{k,j_0} = 0.$$

Thus we have that for all $j_0 \neq 1$,

$$h_{1,j_0} (\sum_{k=1}^{j_0} B_{1,k} h_{k,j_0}) + \sum_{l=2}^{j_0-1} \sum_{k=l}^{j_0} B_{l,k} h_{l,j_0} h_{k,j_0} = 0$$

For $j_0 = 2$, this tells us $0 = h_{1,2}(B_{1,1} h_{1,2} + B_{1,2})$. If $B_{1,2} = 0 (\Rightarrow B_{1,1} \neq 0)$ or $B_{1,1} = 0 (\Rightarrow B_{1,2} \neq 0)$, then this implies that $h_{1,2} = 0$. If $B_{1,2} \neq 0$ and $B_{1,1} \neq 0$, then we have two options for $h_{1,2}$: $h_{1,2} = 0$ and $h_{1,2} = \frac{B_{1,2}}{B_{1,1}}$. For $j_0 > 2$, this is a quadratic expression for h_{1,j_0} in terms of $B_{i,j}$ and h_{k,j_0} for $k > 1$, namely

$$B_{1,1} h_{1,j_0}^2 + (\sum_{k=2}^{j_0} B_{1,k} h_{k,j_0}) h_{1,j_0} + \sum_{l=2}^{j_0-1} \sum_{k=l}^{j_0} B_{l,k} h_{l,j_0} h_{k,j_0} = 0$$

Thus for $j_0 > 2$, given h_{i,j_0} for $i > 1$, there are up to two options for h_{1,j_0}.

Calculation 3. Now for $j_0 > 2$, choose $d_{i,j} = 0$ except for $d_{2,j_0} = d_{j_0,2}$.

Then

$$\mathbf{b} \cdot (\mathbf{h} \mathbf{d} \mathbf{h}^{\mathbf{T}} - \mathbf{d}) = d_{2,j_0} \left(B_{1,2} h_{1,j_0} + \sum_{i=2}^{j_0} B_{1,i} h_{i,j_0} h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,i} h_{i,j_0} \right)$$

So for all $j_0 > 2$, we must have

$$B_{1,2}h_{1,j_0} + \sum_{i=2}^{j_0} B_{1,i}h_{i,j_0}h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,i}h_{i,j_0} = 0.$$

If $B_{1,2} \neq 0$, then for all $j_0 > 2$, given h_{i,j_0} for $i > 2$, the above dictates h_{1,j_0}:

$$h_{1,j_0} = \frac{-1}{B_{1,2}} \left(\sum_{i=2}^{j_0} B_{1,i}h_{i,j_0}h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,k}h_{i,j_0} \right)$$

Case 1. $b_2 \neq 0$

If $B_{1,2} = b_2 \neq 0$, then we have from the first calculation that for all $j_0 > 1$, given h_{i,j_0} for $i > 2$, h_{2,j_0} are dictated. By the second calculation we have that there are at most two options for $h_{1,2}$. And by the third calculation, h_{1,j_0} is dictated for $j_0 > 2$. Thus for $b_2 \neq 0$, we can conclude that

$$\begin{aligned}|L_s| &\leq |\{H : \text{ two options for } H_{1,2}, \text{ and } \forall j > 2, H_{1,j}, H_{2,j} \text{ fixed,}\}| \\ &= 2|\operatorname{Up}_{n-2}(\mathbb{F}_{p^r})| \\ &= 2^{r(n-2)(n-3)/2+1}.\end{aligned}$$

Case 2. $b_2 = 0, b_3 \neq 0$

If $B_{1,2} = b_2 = 0 (\Rightarrow B_{1,1} \neq 0)$: We have by the second calculation that for $j_0 > 2$,

$$0 = B_{1,1}h_{1,j_0}^2 + (\sum_{k=3}^{j_0} B_{1,k}h_{k,j_0})h_{1,j_0} + \sum_{l=2}^{j_0-1} \sum_{k=l}^{j_0} B_{l,k}h_{l,j_0}h_{k,j_0}$$

For $j_0 = 2$, we get $B_{1,1}h_{1,2}^2 = 0$. Thus we must have $h_{1,2} = 0$. For $j_0 = 3$, we get $0 = B_{1,1}h_{1,3}^2 + B_{1,3}h_{1,3} = h_{1,3}(B_{1,1}h_{1,3} + B_{1,3})$. Thus either $h_{1,3} = 0$ or $h_{1,3} = \frac{B_{1,3}}{B_{1,1}}$. For $j_0 > 3$, we have from the first calculation that $\sum_{i=3}^{j_0-1} h_{i,j_0}B_{1,i} = 0$, so the equality from the second calculation becomes

$$0 = B_{1,1}h_{1,j_0}^2 + B_{1,j_0}h_{1,j_0} + \sum_{l=2}^{j_0-1} \sum_{k=l}^{j_0} B_{l,k}h_{l,j_0}h_{k,j_0}$$

We will use the following proposition:

Proposition 16.8 ([17], Proposition 1). *In a finite field of order 2^r, for $f(x) = ax^2 + bx + c$, we have have the following:*

(i) f has exactly one root $\Leftrightarrow b = 0$.

(ii) f has exactly two roots $\Leftrightarrow b \neq 0$ and $Tr(\frac{ac}{b^2}) = 0$.

(iii) f has no root $\Leftrightarrow b \neq 0$ and $Tr(\frac{ac}{b^2}) = 1$,

where $Tr(x) = x + x^2 + \cdots + x^{2^r-1}$.

So, for $j_0 > 3$, if $B_{1,j_0} = 0$, then there is only one option for h_{1,j_0}. Otherwise, it might have two options or no options. Thus we have the following for $j_0 > 3$: If $B_{1,j_0} = 0$, then there is one option for h_{1,j_0}, but h_{k,j_0} can be anything for $k > 1$. And if $B_{1,j_0} \neq 0$, then there is only one option for h_{j_0,k_0} for all $k_0 > 2$ (by the first calculation with $k = j_0, j_0 = k_0$), but h_{1,j_0} might have two options. So we can obtain an upper bound for L_s by choosing $B_{1,j} = 0$ for all $j > 3$ and assuming all the options are in L_s. In this case $h_{2,j}$ can be anything, but $h_{1,j}$ is fixed for all j except $j = 3$, and there are two options for $h_{1,3}$ So we get that

$$\begin{aligned}
|L_s| &\leq |\{H : H_{1,j} \text{ fixed } \forall j \neq 3, H_{1,3} = 0 \text{ or } \frac{B_{1,3}}{B_{1,1}}\}| \\
&= 2|\operatorname{Up}_{n-1}(\mathbb{F}_{2^r})| \\
&= 2^{r(n-1)(n-2)/2+1}
\end{aligned}$$

Step 2: Showing that for $\mathbf{p = 2, n > 2}$: When $\mathbf{s = (b_1, b_2, 0, \cdots, 0)}$ with $\mathbf{b_1, b_2 \neq 0}$, $\mathbf{|L_s| = 2^{r(n-2)(n-3)/2+1}}$, and when $\mathbf{s = (b_1, 0, b_3, \cdots, 0)}$ with $\mathbf{b_1, b_3 \neq 0, |L_s| = 2^{r(n-1)(n-2)/2+1}}$.

Let $p = 2$, $s = (b_1, b_2, \cdots, b_n, 0, \cdots, 0)$. And let B be the corresponding matrix. Then

$$\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = b_1 \sum_{k=2}^{n} h_{1,k}^2 d_{k,k} + \sum_{j=2}^{n} b_j \left([\sum_{l=j}^{n} (h_{j,l} \sum_{k=1}^{n} d_{l,k} h_{1,k})] - d_{1,j} \right)$$

Case 1. $b_1, b_2 \neq 0, b_3, \cdots, b_n = 0$.

Since $B_{1,2} = b_2 \neq 0$, then we have from the first calculation in Step 1 that for all $j_0 > 2$,

$$h_{2,j_0} = \frac{-1}{B_{1,2}} \sum_{i=3}^{j_0-1} h_{i,j_0} B_{1,i} = 0.$$

By the second calculation we have that there are two options for $h_{1,2}$: $h_{1,2} = 0$ and $h_{1,2} = \frac{B_{1,2}}{B_{1,1}}$ And by the third calculation, for $j_0 > 2$,

$$h_{1,j_0} = \frac{-1}{B_{1,2}} \left(\sum_{i=2}^{j_0} B_{1,i} h_{i,j_0} h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,k} h_{i,j_0} \right) = \frac{-1}{B_{1,2}} B_{1,2} h_{2,j_0} h_{1,2} = 0$$

Thus we have

$$\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = d_{2,2} h_{1,2} (B_{1,1} h_{1,2} + B_{1,2})$$

So whether $h_{1,2} = 0$ or $h_{1,2} = \frac{B_{1,2}}{B_{1,1}}$, this is identically 0. Therefore

$$|L_s| = |\{H : H_{1,2} = 0 \text{ or } H_{1,2} = \frac{B_{1,2}}{B_{1,1}}, H_{1,j} = 0 = H_{2,j} \ \forall j > 0\}| = 2|\operatorname{Up}_{n-2}(\mathbb{F}_{2^r})| = 2^{r(n-2)(n-3)/2+1}$$

Case 2. $b_1 \neq 0, b_2 = \cdots = b_n = 0$.

If $B_{1,k} = b_k = 0$ for $2 \leq k \leq n$: We have the following by the work in Step 1:

$h_{1,2} = 0$. By the second calculation we have that there are two options for $h_{1,3}$: $h_{1,2} = 0$ and $h_{1,3} = \frac{B_{1,3}}{B_{1,1}}$. And for $j_0 > 3$,

$$0 = B_{1,1} h_{1,j_0}^2 + B_{1,j_0} h_{1,j_0} + \sum_{l=2}^{j_0-1} \sum_{k=l}^{j_0} B_{l,k} h_{l,j_0} h_{k,j_0} = B_{1,1} h_{1,j_0}^2$$

So we have $h_{1,j_0} = 0$ for $j_0 \neq 1$. Thus

$$\begin{aligned} \mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) &= b_1 \sum_{k=2}^{n} h_{1,k}^2 d_{k,k} && \text{since } b_i = 0 \text{ for } i > 1 \\ &= 0 && \text{since } h_{1,j_0} = 0 \text{ for } j_0 \neq 1 \end{aligned}$$

Therefore

$$|L_s| = |\{H : H_{1,3} = 0 \text{ or } H_{1,3} = \frac{B_{1,3}}{B_{1,1}}, H_{1,j_0} = 0 \text{ for } j_0 \neq 1,3\}| = 2|\operatorname{Up}_{n-1}(\mathbb{F}_{2^r})| = 2^{r(n-1)(n-2)/2+1}$$

□

Lemma 6.14

Lemma (6.14)**.** Let

$$S(2,2m) = \{ \begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} \operatorname{Id}_m & B \\ 0_m & \operatorname{Id}_m \end{pmatrix} : A \in \operatorname{Up}_m(\mathbb{F}_{2^r}), B \in Antisym_0(m, 2^r)\}.$$

Then $S(2,2m) \in \operatorname{Syl}_2(\Omega^\epsilon(2m, 2^r))$ for $\epsilon \in \{\pm\}$.

Proof. Since $\Omega^\epsilon(2m,2^r) \subset O^\epsilon(2m,2^r) \subset Sp(2m,2^r)$, we must have that for $S_1 \in \operatorname{Syl}_2(\Omega^\epsilon(2m,2^r))$, $S_2 \in \operatorname{Syl}_2(O^\epsilon(2m,2^r))$, $S_3 \in \operatorname{Syl}_2(Sp(2m,2^r))$, $S_1 \subset S_2 \subset S_3$. It is straightforward to show that for $S_3 \in \operatorname{Syl}_2(Sp(2m,2^r)$ for $S_3 = N \rtimes O$ where

$$N = \{ \begin{pmatrix} \operatorname{Id}_m & B \\ 0_m & \operatorname{Id}_m \end{pmatrix} : B \in Sym(m, p^r)\} \cong Sym(m, p^r)$$

and

$$O = \{ \begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} : A \in \operatorname{Up}_m(\mathbb{F}_{2^r})\} \cong \operatorname{Up}_m(\mathbb{F}_{2^r}).$$

Note O is a subgroup of both $\Omega^+(2m,2^r)$ and $\Omega^-(2m,2^r)$. O is isomorphic to $\operatorname{Up}_m(\mathbb{F}_{2^r})$. So $|O| = (2^r)^{m(m-1)/2}$. Let

$$N' = \{ \begin{pmatrix} \operatorname{Id}_m & B \\ 0_m & \operatorname{Id}_m \end{pmatrix} : B \in Antisym_0(m, 2^r)\} \subset N$$

Then $N' \cong Antisym_0(m, 2^r)$. And for $M \in N'$,

$$M^T A_m^+ M = \begin{pmatrix} 0_m & \mathrm{Id}_m \\ 0_m & B^T \end{pmatrix}$$

and for $x = (y, z)$,

$$Q(Mx) = y^T z + z^T B^T z$$

And

$$\begin{aligned} z^T B^T z &= \sum_{i,j} B_{i,j} z_i z_j \\ &= \sum_{i<j} 2B_{i,j} z_i z_j + \sum_{i=1}^{n} B_{i,i} z_i^2 \text{ since } B \in Antisym_0(m, 2^r) \subset Sym(m, 2^r) \\ &= 0 \text{ since we are in characteristic 2 and } B_{i,i} = 0,\ \forall i \end{aligned}$$

Therefore, $Q^+(Mx) = y^T z = Q^+(x)$ for all $x = (y, z)$. So $N'^+ \subset O^+(2n, p^r)$. Also, for $M = \begin{pmatrix} \mathrm{Id}_m & B \\ 0_n & \mathrm{Id}_m \end{pmatrix} \in N'$,

$$\begin{aligned} M^T A_n^- M &= \begin{pmatrix} \mathrm{Id}_n & 0_n \\ B^T & \mathrm{Id}_m \end{pmatrix} \begin{pmatrix} 0_m^1 & \mathrm{Id}_m \\ 0_m & 0_m^d \end{pmatrix} \begin{pmatrix} \mathrm{Id}_m & B \\ 0_m & \mathrm{Id}_m \end{pmatrix} \\ &= \begin{pmatrix} \mathrm{Id}_m & 0_m \\ B^T & \mathrm{Id}_m \end{pmatrix} \begin{pmatrix} 0_m^1 & \mathrm{Id}_m \\ 0_m & 0_m^d \end{pmatrix}, \text{ since } B_{m,m} = 0 \\ &= \begin{pmatrix} 0_m^1 & \mathrm{Id}_m \\ 0_m & B^T + 0_m^d \end{pmatrix} \end{aligned}$$

So for $x = (y, z)$,

$$\begin{aligned} Q^-(Mx) &= \mathbf{y}\mathbf{z}^T + y_m^2 + dz_m^2 + \mathbf{z}B^T\mathbf{z}^T \\ &= \mathbf{y}\mathbf{z}^T + y_m^2 + dz_m^2 \text{ since } \mathbf{z}B^T\mathbf{z}^T = 0 \text{ by the work shown above} \end{aligned}$$

$$= Q^-(x)$$

Therefore $N' \subset O^-(2n, p^r)$ as well. And

$$|N'| = (p^r)^{\sum_{k=1}^{m-1} k} = (p^r)^{m(m-1)/2}.$$

Then consider $N' \rtimes O \subset \Omega^\epsilon(2m, 2^r)$ for both $\epsilon = +$ and $\epsilon = -$ (the operation is inherited from $N \rtimes O$). Then we have

$$\begin{aligned}|N' \rtimes O| &= |N'| \cdot |O| \\ &= (2^r)^{n(n-1)/2} \cdot (2^r)^{m(m-1)/2} \\ &= 2^{rn(n-1)}\end{aligned}$$

We learned the following argument from an early draft of [7]:

Note that for $M = \begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} \in O$,

$$\begin{aligned}\delta^+_{2m,2^r}(M) &= \operatorname{rank}(\mathrm{Id}_{2m} - M) \mod 2 \\ &= \operatorname{rank}\begin{pmatrix} \mathrm{Id}_m + A & 0_m \\ 0_m & \mathrm{Id}_m + (A^{-1})^T \end{pmatrix} \mod 2 \\ &= 2 \operatorname{rank}(A) \mod 2 \\ &= 0\end{aligned}$$

And for $M = \begin{pmatrix} \mathrm{Id}_m & B \\ 0_m & \mathrm{Id}_m \end{pmatrix} \in N'$,

$$\delta^+_{2m,2^r}(M) = \operatorname{rank}(\mathrm{Id}_{2m} - M) \mod 2$$

$$= \text{rank}\begin{pmatrix} 0_m & B \\ 0_m & 0_m \end{pmatrix} \mod 2$$

$$= \text{rank}(B) \mod 2$$

And since B is symmetric with $B_{i,i} = 0$, $\forall i$, B determines an alternating symmetric bilinear form, and thus has even rank.

Thus, $\delta^+_{2m,2^r}(M) = 0$ for $M \in N'$ as well. Hence we have that both N' and O are in $\Omega^+(2m, 2^r) = SO^+(2m, 2^r) = \ker(\delta^+_{2m,2^r})$. Therefore, $N' \rtimes O \subset \Omega^+(2n, 2^r)$. And

$$|N' \rtimes O| = 2^{2m(m-1)} = |\Omega^\epsilon(2m, 2^r)|_2$$

Thus we can conclude that for $\epsilon = +, -$,

$$N' \rtimes O \in \text{Syl}_2(\Omega^\epsilon(2m, 2^r)$$

□

Lemmas 6.18 and 6.19

For $p \neq 2$, we define

$$S(p, 2m) = \{ \begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} \text{Id}_m & B \\ 0_m & \text{Id}_m \end{pmatrix} : A \in \text{Up}_m(\mathbb{F}_{p^r}), B \in Antisym(m, p^r)\}.$$

It is easy to show that $S(p, 2m)$ is isomorphic to the elements in $\text{Syl}_p(\Omega^{\pm}(2m, p^r))$ and that

$$S(p, 2m) \cong Antisym(m, p^r) \rtimes \text{Up}_m(\mathbb{F}_{p^r}),$$

where the action is given by $A(B) = ABA^T$.

We also define

$$S(p,2m+1) = \{ \begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & \mathrm{Id}_m & 0_m \\ \mathbf{0} & 0_m & \mathrm{Id}_n \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & A & 0_m \\ \mathbf{0} & 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathrm{Id}_m & B \\ \mathbf{0} & \mathbf{0} & \mathrm{Id}_m \end{pmatrix} : \mathbf{x} \in \mathbb{F}_{p^r}^m, A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), B \in Antisym(m,p^r)\}.$$

It is easy to show that $S(p,2m+1) \in \mathrm{Syl}_p(O(2m+1,p^r))$ and that

$$S(p,2m+1) \cong \big((\mathbb{F}_{p^r}^+)^m \times Antisym(m,p^r)\big) \rtimes \mathrm{Up}_m(\mathbb{F}_{p^r})),$$

where the action of $\mathrm{Up}_m(\mathbb{F}_{p^r})$ on $Antisym(m,p^r)$ is given by $A(B) = ABA^T$. and the action of $\mathrm{Up}_m(\mathbb{F}_{p^r})$ on $(\mathbb{F}_{p^r}^+)^m$ is given by $A(\mathbf{x}) = \mathbf{x}A^T$.

Lemma (6.18)**.** For any prime p, $m > 2$, let $S(p,2m) = S^+(p,2m)$ be defined as above and in Lemma 6.15. Then

$$Z(S(p,2m)) = \{ \begin{pmatrix} \mathrm{Id}_m & D \\ 0_m & \mathrm{Id}_m \end{pmatrix} : D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix} \} \cong \mathbb{F}_{p^r}^+ \cong (\mathbb{Z}/p\mathbb{Z})^r$$

For the proof, we need the following lemma:

Lemma 16.9. *Given* $D \in \begin{cases} Antisym(m,p^r) & p \neq 2 \\ Antisym0(m,2^r) & p = 2 \end{cases}$,

$$AD = D(A^{-1})^T \ \forall A \in \mathrm{Up}_m(\mathbb{F}_{p^r}) \Leftrightarrow D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix}.$$

Remark 10. This lemma is true for any $m \geq 2$.

Granting this lemmma, we can calculate the center:

Proof. For $p \neq 2$,

$$S(p,2m) = \{ \begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} \mathrm{Id}_m & B \\ 0_m & \mathrm{Id}_m \end{pmatrix} : A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), B \in Antisym(m,p^r)\}$$
$$= \{ \begin{pmatrix} A & AB \\ 0_m & (A^{-1})^T \end{pmatrix} : A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), B \in Antisym(m,p^r)\}.$$

and

$$S(2,2m) = \{ \begin{pmatrix} A & 0_m \\ 0_m & (A^{-1})^T \end{pmatrix} \begin{pmatrix} \mathrm{Id}_m & B \\ 0_m & \mathrm{Id}_m \end{pmatrix} : A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), B \in Antisym_0(m,2^r)\}$$
$$= \{ \begin{pmatrix} A & AB \\ 0_n & (A^{-1})^T \end{pmatrix} : A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), B \in Antisym_0(m,2^r)\}.$$

Note that for any p, given

$$\begin{pmatrix} A & AB \\ 0_m & (A^{-1})^T \end{pmatrix}, \begin{pmatrix} C & CD \\ 0_m & (C^{-1})^T \end{pmatrix} \in \Omega^+(2m,2^r)$$

we have

$$\begin{pmatrix} A & AB \\ 0_m & (A^{-1})^T \end{pmatrix}^{-1} \begin{pmatrix} C & CD \\ 0_m & (C^{-1})^T \end{pmatrix} \begin{pmatrix} A & AB \\ 0_m & (A^{-1})^T \end{pmatrix} = \begin{pmatrix} A^{-1}CA & A^{-1}CAB + A^{-1}CD(A^{-1})^T - B((A^{-1}CA)^{-1})^T \\ 0_m & ((A^{-1}CA)^{-1})^T \end{pmatrix}.$$

So

$$\begin{pmatrix} C & CD \\ 0_m & (C^{-1})^T \end{pmatrix} \in Z(S(p,2m))$$

if and only if

$$C \in Z(\mathrm{Up}_m(\mathbb{F}_{p^r})) = \{ \begin{pmatrix} 1 & 0 & x \\ \mathbf{0} & \mathrm{Id}_{m-2} & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \}$$

and

$$CD = CB + CA^{-1}D(A^{-1})^T - B(C^{-1})^T, \text{ for all } A \in \mathrm{Up}_m(\mathbb{F}_{p^r}), B \in \begin{cases} Antisym(m, p^r) & p \neq 2 \\ Antisym0(m, 2^r) & p = 2 \end{cases}.$$

Remark 11. For the remainder of this proof p can be any prime. (When $p = 2$, the negatives will go away, but the argument is the same.)

Choosing $A = \mathrm{Id}_m$, we need

$$CD = CB + CD - B(C^{-1})^T.$$

So we must have

$$CB = B(C^{-1})^T$$

for all

$$B \in \begin{cases} Antisym(m, p^r) & p \neq 2 \\ Antisym0(m, 2^r) & p = 2 \end{cases}.$$

Write

$$C = \begin{pmatrix} 1 & \mathbf{0} & x \\ \mathbf{0} & \mathrm{Id}_{m-2} & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{pmatrix} \in Z(\mathrm{Up}_m(\mathbb{F}_{p^r})).$$

$$(C^{-1})^T = \begin{pmatrix} 1 & \mathbf{0} & -x \\ \mathbf{0} & \mathrm{Id}_m & \mathbf{0} \\ 0 & \mathbf{0} & 1 \end{pmatrix}^T = \begin{pmatrix} 1 & \mathbf{0} & 0 \\ \mathbf{0} & \mathrm{Id}_m & \mathbf{0} \\ -x & \mathbf{0} & 1 \end{pmatrix}.$$

Then for

$$B = (b_{i,j}) \in \begin{cases} Antisym(m, p^r) & p \neq 2 \\ Antisym0(m, 2^r) & p = 2 \end{cases},$$

we get

$$CB = \begin{pmatrix} -xb_{1,m} & b_{1,2} - xb_{2,m} & & \cdots & b_{1,m-1} - xb_{m-1,m} & b_{1,m} \\ -b_{1,2} & 0 & b_{2,3} & & \cdots & b_{2,m} \\ \vdots & & \ddots & & & \vdots \\ -b_{1,m-1} & & & \cdots & & b_{m-1,m} \\ -b_{1,m} & & & \cdots & -b_{m-1,m} & 0 \end{pmatrix}$$

and

$$B(C^{-1})^T = \begin{pmatrix} -xb_{1,m} & b_{1,2} & & \cdots & b_{1,m} \\ -b_{1,2} - xb_{2,m} & 0 & b_{2,3} & \cdots & b_{2,m} \\ \vdots & & \ddots & & \vdots \\ -b_{1,m-1} - xb_{m-1,m} & -b_{2,m-1} & \cdots & & b_{m-1,m} \\ -b_{1,m} & -b_{2,m} & \cdots & -b_{m-1,m} & 0 \end{pmatrix}$$

So if $m > 2$, we must have $x = 0$, and hence $C = \mathrm{Id}_m$.

Remark 12. This is where I need $m > 2$.

So the other requirement above becomes

$$D = A^{-1}D(A^{-1})^T \Leftrightarrow AD = D(A^{-1})^T$$

for all $A \in \mathrm{Up}_m(\mathbb{F}_{p^r})$. Then by Lemma 16.9, we get that

$$Z(S(p, 2m)) = \{ \begin{pmatrix} \mathrm{Id}_m & D \\ 0_m & \mathrm{Id}_m \end{pmatrix} : D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix} \}$$

□

Proof of Lemma 16.9.

⇐: This is a straightforward calculation.

⇒: We will prove this by induction.

Base Case: When $m = 2$, we can write $A = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}$ and $D = \begin{pmatrix} 0 & x \\ -x & 0 \end{pmatrix}$.

$$AD = \begin{pmatrix} -ax & x \\ -x & 0 \end{pmatrix} = D(A^{-1})^T.$$

So the condition that $AD = D(A^{-1})^T$ always holds. When $m = 3$, we can write $A = \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix}$ and $D = \begin{pmatrix} 0 & x & y \\ -x & 0 & z \\ -y & -z & 0 \end{pmatrix}$.

$$AD = \begin{pmatrix} -ax - by & x - bz & y + az \\ -x - cy & -cz & z \\ -y & -z & 0 \end{pmatrix},$$

and

$$D(A^{-1})^T = \begin{pmatrix} -ax + acy - by & x - cy & y \\ -x + acy - bz & -cz & z \\ -y + az - acz + bz & -z & 0 \end{pmatrix}.$$

So in order for these to be equal for all A, we must have $y = 0$ and $z = 0$.

Induction Step: Write

$$D = \begin{pmatrix} 0 & d_{1,2} & d_{1,3} & \cdots & d_{1,m} \\ -d_{1,2} & 0 & d_{2,3} & \cdots & d_{2,m} \\ \vdots & & \ddots & & \vdots \\ -d_{1,m-1} & -d_{2,m-1} & \cdots & 0 & d_{m-1,m} \\ -d_{1,m} & -d_{2,m} & \cdots & -d_{m-1,m} & 0 \end{pmatrix}, \quad A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & a_{m-1,m} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

then

$$AD = \begin{pmatrix} 0 & d_{1,2} & d_{1,3} & \cdots & d_{1,m-1} & d_{1,m} \\ -d_{1,2} & 0 & d_{2,3} & \cdots & d_{2,m-1} & d_{2,m} \\ \vdots & & & \ddots & & \vdots \\ -d_{1,m-1} - a_{m-1,m}d_{1,m} & & \cdots & -d_{m-2,m-1} - a_{m-1,m}d_{m-1,m} & -a_{m-1,m}d_{m-1,m} & d_{m-1,m} \\ -d_{1,m} & & \cdots & & -d_{m-1,m} & 0 \end{pmatrix}$$

And

$$D(A^{-1})^T = \begin{pmatrix} 0 & d_{1,2} & d_{1,3} & \cdots & d_{1,m-2} & d_{1,m-1} - a_{m-1,m}d_{1,m} & d_{1,m} \\ -d_{1,2} & 0 & d_{2,3} & \cdots & d_{2,m-2} & d_{2,m-1} - a_{m-1,m} - d_{2,m} & d_{2,m} \\ \vdots & & & \ddots & & & \vdots \\ -d_{1,m-1} & & \cdots & & d_{m-1,m-2} & -a_{m-1,m}d_{m-1,m} & d_{m-1,m} \\ -d_{1,m} & & \cdots & & -d_{m,m-2} & -d_{m-1,m} & 0 \end{pmatrix}$$

In order for these to be equal for all $a_{m-1,m}$, we must have $d_{k,m} = 0$ for all $k \neq m-1$. Since $m > 2$, we can pick

$$A = \begin{pmatrix} 1 & 0 & 0 & \cdots & 0 \\ 0 & 1 & 0 & \cdots & 0 \\ & & \ddots & & \vdots \\ 0 & \cdots & 1 & a_{m-2,m-1} & 0 \\ 0 & 0 & \cdots & 1 & 0 \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix},$$

so we get

$$AD = \begin{pmatrix} 0 & d_{1,2} & d_{1,3} & \cdots & d_{1,m-1} & d_{1,m} \\ -d_{1,2} & 0 & d_{2,3} & \cdots & d_{2,m-1} & d_{2,m} \\ \vdots & & \ddots & & & \vdots \\ -d_{1,m-2} - a_{m-2,m-1}d_{1,m-1} & & \cdots & -a_{m-2,m-1}d_{m-2,m-1} & d_{m-2,m-1} & d_{m-2,m} + a_{m-2,m-1}d_{m-1,m} \\ -d_{1,m-1} & & \cdots & -d_{m-2,m-1} & 0 & d_{m-1,m} \\ -d_{1,m} & & \cdots & & -d_{m-1,m} & 0 \end{pmatrix}$$

And

$$D(A^{-1})^T = \begin{pmatrix} 0 & \cdots & d_{1,m-3} & d_{1,m-2} - a_{m-2,m-1}d_{1,m-1} & d_{1,m-1} & d_{1,m} \\ -d_{1,2} & \cdots & d_{2,m-3} & d_{2,m-2} - a_{m-2,m-1}d_{2,m-1} & d_{2,m-1} & d_{2,m} \\ \vdots & & \ddots & & \vdots & \\ -d_{1,m-2} & \cdots & -d_{m-2,m-3} & -a_{m-2,m-1}d_{m-2,m-1} & d_{m-2,m-1} & d_{m-2,m} \\ -d_{1,m-1} & \cdots & -d_{m-1,m-3} & -d_{m-2,m-1} & 0 & d_{m-1,m} \\ -d_{1,m} & \cdots & -d_{m,m-3} & -d_{m-2,m} + a_{m-2,m-1}d_{m-1,m} & -d_{m-1,m} & 0 \end{pmatrix}$$

In order for these to be equal for all $a_{m-2,m}$, we must have $d_{k,m-1} = 0$ for all $k \neq m-2$. In particular, we get that $d_{nm,m-1} = d_{m-1,m} = 0$. Thus $d_{k,m} = 0$ for all k. So the matrix

$$D' = \begin{pmatrix} d_{1,1} & d_{1,2} & d_{1,3} & \cdots & d_{1,m-1} \\ -d_{1,2} & d_{2,2} & d_{2,3} & \cdots & d_{2,m-1} \\ \vdots & & \ddots & & \vdots \\ -d_{1,m-2} & -d_{2,m-2} & \cdots & d_{m-2,m-2} & d_{m-2,m} \\ -d_{1,m-1} & -d_{2,m-1} & \cdots & -d_{m-2,m-1} & d_{m-1,m-1} \end{pmatrix}$$

satisfies the condition $A'D' = D'(A'^{-1})^T$ for all $A' \in U_{m-1}(\mathbb{F}_{p^r})$. By induction, we conclude that

$$D' = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-3} \end{pmatrix},$$

and hence

$$D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix}.$$

□

Lemma (6.19)**.** For $p \neq 2$, $S(p, 2m+1)$ defined as above,

$$Z(S(p,2m+1)) = \{ \begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & \mathrm{Id}_m & D \\ \mathbf{0} & 0_m & \mathrm{Id}_m \end{pmatrix} : \mathbf{x} = (x_1, 0, \ldots, 0), D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix} \} \cong (\mathbb{F}_{p^r}^+)^2$$

Proof.

Case 1: $\mathbf{n = 5}$

The proof for $n > 5$ uses the result for $Z(S(p, 2m))$, which we only calculated for $m > 2$. So we must prove the case $m = 2$ separately:

For $m = 2$, the action of $\mathrm{Up}_2(\mathbb{F}_{p^r}) \cong \mathbb{F}_{p^r}$ on $Antisym(2, p^r) \cong \mathbb{F}_{p^r}$ is trivial. And the action on $\mathbb{F}_{p^r}^2$ is given by $a(x, y) = (x + ay, y)$. So we have $S(p, 5) \cong \mathbb{F}_{p^r}^2 \rtimes \mathbb{F}_{p^r}^2$, where the action of $\mathbb{F}_{p^r}^2$ (2nd copy) on $\mathbb{F}_{p^r}^2$ (1st copy) is given by $(b, a)\,((x, y)) = (x + ay, y)$. An element $((x, y), (a, b))$ is in the center if and only if for all $((w, z), (d, c))$ we have

$$((w, z), (d, c))((x, y), (b, a)) = ((x, y), (b, a))((w, z)(d, c))$$

Note that

$$((w, z), (d, c))((x, y), (b, a)) = ((x + w + cy, y + z), (b + d, a + c))$$

and

$$((x, y), (b, a))((w, z)(d, c)) = ((x + w + az, y + z), (b + d, a + c))$$

These will be equal for all $((w, z), (d, c))$ if and only if $a = 0 = y$. Therefore the center is given by

$$\{((x, 0), (b, 0)) : x, b \in \mathbb{F}_{p^r}\}.$$

Translating this back into the original form in a matrix, we get that the center is

$$Z(S(p,5)) = \{ \begin{pmatrix} 1 & 0 & 0 & w & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 \\ w & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & b \\ 0 & 0 & 1 & -b & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 & w & 0 \\ 0 & 1 & 0 & 0 & b \\ 0 & 0 & 1 & -b & 0 \\ w & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{pmatrix} \} \cong (\mathbb{F}_{p^r})^2$$

Case 2: $\mathbf{n > 5}$

Since

$$S(p, 2m+1) \cong (\mathbb{F}_{p^r}^+)^m \rtimes (Antisym(m, p^r) \rtimes \mathrm{Up}_m(\mathbb{F}_{p^r})) \cong (\mathbb{F}_{p^r}^+)^m \rtimes S(p, 2m),$$

we can conclude that

$$Z(S(p, 2m+1)) \cap (\{\mathbf{0}\} \times S(p, 2m))$$

must be a subset of $Z(S(p, 2m))$, which we proved above to be

$$Z(S(p,2m)) = \{ \begin{pmatrix} \mathrm{Id}_m & D \\ 0_m & \mathrm{Id}_m \end{pmatrix} : D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix} \} \cong \mathbb{F}_{p^r}^+ \cong (\mathbb{Z}/p\mathbb{Z})^r (\text{for } m > 2).$$

Thus the center of $(\mathbb{F}_{p^r}^+)^m \rtimes (Antisym(m, p^r) \rtimes \mathrm{Up}_m(\mathbb{F}_{p^r})$ is a subset of

$$(\mathbb{F}_{p^r}^+)^m \rtimes \left\{ \begin{pmatrix} \mathrm{Id}_m & D \\ 0_m & \mathrm{Id}_m \end{pmatrix} : D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix} \right\} = \left\{ \begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & \mathrm{Id}_m & D \\ \mathbf{0} & 0_m & \mathrm{Id}_m \end{pmatrix} : \mathbf{x} \in \mathbb{F}_{p^r}^m, D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix} \right\}$$

Given

$$\begin{pmatrix} 1 & \mathbf{0} & \mathbf{y} \\ \mathbf{y}^T & A & AB \\ \mathbf{0} & 0_m & (A^{-1})^T \end{pmatrix} \in \mathrm{Syl}_p(O(2m+1, p^r)),$$

we have that

$$\begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & \mathrm{Id}_m & D \\ \mathbf{0} & 0_m & \mathrm{Id}_m \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & \mathbf{y} \\ \mathbf{y}^T & A & AB \\ \mathbf{0} & 0_m & (A^{-1})^T \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} & \mathbf{y} + \mathbf{x}(A^{-1})^T \\ \mathbf{x}^T + \mathbf{y}^T & A & \mathbf{x}^T y + AB + D(A^{-1})^T \\ \mathbf{0} & 0_m & (A^{-1})^T \end{pmatrix}$$

and

$$\begin{pmatrix} 1 & \mathbf{0} & \mathbf{y} \\ \mathbf{y}^T & A & AB \\ \mathbf{0} & 0_n & (A^{-1})^T \end{pmatrix} \begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & \mathrm{Id}_m & D \\ \mathbf{0} & 0_m & \mathrm{Id}_m \end{pmatrix} = \begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} + \mathbf{y} \\ \mathbf{y}^T + A\mathbf{x}^T & A & \mathbf{x}y^T + AD + AB \\ \mathbf{0} & 0_m & (A^{-1})^T \end{pmatrix}$$

So in order for

$$\begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & \mathrm{Id}_m & D \\ \mathbf{0} & 0_m & \mathrm{Id}_m \end{pmatrix}$$

to be in the center, we need $\mathbf{x}^T = A\mathbf{x}^T$, $\mathbf{x} = \mathbf{x}(A^{-1})^T$, and $AD = D(A^{-1})^T$ for all choices of A. By the work on even orthogonal groups, $AD = D(A^{-1})^T$ is satisfied if and only if

$$D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix}.$$

Note that the kth entry of $\mathbf{x} = A\mathbf{x}^T$ is given by $x_k + \sum_{i=k+1}^{m} x_i a_{k,i}$. In order for this to be equal to x_k for all $a_{k,i}$, must have $x_i = 0$ for all $i > 1$. So $\mathbf{x} = (x_1, 0, \cdots, 0)$. In this case $\mathbf{x} = \mathbf{x}(A^{-1})^T$ will be satisfied as well. Therefore the center is

$$Z(S(p, 2m+1)) = \left\{ \begin{pmatrix} 1 & \mathbf{0} & \mathbf{x} \\ \mathbf{x}^T & \mathrm{Id}_m & D \\ \mathbf{0} & 0_m & \mathrm{Id}_m \end{pmatrix} : \mathbf{x} = (x_1, 0, \cdots, 0), D = \begin{pmatrix} 0 & x & \mathbf{0} \\ -x & 0 & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & 0_{m-2} \end{pmatrix} \right\} \cong (\mathbb{F}_{p^r}^+)^2$$

□

Section 6.4 Calculation

The calculation that $H \in L_{\mathbf{b}}$ if and only if $\psi(\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1$ for all $\mathbf{d} \in (\mathbb{F}_{p^r}^{+})^{m(m-1)/2}$, where $\mathbf{hdh^T}$ is the vector in $(\mathbb{F}_{p^r}^{+})^{m(m-1)/2}$ corresponding to $HDH^T \in Sym(m, p^r)$ under the isomorphsim $Sym(m, p^r) \cong (\mathbb{F}_{p^r}^{+})^{m(m-1)/2}$:

Remark 13. In all of the following, we view $\psi_{(b_j)}$ as a map on

$$\begin{cases} \Delta \cong Antisym(m, p^r) \cong \mathbb{F}_{p^r}^{m(m-1)/2} & p \neq 2 \\ \Delta \cong Antisym_0(m, 2^r) \cong \mathbb{F}_{2^r}^{m(m-1)/2} & p = 2 \end{cases}.$$

So $\psi_{(b_j)}(D, \mathrm{Id}) = \psi_{(b_j)}(D) = \psi(\mathbf{b} \cdot \mathbf{d})$, where $\mathbf{b} = (b_j)$ and $\mathbf{d}$ is the vector corresponding to the matrix D.

The action of $h \in \mathrm{Syl}_p(\Omega^+(2m, p^r))$ on $\widehat{\Delta}$ is given by

$${}^{h}\psi(D, \mathrm{Id}_m) = \psi(h^{-1}(D, \mathrm{Id}_m)h).$$

So for $h = (0_m, H^{-1})$, the action on $\psi_{(b_j)}$ is given by

$${}^{h}\psi_{(b_j)}(D, \mathrm{Id}_m) = \psi_{(b_j)}((0_m, H)(D, \mathrm{Id}_m)(0_m, H^{-1})).$$

So $(0_m, H^{-1}) \in L_s$ if and only if

$$\psi_{(b_j)}((0_m, H)(D, \mathrm{Id}_m)(0_m, H^{-1})) = \psi_{(b_j)}(D, \mathrm{Id}_m)$$

for all

$$\mathbf{d} \in (\mathbb{F}_{p^r}^{+})^{m(m-1)/2} \text{ corresponding to } D \in \begin{cases} Antisym(m, p^r) & p \neq 2 \\ Antisym_0(m, 2^r) & p = 2 \end{cases}.$$

Let $\mathbf{hdh^T}$ be the vector corresponding to HDH^T. Then since

$$\psi_{(b_j)}((0_m, H)(D, \mathrm{Id}_m)(0_m, H^{-1})) = \psi(\mathbf{b} \cdot \mathbf{hdh^T}),$$

and

$$\psi_{(b_j)}(D, \mathrm{Id}_m) = \psi(\mathbf{b} \cdot \mathbf{d}).$$

we get that $(0_m, H^{-1}) \in L_s$ if and only if

$$\psi(\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1$$

for all

$$\mathbf{d} \in (\mathbb{F}_{p^r})^{m(m-1)/2} \text{ corresponding to } D \in \begin{cases} Antisym(m, p^r) & p \neq 2 \\ Antisym_0(m, 2^r) & p = 2 \end{cases}.$$

Proposition 6.20

Proposition (6.20)**.** For any prime p,

$$\min_{\mathbf{b} \in (\mathbb{F}_{p^r}^+)^{m(m-1)/2},\ b_1 \neq 0} \dim(\theta_{\mathbf{b},1}) = p^{2r(m-2)}.$$

This minimum is achieved when $\mathbf{b} = (b, 0, \ldots, 0)$ with $b \neq 0$.

Proof. Write

$$H = \begin{pmatrix} 1 & h_{1,2} & h_{1,3} & \cdots & h_{1,n} \\ 0 & 1 & h_{2,3} & \cdots & h_{2,m} \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & h_{m-1,m} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}, \qquad D = \begin{pmatrix} 0 & d_{1,2} & d_{1,3} & \cdots & d_{1,m} \\ -d_{1,2} & 0 & d_{2,3} & \cdots & d_{2,m} \\ \vdots & & \ddots & & \vdots \\ -d_{1,m-1} & -d_{2,m-1} & \cdots & 0 & d_{m-1,m} \\ -d_{1,m} & -d_{2,m} & \cdots & -d_{m-1,m} & 0 \end{pmatrix}.$$

We will prove the proposition in two steps:

Step 1: Proving that for any $\mathbf{s = (b_i), b_1 \neq 0, |L_s| \leq |\mathbb{F}_{p^r}| \cdot |U_{m-2}(\mathbb{F}_{p^r})| = p^{2r(m-2)}}$.

In all the following, in characteristic 2, the negatives will go away, but the argument is the same.

Calculation 3. For $j_0 > 2$, choose $d_{i,j} = 0$ except for $d_{1,j_0} = -d_{j_0,1}$.

Then

$$\mathbf{b}\cdot(\mathbf{hdh^T}-\mathbf{d}) = \sum_{i=2}^{j_0-1} h_{i,j_0} d_{1,j_0} B_{1,i} = d_{1,j_0}\left(\sum_{i=2}^{j_0-1} h_{i,j_0} B_{1,i}\right)$$

If $\sum_{i=2}^{j_0-1} h_{i,j_0} B_{1,i} \neq 0$, then as we run through all the values for d_{1,j_0}, we will get that $\mathbf{b}\cdot(\mathbf{hdh^T}-\mathbf{d})$ runs through all the values of $\mathbb{F}_{p^r}$. And since ψ is non-trivial, this means that $\psi(\mathbf{b}\cdot(\mathbf{hdh^T}-\mathbf{d}))$ cannot always equal 1. This is a contradiction. So we must have

$$\sum_{i=2}^{j_0-1} h_{i,j_0} B_{1,i} = 0$$

for all choices of $j_0 > 2$. Recall that $B_{1,2} = b_1 \neq 0$. So, for all $j_0 > 2$, given h_{i,j_0} for $i > 2$, the above dictates h_{2,j_0}: If we know h_{i,j_0} for $i > 1$, then we have

$$\sum_{i=2}^{j_0-1} h_{i,j_0} B_{1,i} = 0 \Rightarrow h_{2,j_0} = \frac{-1}{B_{1,2}} \sum_{i=3}^{j_0-1} h_{i,j_0} B_{1,i}.$$

(In particular, note $h_{2,3} = 0$.) For $3 \leq k \leq n$, if $B_{1,k} \neq 0$, then for all $j_0 > 2$, given h_{i,j_0} for $i \neq 1, k$, the above dictates h_{k,j_0}: If we know h_{i,j_0} for $i \neq 1, k$, then we have

$$\sum_{i=2}^{j_0-1} h_{i,j_0} B_{1,i} = 0 \Rightarrow h_{k,j_0} = \frac{-1}{B_{1,k}} \sum_{i=2, i\neq k}^{j_0-1} h_{i,j_0} B_{1,i}.$$

Calculation 4. Now for $j_0 > 2$, choose $d_{i,j} = 0$ except for $d_{2,j_0} = -d_{j_0,2}$.

Then

$$\mathbf{b}\cdot(\mathbf{hdh^T}-\mathbf{d}) = d_{2,j_0}\left(-B_{1,2}h_{1,j_0} + \sum_{i=2}^{j_0} B_{1,i}h_{i,j_0}h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,i}h_{i,j_0}\right)$$

By the same reasoning as before, we must have

$$-B_{1,2}h_{1,j_0} + \sum_{i=2}^{j_0} B_{1,i}h_{i,j_0}h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,i}h_{i,j_0} = 0$$

for all choices of $j_0 > 2$. Recall that $B_{1,2} = b_1 \neq 0$. So for all $j_0 > 2$, given h_{i,j_0} for $i > 2$, the above dictates h_{1,j_0}: If we know $h_{1,2}$ and h_{i,j_0} for $i > 1$, then we have

$$-B_{1,2}h_{1,j_0}+\sum_{i=2}^{j_0} B_{1,i}h_{i,j_0}h_{1,2}+\sum_{k=3}^{j_0-1} B_{2,i}h_{i,j_0} = 0 \Rightarrow h_{1,j_0} = \frac{1}{B_{1,2}}\left(\sum_{i=2}^{j_0} B_{1,i}h_{i,j_0}h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,k}h_{i,j_0}\right)$$

Thus we can conclude that for all $s = (b_i)$ with $b_1 \neq 0$,

$$|L_s| \leq |\{H : H_{2,j} \text{ fixed }, \forall j > 2, H_{1,j} \text{ fixed }, \forall j > 2\}| = |\mathbb{F}_{p^r}| \cdot |U_{m-2}(\mathbb{F}_{p^r})| = p^{r[(m-2)(m-3)/2+1]}.$$

Step 2: Exhibiting that the max is achieved when $\mathbf{s} = (\mathbf{b}, \mathbf{0}, \cdots, \mathbf{0})$ with $\mathbf{b} \neq \mathbf{0}$. Let B be the matrix corresponding to $s = (b, 0, \cdots, 0)$. So since the only nonzero entry of B is $B_{1,2} = b$, we have that

$$\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = b(HDH^T - D)_{1,2} = b\left([\sum_{l=2}^{n}[h_{2,l}(\sum_{k=1}^{l} d_{k,l}h_{1,k} - \sum_{k=l+1}^{m-1} d_{l,k}h_{1,k})]] - d_{1,2}\right).$$

By the first calculation above, we have that for $j_0 > 2$,

$$h_{2,j_0} = \frac{-1}{B_{1,2}} \sum_{i=3}^{j_0-1} h_{i,j_0}B_{1,i} = 0.$$

So we have

$$\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = b\left([\sum_{k=1}^{2} d_{k,2}h_{1,k} - \sum_{k=3}^{m-1} d_{2,k}h_{1,k}] - d_{1,2}\right)$$

By the second calculation above, we have that for $j_0 > 2$,

$$\begin{aligned} h_{1,j_0} &= \frac{1}{B_{1,2}}\left(\sum_{i=2}^{j_0} B_{1,i}h_{i,j_0}h_{1,2} + \sum_{i=3}^{j_0-1} B_{2,k}h_{i,j_0}\right) \\ &= h_{2,j_0}h_{1,2} \\ &= 0 \end{aligned}$$

So we have

$$\begin{aligned}\mathbf{b}\cdot(\mathbf{hdh^T}-\mathbf{d}) &= b\left([\sum_{k=1}^{2} d_{k,2}h_{1,k}-]-d_{1,2}\right)\\ &= b(d_{1,2}h_{1,1}+d_{2,2}h_{1,2}-d_{1,2})\\ &= 0 \text{ since } h_{1,1}=0, d_{2,2}=0\end{aligned}$$

Thus we have shown that $(0_m, H^{-1}) \in L_s$ if and only if $h_{2,j}=0, \forall j>2$ and $h_{1,j}=0, \forall j>2$. Therefore,

$$L_s = \{(0_m, H^{-1}) : H_{1,j}=0, \forall j>2, H_{2,j}=0, \forall j>2\}.$$

So $|L_s| = |\mathbb{F}_{p^r}|\cdot|U_{m-2}(\mathbb{F}_{p^r})| = p^{r[(m-2)(m-3)/2+1]}$.

□

Proposition 6.21

Proposition (6.21)**.** For $p \neq 2$,

$$\min_{(\mathbf{a},\mathbf{b})\in(\mathbb{F}_{p^r}^{+})^{m+m(m-1)/2},\ b_1\neq 0} \dim(\theta_{(\mathbf{a},\mathbf{b}),1}) = p^{r(m-1)(m-2)}.$$

This minimum is achieved when $\mathbf{a}=\mathbf{0}, \mathbf{b}=(b_1,0,\ldots,0)$ with $b_1\neq 0$. Similarly,

$$\min_{(\mathbf{a},\mathbf{b})\in(\mathbb{F}_{p^r}^{+})^{m+m(m-1)/2},\ a_1\neq 0} \dim(\theta_{(\mathbf{a},\mathbf{b}),1}) = p^{r(m-1)}.$$

This minimum is achieved when $\mathbf{a}=(a_1,0,\ldots,0), \mathbf{b}=\mathbf{0}$ with $a_1\neq 0$.

Proof. **Case 1: $\mathbf{b_1}\neq\mathbf{0}$**

If we take $\mathbf{x}=0$, then $\psi(\mathbf{a}\cdot(\mathbf{x}H^T-\mathbf{x}))+\mathbf{b}\cdot(\mathbf{hdh^T}-\mathbf{d}))=1$ reduces to the condition for $\Omega^+(2m,p^r)$. So $L_{(\mathbf{a},\mathbf{b})}$ must be a subset of the $L_{\mathbf{b}}$ calculated in Proposition 6.20. Thus

$$|L_s| \leq |\{H : H_{2,j} \text{ fixed }, \forall j>2, H_{1,j} \text{ fixed }, \forall j>2\}| = p^{r[(m-2)(m-3)/2+1]}.$$

If $b_i = 0$ for $i \neq 1$, then we get

$$L_s \subset \{H \in \mathrm{Up}_m(\mathbb{F}_{p^r}) : H_{1,j} = 0, \forall j \neq 2, H_{2,j} = 0, \forall j > 2\}.$$

Given H of this form, we have $\mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = 0$. Then for $\mathbf{a} = 0$,

$$\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x}) + \mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d}) = 0.$$

So for $(0, \cdots, 0, b_1, 0, \cdots, 0)$,

$$L_s = \{H \in \mathrm{Up}_m(\mathbb{F}_{p^r}) : H_{1,j} = 0, \forall j \neq 2, H_{2,j} = 0, \forall j > 2\}.$$

Case 1: $\mathbf{a_1} \neq \mathbf{0}$ If we take $\mathbf{d} = \mathbf{0}$ then $\psi(\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x}) + \mathbf{b} \cdot (\mathbf{hdh^T} - \mathbf{d})) = 1$ reduces to $\psi(\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x})) = 1$. Write

$$H = \begin{pmatrix} 1 & h_{1,2} & h_{1,3} & \cdots & h_{1,m} \\ 0 & 1 & h_{2,3} & \cdots & h_{2,m} \\ & & \ddots & & \vdots \\ 0 & 0 & \cdots & 1 & h_{m-1,m} \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

Then

$$\mathbf{x}H^T = (x_1, \cdots, x_m) \begin{pmatrix} 1 & 0 & & \cdots & 0 \\ h_{1,2} & 1 & 0 & \cdots & 0 \\ h_{1,3} & h_{2,3} & 1 & & 0 \\ \vdots & & \ddots & \ddots & \vdots \\ h_{1,m} & h_{2,m} & \cdots & h_{m-1,m} & 1 \end{pmatrix}$$
$$= (\sum_{k=1}^{m} x_k h_{1,k}, \cdots, x_{m-1} + x_m h_{m-1,m}, x_m)$$

So

$$\mathbf{x}H^T - \mathbf{x} = (\sum_{k=2}^{m} x_k h_{1,k}, \cdots, x_m h_{m-1,m}, 0).$$

Thus

$$\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x}) = \sum_{k=1}^{m-1} a_k \cdot (\sum_{j=k+1}^{m} x_j h_{k,j})$$

Calculation. For $j_0 > 1$, $\mathbf{x} = (x_i)$ with $x_i = 0$ except for x_{j_0}.

Then we get

$$\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x}) = \sum_{k=1}^{j_0-1} a_k \cdot x_{j_0} h_{k,j_0} = x_{j_0} \left(\sum_{k=1}^{j_0-1} a_k h_{k,j_0} \right)$$

So for all $j_0 > 1$, we must have

$$\sum_{k=1}^{j_0-1} a_k h_{k,j_0} = 0.$$

So if $a_1 \neq 0$, given h_{i,j_0} for $i \neq 1, k$, the above dictates h_{1,j_0}:

$$h_{1,j_0} = \frac{-1}{a_1} \sum_{k=2}^{j_0-1} a_k h_{k,j_0}.$$

Therefore,

$$|L_s| \leq |\{H : H_{1,j} \text{ fixed } \forall j \neq 1\} = |\operatorname{Up}_{n-1}(\mathbb{F}_{p^r})| = p^{r(n-1)(n-2)/2}.$$

If $a_i = 0$ for $i \neq 0$, then we get from the calculation above that

$$h_{1,j_0} = \frac{-1}{a_1} \sum_{k=2}^{j_0-1} a_k h_{k,j_0} = 0.$$

So

$$\begin{aligned}\mathbf{a} \cdot (\mathbf{x}H^T - \mathbf{x}) &= \sum_{k=1}^{m-1} a_k \cdot (\sum_{j=k+1}^{m} x_j h_{k,j}) \\ &= a_1 \cdot (\sum_{j=2}^{m} x_j h_{1,j}), \qquad \text{since } a_i = 0, i > 1\end{aligned}$$

$$= 0 \qquad \text{since } h_{1,j} = 0, j > 1$$

So we get that for $s = (a_1, 0, \cdots, 0)$ with $a_1 \neq 0$,

$$L_s = \{H : H_{1,j} = 0, \forall j \neq 1\}.$$

□

Lemma 7.3

Lemma (7.3)**.** Let σ_i^j be the permutation which permutes the ith set of l blocks of size l^{j-1}. Then

$$\langle \{\sigma_i^j\}_{1 \leq j \leq \mu_l(n), 1 \leq i \leq \lfloor \frac{n}{l^j} \rfloor} \rangle \in \mathrm{Syl}_l(S_n).$$

Let $P_l(S_n)$ denote this particular Sylow l-subgroup of S_n.

Proof. [2] Let $n' = \lfloor \frac{n}{l} \rfloor$, and let

$$\sigma_1^1 = (1, \cdots, l), \cdots, \sigma_{n'}^1 = ((n'-1)l + 1, \cdots, n'l).$$

Base Case: If $n' = 1$, then $n = l + k$ for $k < l$. Thus the only factor of $n!$ divisible by l is l, so we have $|S_n|_l = l$, and $P_l(S_n) = (\mathbb{Z}/l\mathbb{Z}) \in \mathrm{Syl}_l(S_n)$ (generated by $\sigma_1^1 = (1, \cdots, l)$).

Induction Step:

Let $D \cong (\mathbb{Z}/l\mathbb{Z})^{n'}$. Then $S_{n'}$ acts on D by permuting the σ_i^1. And $D \rtimes S_{n'}$ embeds into S_n. Write $n = ln' + *$ for $* < l$; then

$$\begin{aligned}
\nu_l(n!) &= \nu_l((ln' + *)!) \\
&= \nu_l((ln')!) \\
&= \sum_{i=1}^{ln'} \nu_l(i) \\
&= \sum_{i=1}^{n'} \nu_l(li)
\end{aligned}$$

[2]See [14], Corollary 4.2

$$= \sum_{i=1}^{n'} 1 + \sum_{i=1}^{n'} \nu_l(i)$$

$$= n' + \nu_l(n'!)$$

$$= \nu_l(|D|) + \nu_l(S_{n'})$$

Thus $D \rtimes S_{n'}$ embeds into S_n with index prime to l. Therefore, $P_l(S_n) \cong D \rtimes P_l(S_{n'}) \in \mathrm{Syl}_l(S_n)$.

Let $\mu_l(n)$ be the highest power of l such that $\lfloor \frac{n}{l^{\mu_l(n)}} \rfloor > 0$. Let

$$\sigma_1^2 = (1, l+1, \cdots, l(l-1)+1)$$

$$\cdots$$

$$\sigma^2_{\lfloor \frac{n}{l^2} \rfloor} = (l^2(\lfloor \frac{n}{l^2} \rfloor - 1) + 1, l^2(\lfloor \frac{n}{l^2} - 1) + l + 1), \cdots, l^2 \lfloor \frac{n}{l^2} \rfloor - l + 1)$$

$$\vdots$$

$$\sigma_1^{\mu_l(n)} = (1, l^{\mu_l(n)-1} + 1, \cdots, l^{\mu_l(n)-1}(l-1) + 1),$$

$$\cdots$$

$$\sigma^{\mu_l(n)}_{\lfloor \frac{n}{l^{\mu_l(n)}} \rfloor} = (l^{\mu_l(n)}(\lfloor \frac{n}{l^{\mu_l(n)}} \rfloor - 1) + 1, (l^{\mu_l(n)}(\lfloor \frac{n}{l^{\mu_l(n)}} \rfloor - 1) + l^{\mu_l(n)-1} + 1, \cdots, l^{\mu_l(n)} \lfloor \frac{n}{l^{\mu_l(n)}} \rfloor - l^{\mu_l(n)-1} + 1)$$

Then $P_l(S_n)$ is generated by $\{\sigma_i^j\}$. And for j_0 fixed $\{\sigma_i^{j_0}\}$ generates a subgroup of order $(\mathbb{Z}/l\mathbb{Z})^{\lfloor \frac{n}{l^{j_0}} \rfloor}$. σ_i^j permutes the ith set of l blocks of size l^{j-1}.

□