Forum of Mathematics, Sigma (2024), **Vol. 12**:e73 1–38
doi:10.1017/fms.2024.58

CAMBRIDGE UNIVERSITY PRESS

RESEARCH ARTICLE

Bounds on multiplicities of symmetric pairs of finite groups

Avraham Aizenbud[1] and Nir Avni[2]

[1]Faculty of Mathematics and Computer Science, Weizmann Institute of Science, Rehovot, Israel;
E-mail: aizenr@gmail.com (corresponding author), Url: https://www.wisdom.weizmann.ac.il/~aizenr/.
[2]Northwestern University, Evanston, IL, USA; E-mail: avni.nir@gmail.com.

Received: 27 August 2022; **Revised:** 9 April 2024; **Accepted:** 13 May 2024

2020 Mathematics Subject Classification: *Primary* – 20C15, 20G25, 43A85

Abstract

Let Γ be a finite group, let θ be an involution of Γ and let ρ be an irreducible complex representation of Γ. We bound $\dim\rho^{\Gamma^\theta}$ in terms of the smallest dimension of a faithful $\mathbb{F}_p$-representation of $\Gamma/\mathrm{Rad}_p(\Gamma)$, where p is any odd prime and $\mathrm{Rad}_p(\Gamma)$ is the maximal normal p-subgroup of Γ.

This implies, in particular, that if $\mathbf{G}$ is a group scheme over $\mathbb{Z}$ and θ is an involution of $\mathbf{G}$, then the multiplicity of any irreducible representation in $C^\infty\left(\mathbf{G}(\mathbb{Z}_p)/\mathbf{G}^\theta(\mathbb{Z}_p)\right)$ is bounded, uniformly in p.

Contents

1. Introduction

The main result of this paper is the following:

Theorem A see §10.1 below. *There is an increasing function* $C^{fin} : \mathbb{N} \to \mathbb{N}$ *such that, for any*

- *Odd prime* p,
- *Positive integer* d,
- *Finite group* Γ,
- *Normal* p*-subgroup* $N \lhd \Gamma$,
- *Embedding* $\Gamma/N \hookrightarrow GL_d(\mathbb{F}_p)$,
- *Involution* θ *of* Γ,
- *Irreducible representation* ρ *of* Γ,

the space ρ^{Γ^θ} *of* Γ^θ*-invariant vectors of* ρ *has dimension at most* $C^{fin}(d)$.

As a corollary, we deduce the following

Corollary B (see §10.1 below). *For every integer* d, *there is an integer* Λ *such that, if*

- p *is an odd prime,*
- F *is a purely ramified extension of* $\mathbb{Q}_p$,
- $\mathbf{G}$ *is a connected linear algebraic group over* F *whose reductive quotient has dimension at most* d,
- $K \subset \mathbf{G}(F)$ *is a compact subgroup,*
- θ *is an involution of* K,
- ρ *is an irreducible representation of* K,

then

$$\dim\left(\rho^{K^\theta}\right) \le \Lambda.$$

Remark 1.0.1. An important special case of Theorem A is where $\Gamma = \mathbf{G}(\mathbb{Z}/p^n)$, when $\mathbf{G}$ is a semisimple group scheme and θ is the restriction of an algebraic involution. The uniformity in the involution θ is not essential. The case $n = 1$ (and p varies) was proved in [AA19, She]. The case when p is fixed and n varies is much easier than the general result and can be directly deduced from Corollary 5.0.5.

1.1. Background and motivation

Let G be a group and let X be a transitive G-space. A basic problem of representation theory is to compute the multiplicities with which irreducible representations of G appear in the space of functions on X. This problem can be studied in several settings. In each setting, one considers a different kind of function space. For an example in the algebraic setting, if G is a connected reductive algebraic group over $\mathbb{C}$ and X is a spherical G-variety (this means that the Borel subgroup of G has an open orbit in X), then $\mathbb{C}[X]$ is multiplicity-free as a G-representation.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

Multiplicities for spherical G-varieties are of great interest in other settings. In non-algebraic settings, these multiplicities may be greater than one. One has the following conjecture:

Conjecture C. *Let* $\mathbf{G}$ *be a reductive group scheme over* $\mathbb{Z}$ *and let* $\mathbf{X}$ *be a* $\mathbf{G}$*-scheme. Assume that* $\mathbf{X}(\mathbb{C})$ *is a spherical* $\mathbf{G}(\mathbb{C})$*-space. Then there is an integer* C *such that, if* F *is a local field of large enough characteristic and* ρ *is a smooth, admissible and irreducible representation* $\mathbf{G}(F)$*, then*

$$\dim \mathrm{Hom}(\rho, C^{\infty}(\mathbf{X}(F))) < C.$$

One can study variants of this conjecture in various levels.

- The most basic level is when both F and ρ are fixed. This case was mostly done. See [vdB87, Del10, SV17].
- The next level is when F is fixed and C is required to be independent of ρ. The main known results in this level are for the archimedean case. See [vdB87, KO13, KS16, AGM16].
- The last level is the full conjecture where both F and ρ vary. Here, the only known cases are where the spherical spaces are multiplicity free (i.e., Gelfand pairs) and related situations. Although there are many known Gelfand pairs (see, for example, [GK75, Sha74, vD86, Fli91, BvD94, Nie06, Yak05, AGRS10, AGS08, OS08, AG09b, AG09a, AG10, AAG12, Zha10, JSZ10, JSZ11, AS12, AGJ09, AG12, SZ12, Aiz13, CS15, Car, Rub], and the reference therein), general spherical spaces are not multiplicity free.

Our motivation for Corollary B is the following strategy for proving Conjecture C:

1. Prove a variant of Conjecture C when F ranges over the collection of finite fields.
2. Deduce from (1) a variant of Conjecture C when F ranges over the collection of rings of integers in local fields.
3. Deduce Conjecture C from (2).

Step (1) was done in [AA19, She]. Corollary B implies Step (2) under certain conditions:

Corollary D (see §10.1 below). *Let* $\mathbf{G}$ *be a reductive group scheme over* $\mathbb{Z}$*, let* θ *be an involution of* $\mathbf{G}$ *and let* $\mathbf{X} = \mathbf{G}/\mathbf{G}^{\theta}$ *be the corresponding symmetric space. Then there is an integer* C *such that, for every odd prime* p *and every irreducible representation* ρ *of* $\mathbf{G}(\mathbb{Z}_p)$*,*

$$\dim \mathrm{Hom}(\rho, C^{\infty}(\mathbf{X}(\mathbb{Z}_p))) \leq C.$$

Remark 1.1.1. Originally, we were interested only in Corollary D. However, since our argument is inductive, it turns out to be easier to prove the more general Theorem A.

1.2. The Larsen–Pink theorem

A central ingredient in the proof of Theorem A is a theorem of [LP11] roughly stating that finite subgroups of $\mathrm{GL}_d(\mathbb{F}_p)$ are close to groups of $\mathbb{F}_p$-points of connected algebraic subgroups of GL_d. We use the Larsen–Pink theorem in several ways:

- The Larsen–Pink theorem attaches an algebraic group of GL_n to finite subgroups of $\mathrm{GL}_n(\mathbb{F}_p)$, and we prove Theorem A by induction on the dimension on this algebraic group. In particular, the Larsen–Pink theorem implies that the lengths of decreasing chains of perfect subgroups of $\mathrm{GL}_d(\mathbb{F}_p)$ are bounded when we vary p.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

- It allows us to reduce statements about finite groups with no normal p-subgroups to finite groups of Lie type. We use this to prove the main theorem for groups with trivial p-radical (see §8) and to get bounds on various cohomology groups in §6 and §7.

We discuss the Larsen–Pink theorem and its applications in §4.

1.3. Sketch of the proof of Theorem A

To prove Theorem A, we analyze the extreme cases $N = \Gamma$ and $N = 1$, and we use Clifford's theory to deduce the general cases from them. The main difficulty is to control the multiplicities when describing a representation using Clifford's theory.

We now sketch the proof of Theorem A. We first analyze the case of groups with odd order. The analysis is based on the simple observation that every element in such a group has a unique square root. We prove a Gelfand property (i.e., multiplicity one property) for symmetric pairs of such groups. In addition, we prove a necessary condition (related to conjectures of Lapid and Prasad [Gla18, Pra]) for a representation of a group G of odd order to be distinguished with respect to a symmetric subgroup of G. Finally, we show that the first cohomology of S_2 with coefficients in groups of odd order vanishes. We treat this case in §5.

Next, we analyze the case of a group with a trivial p-radical. Here, we prove a twisted version of the main theorem. Using the Larsen-Pink theorem, we reduce this case to the case of finite groups of Lie type, where we apply a similar reasoning as in [AA19, She]. We treat this case in §8 and Appendix A.

For the general case, we introduce the following invariant of a group Γ: $\overline{\mathrm{rd}}_p(\Gamma)$ is the smallest possible dimension of a connected reductive group $\mathbf{G}$ such that $\Gamma/\mathrm{Rad}_p(\Gamma) \subseteq \mathbf{G}(\mathbb{F}_p)$. Since, in the notations of Theorem A, $\overline{\mathrm{rd}}_p(\Gamma) \leq d^2$, it is enough to bound $\dim \rho^{\Gamma^\theta}$ in terms of $\overline{\mathrm{rd}}_p(\Gamma)$. This is done by induction on $\overline{\mathrm{rd}}_p(\Gamma)$. In the rest of the section, we describe the induction step.

Clifford theory implies that there is a group Δ satisfying $\mathrm{Rad}_p(\Gamma) < \Delta < \Gamma$ and an irreducible representation σ of Δ such that

- $\rho = Ind_\Delta^\Gamma(\sigma)$.
- $\sigma|_{\mathrm{Rad}_p(\Gamma)}$ is isotypic.

By Mackey's formula, the multiplicity $\dim \rho^{\Gamma^\theta}$ is a sum of multiplicities of σ in various transitive Δ-sets. A priori, the number of transitive Δ-sets that might contribute to $\dim \rho^{\Gamma^\theta}$ is $|\Gamma^\theta \backslash \Gamma/\Delta|$, which is unbounded. We use the Lapid–Prasad criterion to bound the number of subgroups of Δ whose contribution is nonzero by $|H^1(S_2, \Delta)|$, which we can bound.

To bound the individual contribution of a transitive Δ-set, we analyze two possibilities:

- $\mathrm{Rad}_p(\Delta) = \mathrm{Rad}_p(\Gamma)$.
  In this case, the bound on $H^2(\Delta/\mathrm{Rad}_p(\Delta), \mu_{p^\infty})$ implies that, for large p, the representation σ is a tensor product of a representation σ_1 that is trivial on $\mathrm{Rad}_p(\Delta)$ and a representation σ_2 that is irreducible when restricted to $\mathrm{Rad}_p(\Delta)$. The multiplicity of σ_2 is at most one since $\mathrm{Rad}_p(\Delta)$ has odd order. The bound on the multiplicity σ_1 follows from the analysis of the case with trivial p-radical mentioned above. At this point of the argument, we need to bound twisted multiplicities of representations of $\Delta/\mathrm{Rad}_p(\Delta)$ rather than usual multiplicities. The reason is that the one-dimensional multiplicity space obtained for $\mathrm{Rad}_p(\Delta)$ manifests itself as a twist here.
- $\mathrm{Rad}_p(\Delta) \neq \mathrm{Rad}_p(\Gamma)$.
  In this case, the Larsen–Pink Theorem implies that there is subgroup of bounded index $\Delta^\circ \lhd \Delta$ such that $\overline{\mathrm{rd}}(\Delta^\circ) < \overline{\mathrm{rd}}(\Gamma)$. We deduce the required bound from the induction assumption.

1.4. Complication related to the action of S_2

The sketch above overlooks one technical point. Namely, although the Larsen–Pink theorem was proved for groups, we need it for symmetric pairs or, equivalently, in the S_2-equivariant setting. One way around

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

this difficulty is to embed Γ into $\Gamma \times \Gamma$ using the graph of θ. Under this embedding, θ becomes the flip $(x, y) \mapsto (y, x)$, which clearly extends to the ambient algebraic group. This way is implemented in Lemma 2.2.3 below. The drawback of this method is that it doubles the dimension of the ambient algebraic group, so it is not suitable for induction. So, in some parts of the argument, we use a different method: We use an iterative procedure, based on the Larsen-Pink Theorem that allows us to replace (without increasing the value of $\overline{\mathrm{rd}}_p$) a subgroup of bounded index with a smaller S_2-invariant subgroup, also of bounded index. We implement this procedure in Lemma 4.1.1 below. This procedure is very costly in terms of the bounds on the indexes, and it is one of the main reasons why our bound on the multiplicities is very large.

1.5. Limitation of our result

- Our bounds on the multiplicities are given in terms of an embedding into a group of $\mathbb{F}_p$-points rather than a group of $\overline{\mathbb{F}_p}$-points. Therefore, we do not bound the multiplicity of symmetric pairs with $G = \mathbf{G}(O_F)$ when F ranges over all extensions of a given local non-archimedean field (of course, if the degree $[O_F/\mathfrak{m}_F : \mathbb{F}_p]$ is fixed, we do get uniform bounds). The reason is that, unlike $\mathbf{G}(\mathbb{F}_p)$, the group $\mathbf{G}(\overline{\mathbb{F}_p})$ has decreasing chains of perfect subgroups of arbitrary length. For this reason, we do not conjecture that Theorem A holds if we replace $\mathbb{F}_p$ with $\overline{\mathbb{F}_p}$.
- The bounds on the multiplicities we obtain are extremely large. We did not try to optimize the bounds since our argument cannot prove any reasonable bounds.
- In the general case, we only bound usual multiplicities and not twisted ones. The reason is that our analysis of odd order groups does not work well in the twisted case. We do not expect any problems with the twisted Gelfand property, and we also think that it will be easy to obtain a criterion for twisted distinction. However, this criterion will be different from the untwisted, so the number of symmetric subgroups of Δ contributing to the multiplicity will not be the size of any homology but rather some other number that we do not know how to bound. It would be interesting to resolve the twisted case, especially since we use bounds on twisted multiplicities in the case of trivial p-radical in order to bound the usual multiplicities in the general case.

1.6. Structure of the paper

In §2, we fix notations and formulate our main result. See Theorem 2.3.1. In particular, we introduce an invariant $\overline{\mathrm{rd}}_p$ to measure ‘dimension’ of a finite group. See Definition 2.2.1.

In §3, we recall some group theoretic facts.

In §4, we quote the Larsen–Pink Theorem and deduce two corollaries that we will use in the paper: Corollary 4.0.13 and Corollary 4.1.2.

In §5, we treat the case of groups of odd order. In this case, we prove a stronger form of the main result along with some other results for this special case. See Lemma 5.0.2 and Corollary 5.0.5.

In §6, we bound the size of the first cohomology group of S_2 with coefficients in a finite group Γ in terms of $\overline{\mathrm{rd}}_p(\Gamma)$. See Corollary 6.0.6.

In §7, we prove a vanishing result for $H^2(\Gamma, \mathbb{Z}/p^n)$, where Γ is a finite group, assuming p is large enough with respect to $\overline{\mathrm{rd}}_p(\Gamma)$. See Proposition 7.0.2.

In §8, we prove a twisted version of the main result for the case of groups with trivial p-radical. See Corollary 8.0.5.

In §9, we recall some basic results of Clifford theory which are needed in our proof.

In §10, we prove our main result, Theorem 2.3.1. In §§10.1, we deduce Theorem A and Corollary B from Theorem 2.3.1.

In Appendix A, we prove a twisted version of the main result for finite groups of Lie type. The argument is an adaptation (to the twisted case) of [She].

In Appendix B, we construct a family of symmetric pairs of reductive groups that includes all symmetric pairs of reductive groups of a given dimension over all finite fields; see Lemma 3.2.1. We use this construction in §4 in order to express the bounds given by the Larsen–Pink theorem in terms of $\overline{\mathrm{rd}}_p$.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

2. Conventions, notations and reformulation of the main result

2.1. Conventions

- By a finite symmetric pair, we will mean a pair (Γ, θ), where Γ is a finite group and θ is a (possibly trivial) involution of Γ. For a symmetric pair (Γ, θ), we get a symmetric subgroup $\Gamma^\theta \subset \Gamma$, a symmetric space Γ/Γ^θ and an action of S_2 on Γ.
- For a group G, we denote the derived subgroup of G by G' and the center of G by $Z(G)$. If $\mathbf{G}$ is an algebraic group, we denote the connected component of identity in $\mathbf{G}$ by $\mathbf{G}^\circ$.
- All schemes considered in this paper are assumed to be of finite type over Noetherian base schemes.
- By a simple algebraic group, we mean a connected algebraic group whose Lie algebra is simple.
- Throughout the paper, we will formulate and prove several lemmas that assert the existence of increasing functions $\mathbb{N} \to \mathbb{N}$ satisfying certain conditions. Each of those lemmas will give the corresponding function a distinct notation. It is implied that, after each such lemma, we fix such a function and use that notation to refer to it. The choices of such functions are not unique, but the only effect of a different choice is different bounds. Since we just claim the existence of bounds, this is irrelevant to us.
- We will usually use capital boldface letters to denote varieties, capital calligraphic letters to denote schemes, and capital gothic letters to denote sheaves.

2.2. Notations

We will use the following invariants of a finite group.

Definition 2.2.1. Let Γ be a finite group and p be a prime.

1. Define the p-reductivity dimension $\mathrm{rd}_p(\Gamma)$ of Γ to be the minimal n such that there exist a connected n-dimensional reductive algebraic group $\mathbf{G}$ and an embedding $\Gamma \hookrightarrow \mathbf{G}(\mathbb{F}_p)$.
2. Define the reduced p-reductivity dimension $\overline{\mathrm{rd}}_p(\Gamma)$ by

$$\overline{\mathrm{rd}}_p(\Gamma) := \mathrm{rd}_p(\Gamma/\mathrm{Rad}_p(\Gamma)),$$

where $\mathrm{Rad}_p(\Gamma)$ is the maximal normal p-subgroup of Γ.

Definition 2.2.2. Let (Γ, θ) be a finite symmetric pair and let p be a prime.

1. Define the p-reductivity dimension $\mathrm{rd}_p(\Gamma, \theta)$ of (Γ, θ) to be the minimal n such that there exist an n-dimensional reductive algebraic group $\mathbf{G}$, an involution t of $\mathbf{G}$ and an embedding $i : \Gamma \to \mathbf{G}(\mathbb{F}_p)$ such that $i(\theta(\gamma)) = t(i(\gamma))$ for all $\gamma \in \Gamma$.
2. Define the reduced p-reductivity dimension $\overline{\mathrm{rd}}_p(\Gamma, \theta)$ by

$$\overline{\mathrm{rd}}_p(\Gamma, \theta) := \mathrm{rd}_p(\Gamma/\mathrm{Rad}_p(\Gamma), \bar{\theta}),$$

where $\bar{\theta}$ is the involution of $\Gamma/\mathrm{Rad}_p(\Gamma)$ induced by θ.

Lemma 2.2.3. *For any symmetric pair (Γ, θ) and every p,* $\mathrm{rd}_p(\Gamma, \theta) \leq 2\mathrm{rd}_p(\Gamma)$.

Proof. Let $i : \Gamma \hookrightarrow \mathbf{G}(\mathbb{F}_p)$ with $\mathbf{G}$ reductive and $\dim \mathbf{G} = \mathrm{rd}_p(\Gamma)$. Let $\mathbf{H} = \mathbf{G} \times \mathbf{G}$, let $t : \mathbf{H} \to \mathbf{H}$ be the flip $\theta(x, y) = (y, x)$ and let $j : \Gamma \hookrightarrow \mathbf{H}(\mathbb{F}_p)$ be $j(\gamma) = (i(\gamma), i(\theta(\gamma)))$. The triple $(\mathbf{H}, t, j)$ gives an equivariant embedding as required. ◻

Next, we introduce some notations relating to multiplicities.

Notation 2.2.4. Let Γ be a finite group.

- We denote the set of (isomorphism classes of) complex irreducible representations of Γ by $\mathrm{Irr}(\Gamma)$.
- We denote the set of (one dimensional) characters of Γ by $\widehat{\Gamma}$.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

- Suppose that θ is an involution of Γ. Denote

$$\nu(\Gamma,\theta)=\max_{\rho\in\mathrm{Irr}(\Gamma)}\dim\rho^{\Gamma^{\theta}},$$

$$\nu(\Gamma)=\max_{\theta\text{ involution of }\Gamma}\nu(\Gamma,\theta),$$

$$\nu'_p(\Gamma)=\max_{\theta\text{ involution of }\Gamma}\ \max_{\substack{\rho\in\mathrm{Irr}(\Gamma)\text{ such that}\\ \rho|_{\mathrm{Rad}_p(\Gamma)}\text{ is isotypic}}}\dim\rho^{\Gamma^{\theta}},$$

$$\mu(\Gamma,\theta)=\max_{\rho\in\mathrm{Irr}(\Gamma),\ \chi\in\widehat{\Gamma^{\theta}}}\dim\rho^{\Gamma^{\theta},\chi},$$

and

$$\mu(\Gamma)=\max_{\theta\text{ involution of }\Gamma}\mu(\Gamma,\theta).$$

2.3. Reformulation of the main theorem

Using the notations above, Theorem A has the following reformulation:

Theorem 2.3.1 (main). *There is an increasing function $C:\mathbb{N}\to\mathbb{N}$ such that, for every prime $p>2$ and every finite group Γ,*

$$\nu(\Gamma)<C(\overline{\mathrm{rd}}_p(\Gamma)).$$

This theorem appears to be slightly weaker then Theorem A. We will deduce Theorem A from it in §10.1.

3. Preliminaries on finite groups and algebraic groups

In this section, we collect several properties of finite and algebraic groups.

3.1. Finite groups of Lie type

The following theorem is well known:

Theorem 3.1.1. *For any finite field F which is not one of $\mathbb{F}_2,\mathbb{F}_3,\mathbb{F}_4,\mathbb{F}_8,\mathbb{F}_9$ and for any connected, simply-connected, semi-simple algebraic group $\mathbf{G}$ defined over F, the following hold:*

1. $\mathbf{G}(F)$ *is generated by its unipotents.*
2. $H^2(\mathbf{G}(F),A)=1$, *for every trivial $\mathbf{G}(F)$-module A.*
3. $\mathbf{G}(F)$ *is perfect.*
4. $Z(\mathbf{G}(F))=Z(\mathbf{G})(F)$.
5. $|Z(\mathbf{G}(F))|\le 2^{\dim\mathbf{G}}$.

Remark 3.1.2. Claim (1) follows from [Ste68, Theorem 12.4], so Claim (2) follows from [Ste68, Remark 12.8(b)].

Claims (3) and (4) follow from Claim (1) and [Mar91, Theorem 1.5.6].

By Claim (4), $|Z(\mathbf{G}(F))|\le|Z(\mathbf{G}(\overline{F}))|$. Since both functions $\mathbf{G}\mapsto|Z(\mathbf{G}(\overline{F}))|$ and $\mathbf{G}\mapsto 2^{\dim\mathbf{G}}$ are multiplicative, it is enough to prove Claim (5) in the case $\mathbf{G}$ is simple. For the classical groups, this is a simple inspection; for the exceptional groups, use the fact that the size of the center is equal to the determinant of the Cartan matrix of the Dynkin diagram of $\mathbf{G}$.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

Corollary 3.1.3. *Let F be a finite field of characteristic greater than 3, let $\mathbf{G}$ be a connected reductive group over F and let $\phi : \widetilde{\mathbf{G}'} \to \mathbf{G}'$ be the universal cover of the derived subgroup $\mathbf{G}'$. Then $\phi\left(\widetilde{\mathbf{G}'}(F)\right) = \mathbf{G}(F)'$.*

Proof. The inclusion $\phi\left(\widetilde{\mathbf{G}'}(F)\right) \subseteq \mathbf{G}(F)'$ follows from 3.1.1(3). For the other direction, it is enough to show that a commutator of two elements of $\mathbf{G}(F)$ belongs to $\phi\left(\widetilde{\mathbf{G}'}(F)\right)$. Let $g_1, g_2 \in \mathbf{G}(F)$. Choose $z_1, z_2 \in Z\left(\mathbf{G}(\overline{F})\right)$ such that $g_1z_1, g_2z_2 \in \mathbf{G}'(\overline{F})$, and choose elements $h_1, h_2 \in \widetilde{\mathbf{G}'}(\overline{F})$ such that $\phi(h_1) = g_1z_1, \phi(h_2) = g_2z_2$. Since $\phi^{-1}(Z(\mathbf{G}')) = Z\left(\widetilde{\mathbf{G}'}\right)$, the element $[h_1, h_2] \in \widetilde{\mathbf{G}'}(\overline{F})$ is independent of the choices of z_i and h_i and hence is fixed by $\mathrm{Gal}(\overline{F}/F)$. Therefore, $[h_1, h_2] \in \widetilde{\mathbf{G}'}(F)$. Hence, $[g_1, g_2] = \phi([h_1, h_2]) \in \phi\left(\widetilde{\mathbf{G}'}(F)\right)$. □

Corollary 3.1.3 and Theorem 3.1.1(3) imply the following:

Corollary 3.1.4. *Let F be a finite field of characteristic greater than 3 and let $\mathbf{G}$ be a connected reductive group over F. Then $\mathbf{G}(F)'$ is perfect.*

Lemma 3.1.5. *Let $\phi : \tilde{\mathbf{G}} \to \mathbf{G}$ be an isogeny of algebraic groups defined over a finite field $\mathbb{F}_q$ and let $\mathbf{K}$ be the kernel of ϕ. Then*

$$\left[\mathbf{G}(\mathbb{F}_q) : \phi\left(\widetilde{\mathbf{G}}(\mathbb{F}_q)\right)\right] \le |\mathbf{K}(\overline{\mathbb{F}}_q)|.$$

Proof. From the long exact sequence of Galois cohomologies

$$\mathbf{K}(\mathbb{F}_q) \to \widetilde{\mathbf{G}}(\mathbb{F}_q) \to \mathbf{G}(\mathbb{F}_q) \to H^1(Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q), \mathbf{K}(\overline{\mathbb{F}}_q)) \to H^1(Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q), \widetilde{\mathbf{G}}(\overline{\mathbb{F}}_q)),$$

we get

$$\begin{aligned}\left[\mathbf{G}(\mathbb{F}_q) : \phi\left(\widetilde{\mathbf{G}}(\mathbb{F}_q)\right)\right] &= |Ker(H^1(Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q), K(\overline{\mathbb{F}}_q)) \to H^1(Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q), \widetilde{\mathbf{G}}(\mathbb{F}_q)))| \\ &\le |H^1(Gal(\overline{\mathbb{F}}_q/\mathbb{F}_q), K(\overline{\mathbb{F}}_q))| \le |K(\overline{\mathbb{F}}_q)|.\end{aligned}$$ □

Lemma 3.1.6. *For every connected reductive group $\mathbf{G}$ defined over a finite field F of characteristic larger than 3, we have*

$$[\mathbf{G}'(F) : \mathbf{G}(F)'] < 2^{\dim(\mathbf{G})}.$$

Proof. We can assume that $\mathbf{G}$ is semisimple. Let $\phi : \widetilde{\mathbf{G}} \to \mathbf{G}$ be the universal cover. By Theorem 3.1.1(5) and Lemma 3.1.5, $|coker\phi| \le 2^{\dim \mathbf{G}}$. The result follows from Corollary 3.1.3. □

Lemma 3.1.7. *Let Γ_i be simple nonabelian groups and let $\Gamma := \prod_{i=1}^n \Gamma_i$. Any normal subgroup Δ of Γ is of the form $\Delta = \prod_{i \in I} \Gamma_i$ for some index set $I \subset \{1, \dots, n\}$. The same holds when Γ_i are simple adjoint algebraic groups and Δ is a normal algebraic subgroup of Γ.*

Proof. Assume that Γ_i are simple nonabelian groups and identify Γ_i as a subgroup of Γ. Let $\pi_i : \Gamma \to \Gamma_i$ be the projection. If $\pi_i(\Delta) \neq 1$, then $[\Delta, \Gamma_i]$ is a nontrivial normal subgroup of Γ_i, so $\Gamma_i = [\Delta, \Gamma_i] \subset \Delta$. Thus, the lemma holds with $I = \{i \mid \pi_i(\Delta) \neq 1\}$.

The proof in the case where Γ_i are algebraic is similar. □

Corollary 3.1.8. *Let Γ_i and Γ be as in Lemma 3.1.7 and let $\theta : \Gamma \to \Gamma$ be an automorphism. Then there is a permutation $\sigma \in S_n$ such that $\theta(\Gamma_i) = \Gamma_{\sigma(i)}$.*

Corollary 3.1.9. *If $p > 3$ is a prime number and $\mathbf{G}$ is a connected semisimple adjoint group defined over $\mathbb{F}_p$, then any automorphism of $\mathbf{G}(\mathbb{F}_p)'$ extends to an algebraic automorphism of $\mathbf{G}$.*

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

For the proof, we will need the following:

Theorem 3.1.10 (easy direction of the classification of finite simple groups; cf. [GLS94, §1] and [Ste60, 3.2]). *For any two finite fields F_1, F_2 of characteristic greater than 3 and any two absolutely simple and adjoint algebraic groups $\mathbf{G}, \mathbf{H}$ defined over F_1, F_2 respectively,*

1. $\mathbf{G}(F_1)'$ *is simple.*
2. *If* $\mathbf{G}(F_1)' \simeq \mathbf{H}(F_2)'$, *then* $F_1 \simeq F_2$ *and* $\mathbf{G} \simeq \mathbf{H}$.
3. *Any isomorphism* $\mathbf{G}(F_1)' \to \mathbf{H}(F_2)'$ *is the composition of* $\phi : \mathbf{G}(F_1)' \to \mathbf{G}^{\phi}(F_2)'$ *and* $\psi : \mathbf{G}^{\phi}(F_2)' \to \mathbf{H}(F_2)$, *where* $\phi : F_1 \to F_2$ *is a field isomorphism,* $\mathbf{G}^{\phi} = \mathbf{G} \times_{\mathrm{Spec}(F_1)} \mathrm{Spec}(F_2)$ *and* ψ *is the restriction of an isomorphism* $\mathbf{G}^{\phi} \to \mathbf{H}$.

Proof of Corollary 3.1.9. Write $\mathbf{G} = \prod \mathbf{G}_i$ where $\mathbf{G}_i$ are simple (not necessarily absolutely simple) adjoint groups defined over $\mathbb{F}_p$. For each i, there is a finite field $\mathbb{F}_{q_i}$ and an absolutely simple adjoint group $\mathbf{S}_i$ defined over $\mathbb{F}_{q_i}$ such that $\mathbf{G}_i \cong (\mathbf{S}_i)_{\mathbb{F}_{q_i}/\mathbb{F}_p}$. We have $\mathbf{G}(\mathbb{F}_q)' = \prod \mathbf{S}_i(\mathbb{F}_{q_i})'$. By Theorem 3.1.10(1), the groups $\mathbf{S}_i(\mathbb{F}_{q_i})'$ are simple. By Corollary 3.1.8, there is a permutation σ such that $\theta(\mathbf{S}_i(\mathbb{F}_{q_i})') = \mathbf{S}_{\sigma(i)}(\mathbb{F}_{q_{\sigma(i)}})'$. The assertion now follows from Theorem 3.1.10(3). □

3.2. *A versal family of reductive groups*

In order to prove uniform results for all reductive groups of a bounded dimension over an arbitrary finite field, we will use the following lemma.

Lemma 3.2.1. *For any integer $n > 0$, there exist a scheme $\mathcal{S}_n$ of finite type, a smooth group scheme $\Phi_n : \mathcal{R}_n \to \mathcal{S}_n$ and an involution $\tau_n : \mathcal{R}_n \to \mathcal{R}_n$ over $\mathcal{S}_n$ such that the following hold:*

1. *For every finite field F and every $s \in \mathcal{S}_n(F)$, the group $(\mathcal{R}_n)_s$ is connected and reductive.*
2. *For every connected and reductive group $\mathbf{G}$ of dimension at most n over a finite field F and for any involution t of $\mathbf{G}$, there is $s \in \mathcal{S}_n(F)$ with*
$$(\mathbf{G}, t) \simeq ((\mathcal{R}_n)_s, (\tau_n)_s).$$
3. *For any root datum $\mathfrak{X}$, there is a subscheme $\mathcal{S}^{\mathfrak{X}} \subset \mathcal{S}_n$ such that, for any geometric point x of $\mathcal{S}_n$, the (absolute) root datum of $(\mathcal{R}_n)_x$ is $\mathfrak{X}$ if and only if x factors through $\mathcal{S}^{\mathfrak{X}}$. Moreover, $\mathcal{S}^{\mathfrak{X}}$ is a union of connected components of $\mathcal{S}_n$.*

We prove this lemma in Appendix B. The proof does not work for infinite fields, but we do have the following:

Lemma 3.2.2. *There is a function $C^{lin} : \mathbb{N} \to \mathbb{N}$ such that any reductive group $\mathbf{G}$ over an arbitrary field F has a faithful F-representation of dimension at most $C^{lin}(\dim \mathbf{G})$.*

4. A theorem of Larsen–Pink and its applications

A theorem of Larsen and Pink is central to our proof. In this section, we quote the theorem and extract two corollaries (Corollaries 4.0.13 and 4.1.2) from it.

Definition 4.0.1. Let $\mathcal{S}$ be a scheme and let $f : \mathcal{G} \to \mathcal{S}$ be a group scheme over $\mathbf{S}$.

1. A *family of subgroups* is a pair consisting of a map $\pi : \mathcal{T} \to \mathcal{S}$ and a $\mathcal{T}$-subgroup scheme $\mathcal{H} \subset \mathcal{G} \times_{\mathcal{S}} \mathcal{T}$. In this case, we write $\mathcal{H} \Subset_{\pi} \mathcal{G}$.
2. Suppose that $\mathcal{H} \Subset_{\pi} \mathcal{G}$, that k is a field, that $s \in \mathcal{S}(k)$ and that $\Gamma \subset \mathcal{G}_s(k)$ is a subgroup. We say that Γ *k-evades* $\mathcal{H}$ if, for every $t \in \pi^{-1}(s)(k)$, we have $\Gamma \not\subset \mathcal{H}_t(k)$.

Definition 4.0.2. Suppose Γ, Δ are subgroups of some group. We say that Γ is big in Δ if $[\Delta, \Delta] \subset \Gamma \subset \Delta$.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

The following is a restatement of [LP11, Theorem 0.5]:

Theorem 4.0.3. *Let $\mathcal{S}$ be a scheme and let $\mathcal{G} \to \mathcal{S}$ be a group scheme over $\mathcal{S}$ such that every geometric fiber is connected, simple and adjoint. There is a family of subgroups $\mathcal{H} \Subset_\pi \mathcal{G}$ such that, for every prime p, every $\overline{\mathbb{F}_p}$-point $s : \operatorname{Spec}(\overline{\mathbb{F}_p}) \to \mathcal{S}$, and every $\Gamma \subset \mathcal{G}_s(\overline{\mathbb{F}_p})$, if Γ $\overline{\mathbb{F}_p}$-evades $\mathcal{H}$, then there is a Frobenius map $\Phi : \mathcal{G}_s \to \mathcal{G}_s$ such that Γ is big in $\mathcal{G}_s(\overline{\mathbb{F}_p})^\Phi$.*

Recall that, for an algebraic group $\mathbf{G}$ defined over $\overline{\mathbb{F}_p}$, a Frobenius map of $\mathbf{G}$ is an automorphism $\Phi : \mathbf{G} \to \mathbf{G}$ for which some positive power Φ^n coincides with some a standard Frobenius.

Corollary 4.0.4. *Let $\mathcal{S}$ be a scheme and let $\mathcal{G} \to \mathcal{S}$ be a group scheme whose geometric fibers are connected, simple and adjoint. There is a family of subgroups $\mathcal{K} \Subset_\tau \mathcal{G}$ such that, for every prime power q, every $s \in \mathcal{S}(\mathbb{F}_q)$ and every $\Gamma \subset \mathcal{G}_s(\mathbb{F}_q)$, if Γ $\mathbb{F}_q$-evades $\mathcal{K}$, then there is a Frobenius map $\Phi : \mathcal{G}_s(\overline{\mathbb{F}_q}) \to \mathcal{G}_s(\overline{\mathbb{F}_q})$ such that Γ is big in $\mathcal{G}_s(\overline{\mathbb{F}_q})^\Phi$.*

For the proof of corollary 4.0.4, we use the following preparations:

Definition 4.0.5. Let $\mathcal{S}$ be a scheme. Fix a closed embedding $(\mathrm{GL}_n)_{\mathbf{S}} \hookrightarrow \mathbb{A}^N_{\mathcal{S}}$.

1. We say that a regular function $f : (\mathrm{GL}_n)_{\mathcal{S}} \to \mathbb{A}^1$ has degree at most δ if it is the restriction of a polynomial of degree at most δ on $\mathbb{A}^N_{\mathcal{S}}$.
2. We say that the degree of $f : (\mathrm{GL}_n)_{\mathcal{S}} \to \mathbb{A}^1$ is δ if its degree is at most δ and not at most $\delta - 1$.
3. Define the complexity of an $\mathcal{S}$-subgroup scheme $\mathcal{L} \subset (\mathrm{GL}_n)_{\mathcal{S}}$ to be the minimal m such that the polynomials of degree at most m in the ideal $I(\mathcal{L})$ generate $I(\mathcal{L})$.

Lemma 4.0.6. *For any two integers n and A, there is an integer B such that, for any field F, if $\mathbf{L} \subset (\mathrm{GL}_n)_F$ is an algebraic subgroup of complexity at most A, then $\mathbf{L}^\circ$ is of complexity at most B.*

Proof. For any integer B, the statement 'the complexity of the connected component of an algebraic group $\mathbf{L}$ is at most B' is a first-order statement on the coefficients of the polynomials defining $\mathbf{L} \subset (GL_n)_F$.

The result follows now by ultraproduct argument. □

Lemma 4.0.7. *Let $\mathcal{G} \to \mathcal{S}$ be a group scheme and let $\mathcal{H} \Subset_\pi \mathcal{G}$ be a family of subgroups.*

1. *For any integer $d \in \mathbb{N}$, there exists a family of subgroups $\mathcal{K} \Subset_\tau \mathcal{G}$ such that, for any geometric point s of $\mathcal{S}$ and any d geometric points $s_1, \dots, s_d$ of $\pi^{-1}(s)$, the group $\mathcal{H}_{s_1} \cap \cdots \cap \mathcal{H}_{s_d}$ is of the form $\mathcal{K}_t$, where t is a point over s (i.e., $\tau(t) = s$).*
2. *There exists a family of subgroups $\mathcal{P} \Subset_\phi \mathcal{G}$ such that, for any geometric point s of $\mathcal{S}$, any open subgroup of $\mathcal{G}_s$ is of the form $\mathcal{P}_t$, where t is a point over s.*

Proof. 1. Let $\mathcal{S}'$ be the domain of definition of π and let $\mathcal{G}_{\mathcal{S}'} := \mathcal{G} \times_{\mathcal{S}} \mathcal{S}'$. Define

$$\mathcal{K} := \mathcal{H} \times_{\mathcal{G}_{\mathcal{S}'}} \cdots \times_{\mathcal{G}_{\mathcal{S}'}} \mathcal{H}$$

and

$$\mathcal{S}'' := \mathcal{S}' \times_{\mathcal{S}} \cdots \times_{\mathcal{S}'} \mathcal{S}'$$

to be the d-fold fibered products. The natural maps $\mathcal{S}'' \to \mathcal{S}$ and $\mathcal{K} \to \mathcal{S}''$ give a subfamily as required.

2. After passing to a stratification of $\mathcal{S}$, we can assume that $\mathcal{G} \subset (\mathrm{GL}_n)_{\mathcal{S}}$ is closed. Fix a closed embedding $(\mathrm{GL}_n)_{\mathcal{S}} \hookrightarrow \mathbb{A}^N_{\mathcal{S}}$.

   Since $\mathcal{G} \to \mathcal{S}$ is of finite type, there is a bound D on the complexity of all subgroups $\mathcal{G}_s$, where s ranges over all geometric points of $\mathcal{S}$. By Lemma 4.0.6, there is a bound E on the complexity of all subgroups $(\mathcal{G}_s)^\circ$, where s ranges over all geometric points of $\mathcal{S}$. Since $\mathcal{G} \to \mathcal{S}$ is of finite type, there is a constant C such that, for any geometric point s of $\mathcal{S}$, the group $\mathcal{G}_s$ has at most C connected

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

components. We get that there is a constant M such that for any geometric point $s \in \mathcal{S}$, any open subgroup of $\mathcal{G}_s$ has complexity at most M.

There is a morphism $\mathcal{T} \to \mathcal{S}$ and a family of subgroups $\mathcal{P} \subset \mathcal{G}_{\mathcal{T}} \to \mathcal{T}$ such that the following holds: for every prime power q, every $s \in \mathcal{S}(\mathbb{F}_q)$ and every algebraic subgroup $\mathcal{P} \subset \mathcal{G}_s$ which is defined over $\mathbb{F}_q$ and has complexity at most M, we have that $\mathcal{P} = \mathcal{P}_t$, for some $t \in \mathcal{T}(\mathbb{F}_q)$. By the arguments above, this family satisfies the requirements. $\square$

Proof of Corollary 4.0.4. It is enough to construct $\mathcal{K}$ and prove that the claim holds for all but finitely many primes. Let $\pi : \mathcal{S}' \to \mathcal{S}$ and $\mathcal{H} \to \mathcal{S}'$ be as in Theorem 4.0.3 and let $d = \dim_{\mathcal{S}} \mathcal{G}$.

By Lemma 4.0.7, we have a family $\mathcal{K} \Subset_\tau \mathcal{G}$, with $\tau : \mathcal{T} \to \mathcal{S}$, such that, for any geometric point s of $\mathcal{S}$ and any d geometric points $s_1, \ldots, s_d$ of $\pi^{-1}(s)$, any open subgroup of $\mathcal{H}_{s_1} \cap \cdots \cap \mathcal{H}_{s_d}$ is of the form $\mathcal{K}_t$, where t is a point over s (i.e., $\tau(t) = s$). We show that such a family $\mathcal{K}$ satisfies the conclusion of the Corollary.

Let q be a prime power, $s \in \mathcal{S}(\mathbb{F}_q)$, and $\Gamma \subset \mathcal{G}_s(\mathbb{F}_q)$ that $\mathbb{F}_q$-evades $\mathcal{K}$. Let $F : \pi^{-1}(s) \to \pi^{-1}(s)$ be the geometric Frobenius. We first show that Γ $\overline{\mathbb{F}_q}$-evades $\mathcal{H}$. Assuming the contrary, there is $s' \in \pi^{-1}(s)(\overline{\mathbb{F}_q})$ such that $\Gamma \subset \mathcal{H}_{s'}(\overline{\mathbb{F}_q})$. For every finite subset $I \subset \mathbb{Z}$, denote $\mathbf{H}_I = \bigcap_{i \in I} \mathcal{H}_{F^i s'}$. There are $i_1, \ldots, i_d$ such that $\dim \mathbf{H}_{\{i_1,\ldots,i_d\}} = \min\{\dim \mathbf{H}_I \mid I \subset \mathbb{Z} \text{ finite}\}$. The group $\mathbf{H}^\circ_{\{i_1,\ldots,i_d\}}$ is invariant under the Frobenius, so it is defined over $\mathbb{F}_q$. It follows that the group $\Gamma\mathbf{H}^\circ_{\{i_1,\ldots,i_d\}}$ is also defined over $\mathbb{F}_q$. By the assumption on $\mathcal{K}$, we have $\Gamma\mathbf{H}^\circ_{\{i_1,\ldots,i_d\}} = \mathcal{K}_t$, for some $t \in \mathcal{T}(\mathbb{F}_q)$. This contradicts the assumption that Γ $\mathbb{F}_q$-evades $\mathcal{K}$.

The result now follows from Theorem 4.0.3. $\square$

Proposition 4.0.8. *There is a function $C_{LP0} : \mathbb{N} \to \mathbb{N}$ such that, if p is a prime number, $\mathbf{G}$ is a connected algebraic group over $\mathbb{F}_p$, $t : \mathbf{G} \to \mathbf{G}$ is an involution, and $\Gamma \subset \mathbf{G}(\mathbb{F}_p)$ is t-invariant, then there is a normal t-invariant subgroup $\Delta \triangleleft \Gamma$ of index at most $C_{LP0}(\dim(\mathbf{G}))$, a connected reductive group $\mathbf{H}$ defined over $\mathbb{F}_p$, an involution s of $\mathbf{H}$ and an S_2-equivariant homomorphism $\rho : \Delta \to \mathbf{H}(\mathbb{F}_p)$ such that:*

1. $\dim \mathbf{H} \le \dim \mathbf{G}$.
2. $\ker \rho$ *is a p-group.*
3. *If* $\dim \mathbf{H} = \dim \mathbf{G}$, *then* $\ker \rho = 1$.
4. $\rho(\Delta)$ *is big in* $\mathbf{H}(\mathbb{F}_p)$.

For the proof, we will need some preparations:

Lemma 4.0.9. *Let $p > 3$, let $\mathbf{H}$ be a connected semi-simple group over $\mathbb{F}_p$ and let $1 \to C \to E \to \mathbf{H}(\mathbb{F}_p)' \to 1$ be a finite central extension. Then there is a finite central extension $\mathbf{E}$ of $\mathbf{H}$ and an embedding $E \hookrightarrow \mathbf{E}(\mathbb{F}_p)$ such that the diagram*

$$\begin{tikzcd} E \arrow[r] \arrow[d, hook] & \mathbf{H}(\mathbb{F}_p)' \arrow[d, hook] \\ \mathbf{E}(\mathbb{F}_p) \arrow[r] & \mathbf{H}(\mathbb{F}_p) \end{tikzcd} \tag{1}$$

commutes. In addition,

1. *If σ is an automorphism of $\mathbf{H}$, τ is an automorphism of E and the map $E \to \mathbf{H}(\mathbb{F}_p)'$ is equivariant, then there is an automorphism of $\mathbf{E}$ such that the map $\mathbf{E} \to \mathbf{H}$ is equivariant.*
2. *If $|C|$ is prime to p, then $E \cap \mathbf{E}^\circ$ is big in $\mathbf{E}^\circ(\mathbb{F}_p)$.*

Proof. Let $\widetilde{\mathbf{H}}$ be the universal cover of $\mathbf{H}$. By Theorem 3.1.1, the universal central extension (or universal cover; cf. [Moo68, §1]) of $\mathbf{H}(\mathbb{F}_p)'$ is $\widetilde{\mathbf{H}}(\mathbb{F}_p)$. Denote the kernel of $\widetilde{\mathbf{H}}(\mathbb{F}_p) \to \mathbf{H}(\mathbb{F}_p)'$ by A and note that

$$A \subset Z(\widetilde{\mathbf{H}}(\mathbb{F}_p)) \overset{3.1.1(4)}{=} Z(\widetilde{\mathbf{H}})(\mathbb{F}_p).$$

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

The extension $1 \to C \to E \to \mathbf{H}(\mathbb{F}_p)' \to 1$ corresponds to a homomorphism $\alpha : A \to C$. In particular, $E = \widetilde{\mathbf{H}}(\mathbb{F}_p) \times C/\delta(A)$, where $\delta(g) = (\alpha(g), g^{-1})$.

Consider A and C as discrete algebraic groups. Let $\mathbf{C}$ be the zero-dimensional algebraic group

$$\mathbf{C} = \left(C \times Z(\widetilde{\mathbf{H}})\right)/\delta(A)$$

and let

$$\mathbf{E} = \left(C \times \widetilde{\mathbf{H}}\right)/\delta(A).$$

The short exact sequence $1 \to \mathbf{C} \to \mathbf{E} \to \mathbf{H} \to 1$ is a central extension, the map $E = \left(C \times \widetilde{\mathbf{H}}(\mathbb{F}_p)\right)/\delta(A) \to \mathbf{E}(\mathbb{F}_p)$ is injective and the diagram (1) commutes.

It remains to prove the additional claims. Claim (1) follows from the construction. For Claim (2), assume that $|C|$ is prime to p. By the construction, $\mathbf{E}^\circ = \widetilde{\mathbf{H}}/\ker(\alpha)$. It follows that $E \cap \mathbf{E}^\circ \supset \widetilde{\mathbf{H}}(\mathbb{F}_p)/\ker(\alpha)$, so the map $E \cap \mathbf{E}^\circ \to \mathbf{H}(\mathbb{F}_p)'$ is onto. Since the order of $Z(\widetilde{\mathbf{H}})(\overline{\mathbb{F}_p})$ is prime to p, the same is true for the size of $\mathbf{C}$ and the size of the kernel of $E \cap \mathbf{E}^\circ \to \mathbf{H}(\mathbb{F}_p)'$. Since the kernel of the surjection $E \cap \mathbf{E}^\circ \to \mathbf{H}(\mathbb{F}_p)'$ is prime to p, we have that the number of p-elements of $E \cap \mathbf{E}^\circ$ is equal to the number of p-elements of $\mathbf{H}(\mathbb{F}_p)'$. By the same reasoning applied to the surjection $\mathbf{E}^\circ(\mathbb{F}_p) \to \mathbf{H}(\mathbb{F}_p)'$, this is also the number of p-elements of $\mathbf{E}^\circ(\mathbb{F}_p)$. Hence, all p-elements in $\mathbf{E}^\circ(\mathbb{F}_p)$ are already in $E \cap \mathbf{E}^\circ$. By Theorem 3.1.1 and Corollary 3.1.3, $\mathbf{E}^\circ(\mathbb{F}_p)'$ is generated by its p-elements, and the second claim follows. □

The next lemma follows from [Mar91, Proposition 1.5.5, Theorem 1.5.6 (i)] and Theorem 3.1.1(1).

Lemma 4.0.10. *Let $p > 3$ and let $\mathbf{H}$ be a reductive group over $\mathbb{F}_p$. Then any $g \in \mathbf{H}(\mathbb{F}_p)$ that commutes with $\mathbf{H}(\mathbb{F}_p)'$ is central in $\mathbf{H}$.*

Proof of Proposition 4.0.8. For every n, let $(\mathcal{R}_n, \mathcal{S}_n, \tau_n)$ be the versal family of reductive groups with involutions from Lemma 3.2.1. By Lemma 3.2.1(3), there is a subscheme $\mathcal{S}_n^s \subset \mathcal{S}_n$ such that, for any geometric point x of $\mathcal{S}_n$, the group $(\mathcal{R}_n)_x$ is absolutely simple adjoint iff x factors through $\mathcal{S}_n^s$. Let $\mathcal{R}_n^s \subset \mathcal{R}_n$ be the preimage of $\mathcal{S}_n^s$.

Applying Corollary 4.0.4 to $\mathcal{R}_n^s \to \mathcal{S}_n^s$, we get a family of subgroups $\mathcal{K}_n \Subset \mathcal{R}_n^s$ parameterized by an $\mathcal{S}_n^s$-scheme $f : \mathcal{S}_n' \to \mathcal{S}_n^s$. Let $D(n)$ be the maximum of the number of connected components of a group of the form $(\mathcal{K}_n)_x \cap (\tau_n)_{f(x)}(\mathcal{K}_n)_x$, or of the form $(\mathcal{K}_n)_x$, where x is a geometric point of $\mathcal{S}_n'$.

We define three functions $C_{LP0}, C_{LP0}^{ss}, C_{LP0}^{adj} : \mathbb{N} \to \mathbb{N}$ by recursion. Set

$$C_{LP0}(1) = C_{LP0}^{ss}(1) = C_{LP0}^{adj}(1) = 1$$

and, for $n \geq 2$, set

$$C_{LP0}^{adj}(n) = \max\{(3^n + 2)^n, C_{LP0}(n-1)D(n)^n\}.$$

$$C_{LP0}^{ss}(n) = 2^n C_{LP0}^{adj}(n).$$

$$C_{LP0}(n) = 2^n C_{LP0}^{ss}(n).$$

Note that $C_{LP0}^{adj} \leq C_{LP0}^{ss} \leq C_{LP0}$. We will show that the proposition holds with this choice of C_{LP0}. The proof is by induction on $n := \dim \mathbf{G}$. The base of the induction, $n = 0$, is trivial. The induction step is divided to the following steps:

Step 1: The claim holds if $p \leq 3^n + 1$ with the bound C_{LP0} replaced by C_{LP0}^{adj}.

In this case, we can take $\Delta = 1$, using the bound $|\mathbf{G}(\mathbb{F}_p)| \leq (p+1)^{\dim \mathbf{G}}$ from [Nor87, Lemma 3.5].

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

Step 2: The claim holds if $\mathbf{G}$ is semisimple and adjoint, with the following improvements:

(a) The bound C_{LP0} is replaced by C_{LP0}^{adj}.

(b) Either $\mathbf{H}$ is semisimple and $Ker(\rho) = 1$, or there is a proper connected t-invariant subgroup $\mathbf{N} < \mathbf{G}$ such that $[\Gamma : \Gamma \cap \mathbf{N}(\mathbb{F}_p)] < D(n)$.

By Step 1, we can assume $p > 3^n + 1$. We have $\mathbf{G} = \mathbf{G}_1 \times \cdots \times \mathbf{G}_m$, where $\mathbf{G}_i$ are simple and adjoint. We denote the projection $\mathbf{G} \to \mathbf{G}_i$ by pr_i. Each $\mathbf{G}_i$ is a restriction of scalars from an absolutely simple (and adjoint) group: $\mathbf{G}_i = \mathrm{Res}_{\mathbb{F}_{q_i}/\mathbb{F}_p} \mathbf{S}_i$.

For any $i \in \{1, \ldots, m\}$, we will define a point $\sigma_i \in \mathcal{S}_n^s(\mathbb{F}_{q_i})$. By Corollary 3.1.8, for any i, we have $t(\mathbf{G}_i) = \mathbf{G}_j$, for some j. If $i \neq j$, we take $\sigma_i \in \mathcal{S}_n^s(\mathbb{F}_{q_i})$ to be such that $(\mathcal{R}_n)_{\sigma_i} \cong \mathbf{S}_i$. This is possible since $\dim(\mathbf{S}_i) \leq \dim(\mathbf{G}_i)$. If $i = j$, we take $\sigma_i = \sigma_j \in \mathcal{S}_n^s(\mathbb{F}_{q_i})$ to be such that $(\mathcal{R}_n)_{\sigma_i} \cong \mathbf{S}_i$ in an S_2-equivariant way.

In both cases, we identify $\mathbf{G}_i(\mathbb{F}_p)$, $\mathbf{S}_i(\mathbb{F}_{q_i})$, and $(\mathcal{R}_n)_{\sigma_i}(\mathbb{F}_{q_i})$. Given $\Gamma \subset \mathbf{G}(\mathbb{F}_p)$, there are two cases:

Case 1: For some i, $pr_i(\Gamma) \subset \mathbf{G}_i(\mathbb{F}_p)$ does not $\mathbb{F}_{q_i}$-evade $\mathcal{K}_n$.

For simplicity, we assume that $t(\mathbf{G}_i) = \mathbf{G}_i$; if $t(\mathbf{G}_i) = \mathbf{G}_j$, the proof is similar (and simpler). In this case, there is a point $x \in \mathcal{S}'(\mathbb{F}_{q_i})$ that lies over σ_i such that $pr_i(\Gamma) \subset (\mathcal{K}_n)_x(\mathbb{F}_{q_i})$. Denote $\mathbf{K} := \mathcal{K}_x$. By the definition of $D(n)$, we have $|\pi_0(\mathbf{K} \cap \mathbf{t}_{\sigma_i}(\mathbf{K}))| \leq D(n)$. Let $\mathbf{M} = \mathrm{Res}_{\mathbb{F}_{q_i}/\mathbb{F}_p}(\mathbf{K} \cap \mathbf{t}_{\sigma_i}(\mathbf{K}))$. We have $|\pi_0(\mathbf{M})| \leq D(n)^n$.

Using the identification $\mathbf{G}_i = \mathrm{Res}_{\mathbb{F}_{q_i}/\mathbb{F}_p} \mathbf{S}_i$, the group $\mathbf{M}$ is a subgroup of $\mathbf{G}_i$ and is defined over $\mathbb{F}_p$. Note that $pr_i(\Gamma) \subset \mathbf{M}(\mathbb{F}_p)$. Since $\dim(pr_i^{-1}(\mathbf{M})) < n$, the result now follows from the induction step applied to $pr_i^{-1}(\mathbf{M})^\circ$ and $\Gamma \cap pr_i^{-1}(\mathbf{M})^\circ(\mathbb{F}_p)$.

Case 2: For all i, $pr_i(\Gamma)$ $\mathbb{F}_{q_i}$-evades $\mathcal{K}_n$.

In this case, there are Frobenius maps $\Phi_i : \mathbf{S}_i(\overline{\mathbb{F}_{q_i}}) \to \mathbf{S}_i(\overline{\mathbb{F}_{q_i}})$ such that $pr_i(\Gamma)$ is big in $\mathbf{S}_i(\overline{\mathbb{F}_{q_i}})^{\Phi_i}$. Let $\Delta := \Gamma \cap \prod_i \left(\mathbf{S}_i(\overline{\mathbb{F}_{q_i}})^{\Phi_i}\right)'$. Since

$$\left[\mathbf{S}_i(\overline{\mathbb{F}_{q_i}})^{\Phi_i} : \left(\mathbf{S}_i(\overline{\mathbb{F}_{q_i}})^{\Phi_i}\right)'\right] \leq 2^{\dim \mathbf{S}_i},$$

we get

$$[\Gamma : \Delta] \leq 2^{\sum \dim \mathbf{S}_i} \leq 2^{\dim \mathbf{G}} \leq C_{LP0}^{adj}(n).$$

Since $\Delta \supset \Gamma'$, it follows that $pr_i(\Delta) = \left(\mathbf{S}_i(\overline{\mathbb{F}_{q_i}})^{\Phi_i}\right)'$, for all i. Since $\left(\mathbf{S}_i(\overline{\mathbb{F}_{q_i}})^{\Phi_i}\right)'$ are simple groups, Goursat's Lemma implies that there is a subset $I \subset [m]$ such that the projection $\Delta \to \prod_{i \in I} \left(\mathbf{S}_i(\overline{\mathbb{F}_{q_i}})^{\Phi_i}\right)'$ is an isomorphism. Since Δ is perfect and $\Delta \subset \Gamma$, it follows that $\Delta = \Gamma'$, and, in particular, $t(\Delta) = \Delta$.

By [Ste68, 11.6], there is a connected semisimple $\mathbb{F}_p$ group $\mathbf{H}$ such that $\mathbf{H}(\mathbb{F}_p) \cong \prod_{i \in I} \mathbf{S}_i(\overline{\mathbb{F}_{q_i}})^{\Phi_i}$.

By Corollary 3.1.9, the restriction of t to Δ extends to an involution s of $\mathbf{H}$.

By [Nor87, Lemma 3.5], $(p-1)^{\dim \mathbf{H}} \leq \left|\mathbf{H}(\mathbb{F}_p)\right|$ and $\left|\mathbf{G}(\mathbb{F}_p)\right| \leq (p+1)^{\dim \mathbf{G}}$, so

$$(p-1)^{\dim \mathbf{H}} \leq \left|\mathbf{H}(\mathbb{F}_p)\right| \leq |\Delta| 2^{\dim \mathbf{G}} \leq \left|\mathbf{G}(\mathbb{F}_p)\right| 2^{\dim \mathbf{G}} \leq (2p+2)^{\dim \mathbf{G}} \leq (3p-3)^{\dim \mathbf{G}}.$$

Since $p > 3^{\dim \mathbf{G}} + 1$, we have

$$\frac{\dim \mathbf{H}}{\dim \mathbf{G}} \leq \frac{\log(3p-3)}{\log(p-1)} < 1 + \frac{1}{\dim \mathbf{G}},$$

so $\dim \mathbf{H} \leq \dim \mathbf{G}$.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

Step 3: The claim holds if $\mathbf{G}$ is semisimple (but not necessarily adjoint), with the bound C^{ss}_{LP0}.
Let $\overline{\mathbf{G}} = \mathbf{G}/\mathbf{Z}(\mathbf{G})$, let $\pi : \mathbf{G} \to \overline{\mathbf{G}}$ be the projection and let $\overline{\Gamma} = \pi(\Gamma)$. Applying the previous step to $\overline{\Gamma}, \overline{\mathbf{G}}$, there are two possible cases:
Case 1: There is a proper connected t -invariant subgroup $\overline{\mathbf{N}} < \overline{\mathbf{G}}$ such that $[\overline{\Gamma} : \overline{\Gamma} \cap \overline{\mathbf{N}}(\mathbb{F}_p)] < D(n)$.
Case 2: There is a subgroup $\overline{\Delta} \subset \overline{\Gamma}$, a semisimple group $\overline{\mathbf{H}}$ with an action of S_2 and an S_2-equivariant injective homomorphism $\overline{\rho} : \overline{\Delta} \to \overline{\mathbf{H}}(\mathbb{F}_p)$, such that $\overline{\rho}(\overline{\Delta}) \subset \overline{\mathbf{H}}(\mathbb{F}_p)$ is big and $[\overline{\Gamma} : \overline{\Delta}] < C^{adj}_{LP0}(n)$.

In the first case, we are done by the induction assumption. For the second case, note that $\rho\left(\overline{\Delta}'\right) = \overline{\mathbf{H}}(\mathbb{F}_p)'$ and, by Lemma 3.1.6, we have $[\overline{\Delta} : \overline{\Delta}'] \le 2^n$. Denote $\Delta := \pi^{-1}(\overline{\Delta}') \cap \Gamma$. We get that

$$[\Gamma : \Delta] < C^{adj}_{LP0}(n)2^n = C^{ss}_{LP0}(n),$$

where Δ is a central extension of $\overline{\Delta}' = \overline{\mathbf{H}}(\mathbb{F}_p)'$. By Lemma 4.0.9, this central extension can be extended to an S_2-equivariant central extension $\mathbf{H}$ of $\overline{\mathbf{H}}$ in such a way that the embedding

$$\Delta \to \mathbf{H}(\mathbb{F}_p)$$

has big image, as required.

Step 4: The claim holds if $\mathbf{G}$ is a direct product of a semisimple group and a torus, with the bound C^{ss}_{LP0}.
Write $\mathbf{G} = \mathbf{G}' \times \mathbf{T}$. Let $p : \mathbf{G} \to \mathbf{G}'$ be the projection and $\bar{\Gamma} := p(\Gamma)$. Applying the previous step to $\bar{\Gamma}$, we get groups $\bar{\Delta}$ and $\bar{\mathbf{H}}$. The claim holds for $\Delta := \bar{\Delta} \times \mathbf{T}(\mathbb{F}_p) \cap \Gamma$ and $\mathbf{H} := \bar{\mathbf{H}} \times \mathbf{T}$.

Step 5: The claim holds if $\mathbf{G}$ is reductive.
Let $\tilde{\mathbf{G}} := \mathbf{G}' \times Z(\mathbf{G})^\circ$. We have an isogeny $\pi : \tilde{\mathbf{G}} \to \mathbf{G}$. By Lemma 3.1.5 and Theorem 3.1.1(5), $[\mathbf{G}(\mathbb{F}_p), \pi(\tilde{\mathbf{G}}(\mathbb{F}_p))] \le 2^n$. Let $\tilde{\Gamma} := \pi^{-1}(\Gamma)$. Applying the previous step to $\tilde{\Gamma} \subset \tilde{\mathbf{G}}(\mathbb{F}_p)$, we get groups $\tilde{\Delta}, \tilde{\mathbf{H}}$ and a map $\tilde{\rho} : \tilde{\Delta} \to \tilde{\mathbf{H}}(\mathbb{F}_p)$. Note that $Ker(\pi) \cap \tilde{\Delta}$ is central in $\tilde{\Delta}$, and thus, $\tilde{\rho}(Ker(\pi) \cap \tilde{\Delta})$ is central in $\tilde{\rho}(\tilde{\Delta})$. Since $\rho(\tilde{\Delta})$ is big in $\tilde{\mathbf{H}}(\mathbb{F}_p)$, we get (by Lemma 4.0.10) that $\tilde{\rho}(Ker(\pi) \cap \tilde{\Delta})$ is central in $\tilde{\mathbf{H}}$. Define $\mathbf{H} = \tilde{\mathbf{H}}/\tilde{\rho}(Ker(\pi) \cap \tilde{\Delta})$ and $\Delta := \pi(\tilde{\Delta}) \cong \tilde{\Delta}/(Ker(\pi) \cap \tilde{\Delta})$. Note that $[\Gamma : \Delta] \le C_{LP0}(n)$. The map $\tilde{\rho}$ desends to a map $\rho : \Delta \to \mathbf{H}(\mathbb{F}_p)$, and we are done.

Step 6: The claim holds for all connected groups $\mathbf{G}$.
Denoting the unipotent radical of $\mathbf{G}$ by $\mathbf{U}$, t induces an involution on $\mathbf{G}/\mathbf{U}$, and the projection $\pi : \mathbf{G} \to \mathbf{G}/\mathbf{U}$ is equivariant. By the previous step, we can assume that $\mathbf{U}$ is positive dimensional. Given Γ, let $\bar{\Gamma} = \pi(\Gamma)$. By induction, there is a subgroup $\bar{\Delta} \subset \bar{\Gamma}$, an algebraic group $\bar{\mathbf{H}}$ and a homomorphism $\bar{\rho} : \bar{\Delta} \to \mathbf{H}(\mathbb{F}_p)$. It is easy to see that $\Delta := \pi^{-1}(\bar{\Delta})$, $\mathbf{H} := \bar{\mathbf{H}}$ and $\rho := \bar{\rho} \circ \pi$ satisfy the requirements of the proposition. □

Corollary 4.0.11. *There is an increasing function $C_{mon} : \mathbb{N} \to \mathbb{N}$ for which the following holds. If p is a prime and $\Delta \subset \Gamma$ are finite groups such that $\mathrm{Rad}_p(\Delta) \neq \Delta \cap \mathrm{Rad}_p(\Gamma)$, then there is a normal subgroup $\Delta^\circ \lhd \Delta$ of index at most $C_{mon0}(\overline{\mathrm{rd}}_p(\Gamma))$ satisfying $\overline{\mathrm{rd}}_p(\Delta^\circ) < \overline{\mathrm{rd}}_p(\Gamma)$.*

For the proof, we will need the following:

Lemma 4.0.12. *Let $p > 3$ be a prime and let $\mathbf{H}$ be a reductive group over $\mathbb{F}_p$. Let $\Gamma < \mathbf{H}(\mathbb{F}_p)$ be a big subgroup. Then Γ does not have a nontrivial normal p-subgroup.*

Proof. Suppose that P is a nontrivial normal p-subgroup of Γ. Since the index of $\mathbf{H}(\mathbb{F}_p)'$ in $\mathbf{H}(\mathbb{F}_p)$ is prime to p, we have $P \subset \mathbf{H}(\mathbb{F}_p)'$. For similar reasons, $P \cap Z(\mathbf{H}(\mathbb{F}_p)') = 1$. This gives an embedding of P into $\mathbf{H}(\mathbb{F}_p)'/Z(\mathbf{H}(\mathbb{F}_p)')$, which is a product of nonabelian simple groups, a contradiction. □

Proof of Corollary 4.0.11. Set $C_{mon0}(n) := \max(4^n, (C_{LP0}(n) + 1)^n)$. Suppose that $\Delta \subset \Gamma$ are as in the statement of the corollary. Without loss of generality, we can assume that $\mathrm{Rad}_p(\Gamma)$ is trivial. Let $n := \overline{\mathrm{rd}}_p(\Gamma)$. Using the bound $|\mathbf{G}(\mathbb{F}_p)| \le (p+1)^{\dim \mathbf{G}}$ from [Nor87, Lemma 3.5], we may also assume

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

that $p > 3$ and $p > C_{LP0}(n)$ (otherwise, the claim holds with $\Delta^\circ = 1$). Embed $\Gamma \hookrightarrow \mathbf{G}(\mathbb{F}_p)$ with $\mathbf{G}$ connected reductive of dimension n. Applying Proposition 4.0.8 to $\Delta \subset \mathbf{G}(\mathbb{F}_p)$, there is a normal subgroup $\Delta^\circ \triangleleft \Delta$, a connected reductive group $\mathbf{H}$ defined over $\mathbb{F}_p$, and a homomorphism $\rho : \Delta^\circ \to \mathbf{H}(\mathbb{F}_p)$ such that

1. $[\Delta : \Delta^\circ] \le C_{LP0}(n)$.
2. $\ker \rho$ is a p-group.
3. $\rho(\Delta^\circ)$ is big in $\mathbf{H}(\mathbb{F}_p)$.
4. $\dim \mathbf{H} \le n$.
5. If $\dim \mathbf{H} = n$, then $\ker \rho = 1$.

By Lemma 4.0.12, $\ker \rho = \mathrm{Rad}_p(\Delta^\circ)$. In particular, $\overline{\mathrm{rd}}_p(\Delta^\circ) \le \dim \mathbf{H}$.

If $\dim \mathbf{H} < n$, we are done. Otherwise, since $[\Delta : \Delta^\circ] < C_{LP0}(n) < p$, we get that

$$\mathrm{Rad}_p(\Delta) \subset \mathrm{Rad}_p(\Delta^\circ) = \ker \rho = 1,$$

contradicting the condition that $\mathrm{Rad}_p(\Delta) \neq \Delta \cap \mathrm{Rad}_p(\Gamma)$. □

Corollary 4.0.13. *There is an increasing function $C_{LP} : \mathbb{N} \to \mathbb{N}$ for which the following holds. If p is a prime, (Γ, θ) is a finite symmetric pair and $\mathrm{Rad}_p(\Gamma) = 1$, then there is a θ-invariant normal subgroup $\Delta \triangleleft \Gamma$ satisfying $[\Gamma : \Delta] < C_{LP}(\mathrm{rd}_p(\Gamma))$, a connected reductive algebraic group $\mathbf{H}$ satisfying $\dim \mathbf{H} \le 2\mathrm{rd}_p(\Gamma)$, an involution t of $\mathbf{H}$ and an S_2-equivariant embedding $\Delta \subset \mathbf{H}(\mathbb{F}_p)$ such that $\mathbf{H}(\mathbb{F}_p)' \subset \Delta \subset \mathbf{H}(\mathbb{F}_p)$.*

Proof. Set $C_{LP}(n) = C_{LP0}(2n)$. Embed $\Gamma \hookrightarrow \mathbf{G}$ and apply Proposition 4.0.8 to $\mathbf{G} \times \mathbf{G}$, the involution $t(x, y) = (y, x)$ and the subgroup $\{(x, \theta(x)) \mid x \in \Gamma\} \cong \Gamma$. □

4.1. θ-invariant subgroups of bounded index

In this subsection, we prove Corollary 4.1.2, which is a S_2-equivariant version of the monotonicity of $\overline{\mathrm{rd}}$, Corollary 4.0.11.

Lemma 4.1.1. *There is a function $C_{inv} : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$ which is increasing in both variables such that, for any*

- *pair of finite groups $\Delta < \Gamma$ and*
- *a prime p,*

there exists a subgroup $\Delta^\circ \triangleleft \Delta$ which is normal in Γ and satisfies

$$[\Gamma : \Delta^\circ] \le C_{inv}(\overline{\mathrm{rd}}_p(\Delta), [\Gamma : \Delta])$$

and

$$\overline{\mathrm{rd}}_p(\Delta^\circ) \le \overline{\mathrm{rd}}_p(\Delta).$$

Proof. Define recursively

$$C_{inv}(0, k) = k!$$

and

$$C_{inv}(n, k) := k! C_{mon0}(n) C_{inv}(n - 1, k! C_{mon0}(n)).$$

We will prove the lemma by induction on $\overline{\mathrm{rd}}_p(\Delta)$. For $\overline{\mathrm{rd}}_p(\Delta) = 0$, the claim is clear. For the induction step, let $n > 0$ be an integer and assume the lemma holds if $\overline{\mathrm{rd}}_p(\Delta) < n$. We prove the lemma for $\overline{\mathrm{rd}}_p(\Delta) = n$. Let

$$\Delta_1 := \bigcap_{\gamma \in \Gamma} \gamma \Delta \gamma^{-1}.$$

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

We consider the following cases:

Case 1. $\mathrm{Rad}_p(\Delta_1) = \mathrm{Rad}_p(\Delta) \cap \Delta_1$.
In this case, $\overline{\mathrm{rd}}_p(\Delta_1) \leq \overline{\mathrm{rd}}_p(\Delta) = n$, so we can take $\Delta^\circ := \Delta_1$, and we are done.

Case 2. $\mathrm{Rad}_p(\Delta_1) \neq \mathrm{Rad}_p(\Delta) \cap \Delta_1$.
In this case, Corollary 4.0.11 implies that we can find Δ_2 such that

$$\overline{\mathrm{rd}}_p(\Delta_2) < \overline{\mathrm{rd}}_p(\Delta) = n$$

and

$$[\Delta_1 : \Delta_2] \leq C_{mon0}(n).$$

By the induction hypothesis, there exists $\Delta^\circ \lhd \Delta_2$ which is normal in Γ and satisfies

$$[\Delta_2 : \Delta^\circ] \leq C_{inv}(n-1, [\Gamma : \Delta_2])$$

and

$$\overline{\mathrm{rd}}_p(\Delta^\circ) \leq \overline{\mathrm{rd}}_p(\Delta_2) < n.$$

We get

$$\begin{aligned}
[\Gamma : \Delta^\circ] &\leq [\Gamma : \Delta_1] \cdot [\Delta_1 : \Delta_2] \cdot [\Delta_2 : \Delta^\circ] \\
&\leq [\Gamma : \Delta]! C_{mon0}(n) C_{inv}(n-1, [\Gamma : \Delta_2]) \\
&\leq [\Gamma : \Delta]! C_{mon0}(n) C_{inv}(n-1, [\Gamma : \Delta_1] \cdot [\Delta_1 : \Delta_2]) \\
&\leq [\Gamma : \Delta]! C_{mon0}(n) C_{inv}(n-1, [\Gamma : \Delta]! C_{LP}(n)) = C_{inv}(n, [\Gamma : \Delta]). \qquad \square
\end{aligned}$$

The last lemma and Corollary 4.0.11 imply the following:

Corollary 4.1.2. *There is a function $C_{mon} : \mathbb{N} \to \mathbb{N}$ such that, for any odd prime p, any finite group Γ, any subgroup $\Delta < \Gamma$ satisfying $\mathrm{Rad}_p(\Delta) \neq \Delta \cap \mathrm{Rad}_p(\Gamma)$, and any involution θ of Δ, there is a normal θ-invariant subgroup $\Delta^\circ \lhd \Delta$ such that*

- $\overline{\mathrm{rd}}_p(\Delta^\circ) < \overline{\mathrm{rd}}_p(\Gamma)$.
- $[\Delta : \Delta^\circ] \leq C_{mon}(\overline{\mathrm{rd}}_p(\Gamma))$.

Proof. Set

$$C_{mon}(n) := C_{inv}(n, 2C_{mon0}(n)).$$

By the monotonicity of the $\overline{\mathrm{rd}}_p$ (Corollary 4.0.11), we can find $\Delta_1 \lhd \Delta$ satisfying

$$\overline{\mathrm{rd}}_p(\Delta_1) < \overline{\mathrm{rd}}_p(\Gamma)$$

and

$$[\Delta : \Delta_1] \leq C_{mon0}(\overline{\mathrm{rd}}_p(\Gamma)).$$

Let $\tilde{\Delta} := \langle\theta\rangle \ltimes \Delta$. By Lemma 4.1.1, there is a normal subgroup $\Delta^\circ \lhd \Delta_1$ which is also normal in $\tilde{\Delta}$ and satisfies

$$[\tilde{\Delta} : \Delta^\circ] \leq C_{inv}(\overline{\mathrm{rd}}_p(\Delta_1), [\tilde{\Delta} : \Delta_1])$$

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

and

$$\overline{\mathrm{rd}}_p(\Delta^\circ) \le \overline{\mathrm{rd}}_p(\Delta_1) < \overline{\mathrm{rd}}_p(\Gamma).$$

The fact that Δ° is normal in $\tilde{\Delta}$ implies that Δ° is θ-invariant. We also have

$$\begin{aligned}[\Delta : \Delta^\circ] \le [\tilde{\Delta} : \Delta^\circ] &\le C_{inv}(\overline{\mathrm{rd}}_p(\Delta_1), [\tilde{\Delta} : \Delta_1]) \\ &\le C_{inv}(\overline{\mathrm{rd}}_p(\Gamma), [\tilde{\Delta} : \Delta_1]) = C_{inv}(\overline{\mathrm{rd}}_p(\Gamma), 2[\Delta : \Delta_1]) \\ &\le C_{inv}(\overline{\mathrm{rd}}_p(\Gamma), 2C_{mon0}(\overline{\mathrm{rd}}_p(\Gamma))) = C_{mon}(\overline{\mathrm{rd}}_p(\Gamma)).\end{aligned}$$ □

5. Groups of odd order

In this section, we analyze symmetric pairs of groups of odd order and prove several statements about them that will be used in the proof of the main theorem. In particular, we prove a strong version of the main theorem for symmetric pairs of groups of odd order. Namely, we prove that they are all Gelfand pairs (Corollary 5.0.5(1)).

We also prove some other results for symmetric pairs of groups of odd order; see Lemma 5.0.2 and Corollary 5.0.5(2).

Remark 5.0.1.

1. Even though the results in this section are valid for arbitrary groups of odd order, we will only use them for p-groups for odd p.
2. All the proofs in this section are based on the fact that, for a group of odd order n, the map $x \mapsto x^{\frac{n+1}{2}}$ is a square root.

The following is a special case of the Schur–Zassenhaus theorem:

Lemma 5.0.2. *If Ω is a finite group of odd order and θ is its involution, then $H^1(S_2, \Omega) = 1$.*

Proof. We need to show that, for every element $s \in \Omega$ that satisfies $s = \theta(s^{-1})$, there exists an element $g \in \Omega$ such that $s = \theta(g^{-1})g$.

Let $g = s^{\frac{|\Omega|+1}{2}}$. Then

$$\theta(g^{-1})g = \theta((s^{\frac{|\Omega|+1}{2}})^{-1})s^{\frac{|\Omega|+1}{2}} = \theta(s^{-1})^{\frac{|\Omega|+1}{2}} s^{\frac{|\Omega|+1}{2}} = s^{\frac{|\Omega|+1}{2}} s^{\frac{|\Omega|+1}{2}} = s^{|\Omega|+1} = s.$$ □

Lemma 5.0.3 (Gelfand-Kazhdan property for symmetric pairs of odd order). *If Ω is a finite group of odd order and $\theta : \Omega \to \Omega$ is an involution, then, for any $g \in \Omega$, there are $h_1, h_2 \in \Omega^\theta$ such that $h_1 g h_2 = \theta(g^{-1})$.*

Lemma 5.0.3 follows immediately from the following:

Lemma 5.0.4 (polar decomposition for symmetric pairs of odd order.) *If Ω is a finite group of odd order and $\theta : \Omega \to \Omega$ is an involution, then*

$$\Omega = \Omega^\theta \cdot \Omega^{\theta\circ inv},$$

where $\Omega^{\theta\circ inv} := \{g \in \Omega | \theta(g) = g^{-1}\}$.

Proof. Let $g \in \Omega$. Define $s = (\theta(g^{-1})g)^{\frac{|\Omega|+1}{2}}$ and $o = gs^{-1}$. Then,

$$\begin{aligned}
\theta(s) &= \theta((\theta(g^{-1})g)^{\frac{|\Omega|+1}{2}}) \\
&= (\theta(\theta(g^{-1})g))^{\frac{|\Omega|+1}{2}} \\
&= (g^{-1})\theta(g))^{\frac{|\Omega|+1}{2}} \\
&= ((\theta(g^{-1})g)^{-1})^{\frac{|\Omega|+1}{2}} \\
&= ((\theta(g^{-1})g)^{\frac{|\Omega|+1}{2}})^{-1}) = s^{-1}, \\
\theta(o) &= \theta(gs^{-1}) = \theta(g)s \\
&= \theta(g)(\theta(g^{-1})g)^{\frac{|\Omega|+1}{2}} \\
&= \theta(g)\theta(g^{-1})g(\theta(g^{-1})g)^{\frac{|\Omega|+1}{2}-1} \\
&= g(\theta(g^{-1})g)^{\frac{|\Omega|+1}{2}-1} \\
&= g(\theta(g^{-1})g)^{\frac{|\Omega|-1}{2}} \\
&= g(\theta(g^{-1})g)^{|\Omega|-\frac{|\Omega|+1}{2}} \\
&= g(\theta(g^{-1})g)^{-\frac{|\Omega|+1}{2}} = gs^{-1} = o
\end{aligned}$$

and, thus,

$$g = gs^{-1}s = os. \qquad \square$$

Lemma 5.0.3 gives the following:

Corollary 5.0.5. *If Γ is a finite group of odd order and θ is an involution of Ω, then*

1. *(Gelfand property for symmetric pairs of odd order:) (Ω, Ω^θ) is a Gelfand pair – that is, for any $\rho \in \mathrm{Irr}(\Omega)$,*

$$\dim \rho^{\Omega^\theta} \leq 1.$$

2. *(Lapid-Prasad property for symmetric pairs of odd order:) Any representation ρ of G which is Ω^θ distinguished (i.e., satisfies $\dim \rho^{\Omega^\theta} > 0$) also satisfies*

$$\rho^* \simeq \rho \circ \theta.$$

Proof. The claims follow from Lemma 5.0.3 and [Aiz, Theorem 2] (which is an adaptation of results from [GK75] and [JR96]). $\square$

6. Bounds on $H^1(S_2, \Gamma)$

In this section, we prove Corollary 6.0.6, which gives bounds on the cohomology group $H^1(S_2, \Delta)$ for a finite symmetric pair (Δ, θ).

Lemma 6.0.1. *There is an increasing function $C_{H1R0} : \mathbb{N} \to \mathbb{N}$ such that, for any finite field F of odd characteristic, any connected reductive group $\mathbf{G}$ and any involution t of $\mathbf{G}$, both defined over F,*

$$|H^1(S_2, \mathbf{G}(F))| < C_{H1R0}(\dim \mathbf{G}).$$

Proof. Let n be an integer. Let $\Phi_n : \mathcal{R}_n \to \mathcal{S}_n$ and τ_n be as in Lemma 3.2.1. Let s_n be the anti-automorphism $s_n(g) := \tau_n(g^{-1})$. Let $C_{H1R0}(n)$ be such that, for any geometric point x of $\mathcal{S}_n$,

$$\left|\pi_0\left(\Phi_n^{-1}(x)^{s_n}\right)\right| < C_{H1R0}(n).$$

Fix $x \in \mathcal{S}_n(F)$ and let $\mathbf{G} := \Phi_n^{-1}(x)$. We need to show that

$$|H^1(S_2, \mathbf{G}(F))| \le C_{H1R0(n)}.$$

By definition, we have $H^1(S_2, \mathbf{G}(F)) = \mathbf{G}(F)^{s_n}/\mathbf{G}(F)$, where the action of $\mathbf{G}$ on $\mathbf{G}^{s_n}$ is given by $g \cdot x := gxs_n(g)$. Since $\mathbf{G}$ is connected, Lang's theorem implies that the map $\mathbf{G}(F)^{s_n}/\mathbf{G}(F) \to (\mathbf{G}^{s_n}/\mathbf{G})(F)$ is an embedding. By analyzing the action of the Lie algebra, it is easy to see that the orbits of the action of $\mathbf{G}$ on $\mathbf{G}^{s_n}$ are open. Thus,

$$|H^1(S_2, \mathbf{G}(F))| = |\mathbf{G}(F)^{s_n}/\mathbf{G}(F)| \le |(\mathbf{G}^{s_n}/\mathbf{G})(F)| \le |(\mathbf{G}^{s_n}/\mathbf{G})(\overline{F})| = |\pi_0(\mathbf{G}_{\overline{F}}^{s_n})| \le C_{H1R0}(n).$$

□

The following lemmas are straightforward:

Lemma 6.0.2. *Let A be a finite abelian group with an action of S_2. Denote $A[2] = \left\{x \in A \mid x^2 = 0\right\}$. Then $|H^1(S_2, A)| \le |A[2]|^2$.*

Proof. Let $\theta \in \mathrm{Aut}(A)$ be the nontrivial element of S_2. Denote $C = \{x \in A \mid x\theta(x) = 1\}$, $B = \left\{x^{-1}\theta(x) \mid x \in A\right\}$ and $S = \left\{x^2 \mid x \in A\right\}$. We need to show that $|C/B| \le |A[2]|^2$. Since $|C/B| = |C/C\cap S| \cdot |C\cap S/B\cap S| \le |A[2]| \cdot |C\cap S/B\cap S|$, it in enough to show that $|C\cap S/B\cap S| \le |A[2]|$.

Let $x \in C \cap S$ and let $z \in A$ be such that $z^2 = x$. Then $z\theta(z) \in A[2]$ and $x\left(z^{-1}\theta(z)\right) = z\theta(z) \in A[2]$. Hence, $C \cap S \subseteq A[2] \cdot B$, so $|C \cap S/B \cap S| \le |A[2] \cdot B/B| \le |A[2]|$. □

Lemma 6.0.3. *Let Γ be a finite group, let θ be an involution of Γ and let $N \triangleleft \Gamma$ be a normal θ-invariant subgroup. Then*

1. $|H^1(S_2, N)| \le |H^1(S_2, \Gamma)| \cdot [\Gamma : N]$.
2. $$|H^1(S_2, \Gamma)| \le |H^1(S_2, \Gamma/N)| \cdot \max_{\tau} |H^1_{\tau}(S_2, N)|,$$

   where τ ranges over all involutions of N (including $\tau = 1$) and $H^1_\tau(S_2, N)$ is the cohomology of the S_2-module N given by the involution τ.

Proof. In the proof, if G is a group with involution σ, we identify $H^1(S_2, G)$ with the quotient of $C_{G,\sigma} := \{x \in G \mid x\sigma(x) = 1\}$ by the action of G given by $g \cdot x = \sigma(g)xg^{-1}$.

1. We have have a map $\alpha : C_{N,\theta}/N \to C_{\Gamma,\theta}/\Gamma$ taking $N \cdot x$ to $\Gamma \cdot x$. Given $x \in C_{N,\theta}$, the fiber $\alpha^{-1}(\alpha(N \cdot x)) = \alpha^{-1}(\Gamma \cdot x)$ is equal to $(\Gamma \cdot x)/N$, so its size is at most $[\Gamma : N]$. Hence, $|C_{N,\theta}/N| \le |C_{\Gamma,\theta}/\Gamma| \cdot [\Gamma : N]$.
2. We have a map $\beta : C_{\Gamma,\theta}/\Gamma \to C_{\Gamma/N,\theta}/(\Gamma/N)$ sending $\Gamma \cdot x$ to $(\Gamma/N) \cdot (xN)$. It is enough to show that the sizes of the fibers of β are bounded by $\max_\tau |H^1_\tau(S_2, N)|$.

   For $x \in C_{\Gamma,\theta}$, let $\tau_x : N \to N$ be the automorphism $\tau_x(n) = x^{-1}\theta(n)x$. Since $\tau_x^2(n) = x^{-1}\theta(x^{-1})n\theta(x)x = n$, the automorphism τ_x is an involution.

   Suppose that $y \in C_{\Gamma,\theta}$ and $\beta(\Gamma \cdot x) = \beta(\Gamma \cdot y)$. Then there is $y' \in \Gamma \cdot y$ such that $y' = xn$, for some $n \in N$. Since

$$1 = \theta(y')y' = \theta(x)\theta(n)xn = \theta(x)xx^{-1}\theta(n)xn = \tau_x(n)n,$$

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

we get that $n \in C_{N,\tau_x}$. Hence, $\beta^{-1}(\beta(\Gamma \cdot x))$ can be identified with $xC_{N,\tau_x}/\Gamma$. For any $m \in N$,

$$m \cdot y' = \theta(m)xnm^{-1} = x\tau_x(m)nm^{-1},$$

so $|\beta^{-1}(\beta(\Gamma \cdot x))| \leq |xC_{N,\tau_x}/N| = |H^1_{\tau_x}(S_2, N)|$. □

Now Lemma 6.0.1 implies the following:

Corollary 6.0.4. *There is an increasing function $C_{H1R} : \mathbb{N} \to \mathbb{N}$ such that, for any prime p, any connected semi-simple group $\mathbf{G}$, defined over $\mathbb{F}_p$, any involution θ of $\mathbf{G}(\mathbb{F}_p)'$, we have*

$$|H^1(S_2, \mathbf{G}(\mathbb{F}_p)')| < C_{H1R}(\dim \mathbf{G}).$$

Proof. Take $C_{H1R}(n) = C_{H1R0}(\dim \mathbf{G})4^{\dim G}$, where C_{H1R0} is the function given by Lemma 6.0.1.

Using the bound $|\mathbf{G}(\mathbb{F}_p)| \leq (p+1)^{\dim \mathbf{G}}$ from [Nor87, Lemma 3.5], we can assume that $p > 3$.

Let $\bar{\mathbf{G}} := \mathbf{G}/Z(\mathbf{G})$. By Corollary 3.1.3, the induced map $\mathbf{G}(\mathbb{F}_p)' \to \bar{\mathbf{G}}(\mathbb{F}_p)'$ is onto, and its kernel is $Z(\mathbf{G}(\mathbb{F}_p)')$. Let $\bar{\theta}$ be the involution induced by θ on $\bar{\mathbf{G}}(\mathbb{F}_p)'$. By Theorem 3.1.10, we can lift $\bar{\theta}$ to an involution t of $\bar{\mathbf{G}}$. By Lemmas 6.0.3, 6.0.1, 3.1.6 and Theorem 3.1.1, we have

$$\begin{aligned}
|H^1(S_2, \mathbf{G}(\mathbb{F}_p)')| &\overset{6.0.3}{\leq} |H^1(S_2, \bar{\mathbf{G}}(\mathbb{F}_p)')| \max_\tau |H^1_\tau(S_2, Z(\mathbf{G}(\mathbb{F}_p)'))| \leq |H^1(S_2, \bar{\mathbf{G}}(\mathbb{F}_p)')| \cdot |Z(\mathbf{G}(\mathbb{F}_p)')| \\
&\overset{3.1.1}{\leq} |H^1(S_2, \bar{\mathbf{G}}(\mathbb{F}_p)')| 2^{\dim G} \overset{6.0.3}{\leq} |H^1_t(S_2, \bar{\mathbf{G}}(\mathbb{F}_p))| \cdot [\bar{\mathbf{G}}(\mathbb{F}_p) : \bar{\mathbf{G}}(\mathbb{F}_p)'] 2^{\dim G} \\
&\overset{3.1.6}{\leq} |H^1_t(S_2, \bar{\mathbf{G}}(\mathbb{F}_p))| \cdot 4^{\dim G} \overset{6.0.1}{<} C_{H1R0}(\dim \mathbf{G}) 4^{\dim G} = C_{H1R}(\dim \mathbf{G}).
\end{aligned}$$ □

Now we can derive our bound on the first cohomology:

Proposition 6.0.5. *There is a function $C_{H1} : \mathbb{N} \to \mathbb{N}$ such that for any finite group Γ, any involution θ of Γ and any prime $p > 2$, we have*

$$H^1(S_2, \Gamma) < C_{H1}(\overline{\mathrm{rd}}_p(\Gamma)).$$

Proof. We take

$$C_{H1}(n) := C_{H1R}(2n) C_{LP}(n) 2^{8n},$$

where C_{H1R} is the function given by Corollary 6.0.4 and C_{LP} is the function given by Corollary 4.0.13.

Using the bound $|\mathbf{G}(\mathbb{F}_p)| \leq (p+1)^{\dim \mathbf{G}}$ from [Nor87, Lemma 3.5] and Lemmas 5.0.2, 6.0.3, we may assume that $p > 3$.

Let $\bar{\theta}$ be the involution of $\Gamma/\mathrm{Rad}_p(\Gamma)$ induced by θ. By Corollary 4.0.13, there is a $\bar{\theta}$-invariant normal subgroup Δ of $\Gamma/\mathrm{Rad}_p(\Gamma)$, a connected reductive group $\mathbf{H}$ defined over $\mathbb{F}_p$ and an involution t of $\mathbf{H}$ such that

- $[\Gamma/\mathrm{Rad}_p(\Gamma) : \Delta] \leq C_{LP}(\overline{\mathrm{rd}}(\Gamma))$,
- $\dim \mathbf{H} \leq 2\overline{\mathrm{rd}}(\Gamma)$,
- There is an equivariant embedding $(\Delta, \bar{\theta}|_\Delta) \hookrightarrow (\mathbf{H}(\mathbb{F}_p), t)$,
- $\mathbf{H}(\mathbb{F}_p)' < \Delta < \mathbf{H}(\mathbb{F}_p)$.

By Corollary 3.1.4, we have $\Delta' = \mathbf{H}(\mathbb{F}_p)'$.

Applying Theorem 3.1.1, Corollary 6.0.4 and Lemmas 5.0.2, 6.0.2, 6.0.3, we get

$$
\begin{aligned}
|H^1(S_2,\Gamma)| &\overset{6.0.3}{\leq} |H^1(S_2,\Gamma/\mathrm{Rad}_p(\Gamma))| \cdot \max_\tau |H^1_\tau(S_2,\mathrm{Rad}_p(\Gamma))| \overset{5.0.2}{=} |H^1(S_2,\Gamma/\mathrm{Rad}_p(\Gamma))| \\
&\overset{6.0.3}{\leq} \max_\tau |H^1_\tau(S_2,\Delta)| \cdot |H^1(S_2,(\Gamma/(\mathrm{Rad}_p(\Gamma))/\Delta))| \\
&\overset{6.0.3}{\leq} \max_\tau |H^1_\tau(S_2,\Delta)| \cdot [\Gamma/\mathrm{Rad}_p(\Gamma):\Delta] \\
&\leq \max_\tau |H^1_\tau(S_2,\Delta)| C_{LP}(\overline{\mathrm{rd}}(\Gamma)) \\
&\overset{6.0.3}{\leq} \max_\sigma |H^1_\sigma(S_2,\Delta')| \cdot \max_\tau |H^1_\tau(S_2,\Delta/\Delta')| \cdot C_{LP}(\overline{\mathrm{rd}}(\Gamma)) \\
&\overset{6.0.2}{\leq} \max_\sigma |H^1_\sigma(S_2,\mathbf{H}(\mathbb{F}_p)')| \cdot |(\Delta/\Delta')[2]|^2 \cdot C_{LP}(\overline{\mathrm{rd}}(\Gamma)) \\
&\overset{6.0.4}{\leq} C_{H1R}(2\overline{\mathrm{rd}}(\Gamma)) \cdot |(\Delta/\Delta')[2]|^2 \cdot C_{LP}(\overline{\mathrm{rd}}(\Gamma)) \\
&\leq C_{H1R}(2\overline{\mathrm{rd}}(\Gamma)) \cdot |\big(\mathbf{H}(\mathbb{F}_p)/\mathbf{H}(\mathbb{F}_p)'\big)[2]|^2 \cdot C_{LP}(\overline{\mathrm{rd}}(\Gamma)) \\
&\leq C_{H1R}(2\overline{\mathrm{rd}}(\Gamma)) \cdot |\big(\mathbf{H}(\mathbb{F}_p)/\mathbf{H}'(\mathbb{F}_p)\big)[2]|^2 \cdot [\mathbf{H}'(\mathbb{F}_p):\mathbf{H}(\mathbb{F}_p)']^2 \cdot C_{LP}(\overline{\mathrm{rd}}(\Gamma)) \\
&\overset{3.1.6}{\leq} C_{H1R}(2\overline{\mathrm{rd}}(\Gamma)) \cdot |\big((\mathbf{H}/\mathbf{H}')(\mathbb{F}_p)\big)[2]|^2 \cdot 2^{4\overline{\mathrm{rd}}(\Gamma)} \cdot C_{LP}(\overline{\mathrm{rd}}(\Gamma)) \\
&\leq C_{H1R}(2\overline{\mathrm{rd}}(\Gamma)) \cdot 2^{8\overline{\mathrm{rd}}(\Gamma)} \cdot C_{LP}(\overline{\mathrm{rd}}(\Gamma)) = C_{H1}(\overline{\mathrm{rd}}(\Gamma)).
\end{aligned}
$$
□

Corollary 6.0.6. *There is an increasing function $C^{her}_{H1}:\mathbb{N}\to\mathbb{N}$ such that, for any pair of finite groups $\Delta\subset\Gamma$, any involution θ of Δ and any prime $p>2$,*

$$|H^1(S_2,\Delta)| < C^{her}_{H1}(\overline{\mathrm{rd}}_p(\Gamma)).$$

Proof. Define

$$C^{her}_{H1}(n) := C_{mon}(n)C_{H1}(n).$$

By Corollary 4.1.2, there is a θ-invariant normal subgroup $\Delta^\circ \lhd \Delta$ such that $\overline{\mathrm{rd}}_p(\Delta^\circ)\leq\overline{\mathrm{rd}}_p(\Gamma)$ and $[\Delta:\Delta^\circ]\leq C_{mon}(\overline{\mathrm{rd}}_p(\Gamma))$. The previous proposition (Proposition 6.0.5) implies that $|H^1(S_2,\Delta^\circ)| < C_{H1}(\overline{\mathrm{rd}}_p(\Gamma))$. From the exact sequence

$$H^1(S_2,\Delta^\circ)\to H^1(S_2,\Delta)\to H^1(S_2,\Delta/\Delta^\circ),$$

we get

$$
\begin{aligned}
|H^1(S_2,\Delta)| &\leq |H^1(S_2,\Delta^\circ)|\cdot|H^1(S_2,\Delta/\Delta^\circ)| \\
&\leq C_{H1}(\overline{\mathrm{rd}}_p(\Gamma))[\Delta:\Delta^\circ] \\
&\leq C_{H1}(\overline{\mathrm{rd}}_p(\Gamma))C_{mon}(\overline{\mathrm{rd}}_p(\Gamma)) \\
&= C^{her}_{H1}(\overline{\mathrm{rd}}_p(\Gamma)).
\end{aligned}
$$
□

7. Bounds on $H^2(\Gamma,\mu_{p^\infty})$

Let μ_{p^∞} denote the group of roots of unity of order which is a power of p. In this section, we prove that $H^2(\Gamma,\mu_{p^\infty})$ is trivial whenever $\mathrm{Rad}_p(\Gamma)=1$ and p is large with respect to $\mathrm{rd}_p(\Gamma)$. See Proposition 7.0.2 below.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

We will need the following:

Lemma 7.0.1. *For any short exact sequence of finite groups*

$$1 \to \Gamma_1 \to \Gamma_2 \to \Gamma_3 \to 1,$$

we have

1. *If $p \nmid |\Gamma_1|$, then $H^i(\Gamma_2, \mathbb{F}_p) \cong H^i(\Gamma_3, \mathbb{F}_p)$, for all i.*
2. *If $p \nmid |\Gamma_3|$, then $H^i(\Gamma_2, \mathbb{F}_p) \cong H^i(\Gamma_1, \mathbb{F}_p)^{\Gamma_3}$, for all i.*

Proof. For a pair finite group $\Gamma \lhd \Gamma'$, let $I_\Gamma^{\Gamma'} : \mathcal{M}_{\mathbb{F}_p}(\Gamma') \to \mathcal{M}(\Gamma'/\Gamma)$ be the functor of Γ-invariants from the category of $\mathbb{F}_p$-representations of Γ' to the category of $\mathbb{F}_p$-representations of Γ'/Γ. Note that, if $p \nmid |\Gamma|$, then $I_\Gamma^{\Gamma'}$ is exact. Also denote

$$I_\Gamma := I_\Gamma^\Gamma.$$

Now

1. If $p \nmid |\Gamma_1|$, then

$$\begin{aligned} H^i(\Gamma_2, \mathbb{F}_p) &\cong R^i(I_{\Gamma_2})(\mathbb{F}_p) \cong R^i(I_{\Gamma_3} \circ I_{\Gamma_1}^{\Gamma_2})(F_p) \cong R^i(I_{\Gamma_3}) \circ I_{\Gamma_1}^{\Gamma_2}(\mathbb{F}_p) \cong \\ &\cong R^i(I_{\Gamma_3})(\mathbb{F}_p) \cong H^i(\Gamma_3, \mathbb{F}_p). \end{aligned}$$

2. If $p \nmid |\Gamma_3|$, then

$$\begin{aligned} H^i(\Gamma_2, \mathbb{F}_p) &\cong R^i(I_{\Gamma_2})(\mathbb{F}_p) \cong R^i(I_{\Gamma_3} \circ I_{\Gamma_1}^{\Gamma_2})(F_p) \\ &\cong I_{\Gamma_3} \circ R^i I_{\Gamma_1}^{\Gamma_2}(\mathbb{F}_p) \cong I_{\Gamma_3}(H^i(\Gamma_1, \mathbb{F}_p)) \cong H^i(\Gamma_1, \mathbb{F}_p)^{\Gamma_3}. \end{aligned}$$

□

Now we can prove the main result of this section:

Proposition 7.0.2 (vanishing of H^2 for large p). *There is an increasing function $C_{H2} : \mathbb{N} \to \mathbb{N}$ such that for any*

1. *integer n,*
2. *prime $p > C_{H2}(n)$,*
3. *finite group Γ such that $\mathrm{Rad}_p(\Gamma) = 1$ and $\mathrm{rd}_p(\Gamma) \leq n$,*

the group $H^2(\Gamma, \mu_{p^\infty})$ is trivial.

Proof. It is enough to show the claim after replacing μ_{p^∞} by $\mathbb{F}_p$. Define

$$C_{H2}(n) := \max(3, C_{LP0}(n), 4^n).$$

Fix n. Let $p > C_{H2}(n)$ be a prime and Γ be a finite group such that $\mathrm{Rad}_p(\Gamma) = 1$, and $\mathrm{rd}_p(\Gamma) \leq n$. We have to show that

$$H^2(\Gamma, \mathbb{F}_p) = 0.$$

By Corollary 4.0.13 applied with trivial involution,[1] there are a normal subgroup $\Delta \lhd \Gamma$, a connected reductive algebraic group $\mathbf{H}$ defined over $\mathbb{F}_p$ and an injective homomorphism $\rho : \Delta \to \mathbf{H}(\mathbb{F}_p)$ such that

1. $[\Gamma : \Delta] \leq C_{LP}(n)$.
2. $\mathbf{H}(\mathbb{F}_p)' < \rho(\Delta) < \mathbf{H}(\mathbb{F}_p)$.
3. $\dim \mathbf{H} \leq 2n$.

[1]In fact, Proposition 4.0.8 is enough.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

Applying 7.0.1(2) to the embedding $\Delta \subset \Gamma$, it is enough to prove that $H^2(\Delta, \mathbb{F}_p) = 0$. We will identify $\rho(\Delta)$ with Δ.

Let $\Delta_0 = \Delta \cap \mathbf{H}'(\mathbb{F}_p)$. We have an embedding of Δ/Δ_0 into $(\mathbf{H}/\mathbf{H}')(\mathbb{F}_p)$. Thus, $p \nmid [\Delta, \Delta_0]$. By descent of H^2 to a subgroup (Lemma 7.0.1(2)), this implies that it is enough to show that

$$H^2(\Delta_0, \mathbb{F}_p) = 0.$$

By Lemma 3.1.6, $[\Delta_0 : \mathbf{H}'(\mathbb{F}_p)'] \leq 4^n$. By Lemma 7.0.1(2), it is enough to show that $H^2(\mathbf{H}'(\mathbb{F}_p)', \mathbb{F}_p) = 0$.

Let $\pi : \widetilde{\mathbf{H}'} \to \mathbf{H}'$ the universal cover. By Corollary 3.1.3,

$$H^2(\mathbf{H}'(\mathbb{F}_p)', \mathbb{F}_p) = H^2(\pi(\widetilde{\mathbf{H}'}(\mathbb{F}_p)), \mathbb{F}_p),$$

and the latter group vanishes by combining descent of H^2 to a quotient (Lemma 7.0.1(1)) and vanishing of H^2 for simply connected groups (Theorem 3.1.1(2)). $\square$

8. The case of trivial p-radical

In this section, we prove a twisted version of the main result of the paper for the special case when Γ has a trivial p-radical (see Corollary 8.0.5 below).

We start with the case that Γ is a finite group of Lie type. This case, in the larger generality of spherical pairs but without a twist, was proved in [She]. A variation of the argument of [She] proves the twisted case. We include this variation in Appendix A. In particular, the following is a special case of Theorem 1.0.1:

Theorem 8.0.1. *There is an increasing function $C_{rd} : \mathbb{N} \to \mathbb{N}$ such that, for every finite field F of characteristic > 3, every connected reductive group $\mathbf{G}$ and every involution t of $\mathbf{G}$, we have*

$$\mu(\mathbf{G}(F), t) < C_{rd}(\dim(\mathbf{G})).$$

In order to apply this theorem to arbitrary groups with trivial p-radical, we will need the following:

Lemma 8.0.2 (cf. [AA19, Lemma 3.2.1]). *Let $\phi : \Gamma_1 \to \Gamma_2$ be morphism finite groups and let θ_1, θ_2 be involutions of Γ_1, Γ_2 such that $\theta_2 \circ \phi = \phi \circ \theta_1$. Then,*

1. $\mu(\Gamma_2, \theta_2) \leq [\Gamma_2 : \phi(\Gamma_1)]\mu(\Gamma_1, \theta_1)$.
2. $\nu(\Gamma_2, \theta_2) \leq [\Gamma_2 : \phi(\Gamma_1)]\nu(\Gamma_1, \theta_1)$.

Lemma 8.0.3. *For every prime p and every connected reductive group $\mathbf{H}$ over $\mathbb{F}_p$, we have $\left[\mathbf{H}(\mathbb{F}_p) : \mathbf{H}(\mathbb{F}_p)' \cdot Z(\mathbf{H})(\mathbb{F}_p)\right] \leq 2^{2\dim \mathbf{H}}$.*

Proof. The map $\phi : \mathbf{H}' \times Z(\mathbf{H}) \to \mathbf{H}$ is an isogeny. By Lemma 3.1.5 and Theorem 3.1.1,

$$\left[\mathbf{H}(\mathbb{F}_p) : \mathbf{H}'(\mathbb{F}_p) \cdot Z(\mathbf{H})(\mathbb{F}_p)\right] \leq |(\ker \phi)(\overline{\mathbb{F}_p})| = |Z(\mathbf{H}'(\overline{\mathbb{F}_p})| \leq |Z(\widetilde{\mathbf{H}'}(\overline{\mathbb{F}_p}))| \leq 2^{\dim \mathbf{H}'},$$

where $\widetilde{\mathbf{H}'}$ is the universal cover of $\mathbf{H}'$. By Lemma 3.1.6, $[\mathbf{H}'(\mathbb{F}_p) : \mathbf{H}(\mathbb{F}_p)'] \leq 2^{\dim \mathbf{H}'}$, and the result follows. $\square$

The following lemma is straightforward.

Lemma 8.0.4. *If A, B are finite groups and θ_A, θ_B are involutions of A, B, then $\mu(A \times B, \theta_A \times \theta_B) = \mu(A, \theta_A)\mu(B, \theta_B)$.*

Corollary 8.0.5. *There is an increasing function $C_{nr} : \mathbb{N} \to \mathbb{N}$ such that, for any prime $p > 3$ and any finite group Γ that has a trivial p-radical, we have $\mu(\Gamma) < C_{nr}(\mathrm{rd}(\Gamma))$.*

Proof. Set

$$C_{nr}(n) := C_{LP}(n)16^n C_{rd}(2n).$$

Let θ be an involution of Γ. Applying Corollary 4.0.13 to Γ, we get a triple $\Delta, \mathbf{H}, t$. By Lemma 8.0.2, we have

$$\mu(\Gamma,\theta) \le [\Gamma : \Delta] \cdot \mu(\Delta,\theta) \le C_{LP}(\mathrm{rd}_p(\Gamma))\mu(\Delta,\theta).$$

Denote $S = \mathbf{H}(\mathbb{F}_p)'$ and $Z = Z(\mathbf{H})(\mathbb{F}_p)$. Note that S and Z are t-invariant subgroups of $\mathbf{H}(\mathbb{F}_p)$. By Lemma 8.0.3,

$$\mu(\Delta,\theta) \le [\Delta : \Delta \cap S \cdot Z]\mu(\Delta \cap S \cdot Z,\theta) \le 2^{\dim \mathbf{H}}\mu(\Delta \cap S \cdot Z,\theta) \le 4^{\mathrm{rd}_p(\Gamma)}\mu(\Delta \cap S \cdot Z,\theta).$$

Let $\varphi : S \times Z \longrightarrow H(\mathbb{F}_p)$ be the multiplication map. φ is equivariant if we use the involution $\theta \times \theta$ on $S \times Z$. By Lemma 8.0.2(1),

$$\mu(\Delta \cap S \cdot Z,\theta) \le \mu(\varphi^{-1}(\Delta),\theta \times \theta).$$

Since $S \subset \Delta$, we get that $\varphi^{-1}(\Delta) = S \times A$, for some $A \subset Z$. Therefore, by Lemma 8.0.4,

$$\mu(\varphi^{-1}(\Delta),\theta \times \theta) \le \mu(S,\theta).$$

Finally, by Lemma 3.1.6,

$$\mu(S,\theta) \le \left[\mathbf{H}'(\mathbb{F}_p) : S\right]\mu(\mathbf{H}'(\mathbb{F}_p),t) \le 2^{\dim(\mathbf{H}')}\mu(\mathbf{H}'(\mathbb{F}_p),t) \le 4^{\mathrm{rd}_p(\Gamma)}\mu(\mathbf{H}'(\mathbb{F}_p),t),$$

and the result follows from Theorem 8.0.1. □

9. Clifford theory

We recall the elements of Clifford theory. The following lemma is standard.

Lemma 9.0.1. *Let Γ be a finite group, let ρ be an irreducible representation of Γ and let $N \lhd \Gamma$ be a normal subgroup of Γ. Let τ be an irreducible subrepresentation of $\rho\restriction_N$ and let σ be the τ-isotypic component of $\rho\restriction_N$. Let $\Delta := \Gamma_\tau$ be the stabilizer of $\tau \in \mathrm{Irr}(N)$ with respect to the adjoint action. Then σ is Δ-invariant and*

$$\rho \cong \mathrm{ind}_\Delta^\Gamma \sigma.$$

Lemma 9.0.2. *Let Γ be a finite group, let ρ be an irreducible representation of Γ and let $N \lhd \Gamma$ be a normal p-subgroup of Γ, and $\rho \in \mathrm{Irr}(\Gamma)$. Assume that $\rho\restriction_N$ is isotypic and that $H^2(\Gamma/N, \mu_{p^\infty})$ is trivial.*

Then there exist $\pi_1, \pi_2 \in \mathrm{Irr}(\Gamma)$ such that $\pi_1\restriction_N$ is irreducible, the action of N on π_2 is trivial, and $\rho \simeq \pi_1 \otimes \pi_2$.

Proof. Write $\rho\restriction_N = \tau^{\oplus C}$, where $(\tau, V) \in Irr(N)$. Recall the construction of the 2-cocycle corresponding to the triple (Γ, N, τ): choose a set of coset representatives $T \subset \Gamma$ such that $1 \in T$. For every $t \in T \setminus \{1\}$, choose an isomorphism $A_t : \tau^t \longrightarrow \tau$ such that $\det(A_t) = 1$, and let $A_1 = I$.

Define a map $\pi : \Gamma \longrightarrow \mathrm{End}_{\mathbb{C}}(V)$ by $\pi(tn) = A_t\tau(n)$ for $t \in T$ and $n \in N$. This is a projective representation of Γ that extands τ and satisfies $\pi(tn) = \pi(t)\pi(n)$ and

$$\pi(nt) = \pi(tt^{-1}nt) = A_t\tau(t^{-1}nt) = A_t\tau^t(n) = \tau(n)A_t = \pi(n)\pi(t).$$

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

For every $\gamma_1, \gamma_2 \in \Gamma$, the map

$$\pi(\gamma_2^{-1})\pi(\gamma_1^{-1})\pi(\gamma_1\gamma_2)$$

is an intertwiner of τ, so

$$\pi(\gamma_2^{-1})\pi(\gamma_1^{-1})\pi(\gamma_1\gamma_2) = \alpha(\gamma_1, \gamma_2)I,$$

for some $\alpha(\gamma_1, \gamma_2) \in \mathbb{C}^\times$. The map $\alpha : \Gamma \times \Gamma \to \mathbb{C}^\times$ is a 2-cocycle of Γ with coefficients in $\mathbb{C}^\times$, and a simple computation shows that α descends to a 2-cocycle on Γ/N. Since N is a p-group, $\det(\tau(n)) \in \mu_{p^\infty}$, for every $n \in N$. Since $\det(A_t) = 1$, for every $t \in T$, we get that $\alpha(\gamma_1, \gamma_2)^{\dim \tau} \in \mu_{p^\infty}$. Since $\dim \tau$ is a p-th power, we get that $\alpha(\gamma_1, \gamma_2) \in \mu_{p^\infty}$.

By assumption, this implies that α is cohomologous to the trivial cocycle, and, therefore, there is a representation τ_1 of Γ such that $\tau_1 \restriction_N = \tau$. Since τ is irreducible, so is τ_1. By [Isa06, Corollary 6.17], $\rho = \tau_1 \otimes \tau_2$, for some $\tau_2 \in \mathrm{Irr}(\Gamma/N)$. □

10. Proof of the main theorem

In this section, we prove Theorem c and deduce Theorem A and Corollary B.

Lemma 10.0.1 the main theorem for product case. *Let C_{nr} be the increasing function given by Corollary 8.0.5. Then, for every*

- *prime $p > 2$,*
- *symmetric pair of finite groups (Γ, Γ^θ),*
- *$\rho_1 \in \mathrm{Irr}(\Gamma)$ such that $\rho_1|_{\mathrm{Rad}_p(\Gamma)}$ is irreducible,*
- *$\rho_2 \in \mathrm{Irr}(\Gamma)$ that factors through $\Gamma/\mathrm{Rad}_p(\Gamma)$,*

we have

$$\dim\left((\rho_1 \otimes \rho_2)^{\Gamma^\theta}\right) < C_{nr}(\overline{\mathrm{rd}}(\Gamma)).$$

Proof. Since odd order symmetric pairs are Gelfand pairs (Corollary 5.0.5(1)), we have

$$\dim \rho_1^{Rad_p(\Gamma)^\theta} \leq 1.$$

If $(\rho_1 \otimes \rho_2)^{\Gamma^\theta} = 0$, the claim trivially holds. Otherwise, let χ be the character with which $\Gamma^\theta/Rad_p(\Gamma)^\theta$ acts on $\rho_1^{Rad_p(\Gamma)^\theta}$. Using Corollary 8.0.5,

$$\dim(\rho_1 \otimes \rho_2)^{\Gamma^\theta} = \dim(\chi \otimes \rho_2)^{\Gamma^\theta/Rad_p(\Gamma)^\theta} \leq \mu(\Gamma/Rad_p(\Gamma)) \leq C_{nr}(\mathrm{rd}(\Gamma/Rad_p(\Gamma))) \leq C_{nr}(\overline{\mathrm{rd}}(\Gamma)).$$

□

Using Clifford theory, the last lemma implies the following:

Corollary 10.0.2. *There is an increasing function $C_{\nu'} : \mathbb{N} \to \mathbb{N}$ such that, for every prime $p > 2$ and any finite group Γ, we have*

$$\nu'_p(\Gamma) < C_{\nu'}(\overline{\mathrm{rd}}_p(\Gamma)),$$

where ν'_p is the function defined in Notations 2.2.4.

Proof. Define $C_{\nu'}(n) = \max((C_{H2}(n) + 1)^n, C_{nr}(n))$. We will prove the corollary by analyzing two cases:

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

Case 1. $p \le C_{H2}(\overline{\mathrm{rd}}(\Gamma))$.
In this case,

$$|\Gamma/Rad_p(\Gamma)| \le (p+1)^{\overline{\mathrm{rd}}(\Gamma)} \le (C_{H2}(\overline{\mathrm{rd}}(\Gamma))+1)^{\overline{\mathrm{rd}}(\Gamma)} \le C_{\nu'}(\overline{\mathrm{rd}}(\Gamma)).$$

Since we can control multiplicities when we pass to subgroup of bounded index (Lemma 8.0.2), we get that

$$\nu(\Gamma) \le |\Gamma/Rad_p(\Gamma)| \cdot \nu(Rad_p(\Gamma)).$$

Since odd order symmetric pairs are Gelfand pairs (Corollary 5.0.5(1)), we have that

$$\nu(Rad_p(\Gamma)) = 1.$$

We obtain

$$\nu'_p(\Gamma) \le \nu(\Gamma) \le \#(\Gamma/Rad_p(\Gamma)) \le C_{\nu'}(\overline{\mathrm{rd}}(\Gamma))$$

Case 2. $p > C_{H2}(\overline{\mathrm{rd}}(\Gamma))$.
By Proposition 7.0.2, the group $H^2(\Gamma, \mu_{p^\infty})$ is trivial. Let $\rho \in \mathrm{Irr}(\Gamma)$ be such that $\rho|_{Rad_p(\Gamma)}$ is isotypic. By Clifford theory (Lemma 9.0.2), there exist $\pi_1, \pi_2 \in \mathrm{Irr}(\Gamma)$ such that $\pi_1|_{Rad_p(\Gamma)}$ is irreducible, the action of $Rad_p(\Gamma)$ on π_2 is trivial and $\rho \simeq \pi_1 \otimes \pi_2$. Thus, the main theorem for product case (Lemma 10.0.1) implies that, for any involution θ of Γ, we have

$$\rho^{\Gamma^\theta} = (\pi_1 \otimes \pi_2)^{\Gamma^\theta} \le C_{nr}(\overline{\mathrm{rd}}(\Gamma)) \le C_{\nu'}(\overline{\mathrm{rd}}(\Gamma)). \qquad \square$$

We are now ready to prove the main theorem:

Proof of Theorem 2.3.1. Define C recursively by

1. $C(0) := 1$
2. $C(n) := C^{her}_{H1}(n)\max(C_{\nu'}(n), C(n-1)C_{mon}(n))$,

where C^{her}_{H1} is given by Corollary 6.0.6, $C_{\nu'}$ is given by Corollary 10.0.2 and C_{mon} is given by Corollary 4.1.2. We will prove the theorem by induction. We assume the theorem holds if $\overline{\mathrm{rd}}_p(\Gamma) < n$ and prove it in the case $\overline{\mathrm{rd}}(\Gamma) = n$.

Let θ be an involution of Γ and $\rho \in \mathrm{Irr}\,\Gamma$. Let $N := Rad_p(\Gamma)$. If $(\rho|_N)^{N^\theta} = 0$, we are done. Otherwise, let τ be an irreducible direct summand of $\rho|_N$ such that $(\tau)^{N^\theta} \neq 0$. By the Lapid–Prasad property for symmetric pairs of odd order (Corollary 5.0.5(2)), we have $(\tau)^\theta \cong \tau^*$. Let $\Delta := \Gamma_\tau$. We have

$$\theta(\Delta) = \Gamma_{\tau^\theta} = \Gamma_{\tau^*} = \Gamma_\tau = \Delta,$$

showing that Δ is θ-stable.

By Clifford theory (Lemma 9.0.1), we have

$$\rho = ind_\Delta^\Gamma(\sigma),$$

where $\sigma \in \mathrm{Irr}(\Delta)$ is such that $\sigma|_N$ is τ-isotypic. Therefore,

$$\rho^{\Gamma^\theta} = (ind_\Delta^\Gamma(\sigma))^H = \oplus_{[g]\in\Delta\backslash\Gamma/\Gamma^\theta}\sigma^{\Delta\cap(\Gamma^\theta)^g} = \oplus_{[g]\in\Delta\backslash\Gamma^{dis}/\Gamma^\theta}\sigma^{\Delta\cap(\Gamma^\theta)^g}, \tag{2}$$

where

$$\Gamma^{dis} = \{g \in \Gamma | \sigma^{\Delta \cap (\Gamma^\theta)^g} \neq 0\} \subset \{g \in \Gamma | \sigma^{N \cap (\Gamma^\theta)^g} \neq 0\} = \{g \in \Gamma | \tau^{N \cap (\Gamma^\theta)^g} \neq 0\} =$$
$$= \{g \in \Gamma | (\tau^g)^{N \cap (\Gamma^\theta)} \neq 0\} = \{g \in \Gamma | (\tau^g)^{N^\theta} \neq 0\} \subset \{g \in \Gamma | (\tau^g)^* \circ \theta \simeq \tau^g\} =: \Gamma^{inv}.$$

The last inclution is by the Lapid-Prasad property for symmetric pairs of odd order (Corollary 5.0.5(2)).

We analyze the quotient $\Delta \backslash \Gamma^{inv} / \Gamma^\theta$. Since $(\tau^g)^* \circ \theta = (\tau^* \circ \theta)^{\theta(g)} = \tau^{\theta(g)}$, we have

$$\Gamma^{inv} = \{g \in \Gamma | \tau^{\theta(g)} \simeq \tau^g\} = \{g | \tau^{g\theta(g^{-1})} \simeq \tau\} = \{g | g\theta(g^{-1}) \in \Delta\}.$$

Thus, for any $g \in \Gamma^{inv}$, we have

$$\theta(ad(g^{-1})(\Delta)) = ad(\theta(g^{-1}))(\Delta) = ad(g^{-1} g\theta(g^{-1}))(\Delta) = ad(g^{-1})(\Delta),$$

and hence, $ad(g^{-1})(\Delta)$ is θ-stable.

We also have

$$\Gamma^{inv} / \Gamma^\theta = \{g\theta g^{-1} \in \Delta | g \in \Gamma\},$$

and thus,

$$\Delta \backslash \Gamma^{inv} / \Gamma^\theta = Ker(H^1(S_2, \Delta) \to H^1(S_2, \Gamma)).$$

Combining the last equality with (2), we get

$$\begin{aligned}
\dim \rho^{\Gamma^\theta} &\leq |H^1(S_2, \Delta)| \max_{g \in \Gamma^{inv}} \dim \sigma^{\Delta \cap (\Gamma^\theta)^g} \\
&= |H^1(S_2, \Delta)| \max_{g \in \Gamma^{inv}} \dim(\sigma \circ ad(g))^{(ad(g^{-1})(\Delta)) \cap \Gamma^\theta} \\
&= |H^1(S_2, \Delta)| \max_{g \in \Gamma^{inv}} \dim(\sigma \circ ad(g))^{(ad(g^{-1})(\Delta))^\theta} \\
&= |H^1(S_2, \Delta)| \max_{g \in \Gamma^{inv}} \dim \sigma^{\Delta^{ad(g) \circ \theta \circ ad(g^{-1})}} \\
&\leq |H^1(S_2, \Delta)| \max_{\theta' \text{ is an involution of } \Delta} (\dim(\sigma^{\Delta^{\theta'}})).
\end{aligned}$$

By our bound on $H^1(S_2, \Delta)$ (Corollary 6.0.6),

$$\dim \rho^{\Gamma^\theta} \leq C^{her}_{H1}(\overline{\mathrm{rd}}_p(\Gamma)) \max_{\theta' \text{ is an involution of } \Delta} (\dim(\sigma^{\Delta^{\theta'}})). \tag{3}$$

We finish the proof by analyzing the following cases:

Case 1. $\mathrm{Rad}_p(\Gamma) \neq \mathrm{Rad}_p(\Delta)$:

In order to bound $\nu(\Delta)$, we fix an involution θ' of Δ. By Corollary 4.1.2, we can find a θ'-invariant subgroup $\Delta^\circ \lhd \Delta$ such that

$$\overline{\mathrm{rd}}_p(\Delta^\circ) < \overline{\mathrm{rd}}_p(\Gamma)$$

and

$$[\Delta : \Delta^\circ] \leq C_{mon}(\overline{\mathrm{rd}}_p(\Gamma)).$$

The induction assumption implies that $\nu(\Delta^\circ) \leq C(\overline{\mathrm{rd}}_p(\Gamma) - 1)$. Lemma 8.0.2(2) implies that

$$\nu(\Delta, \theta') \leq [\Delta : \Delta^\circ] \cdot \nu(\Delta^\circ, \theta'|_{\Delta^\circ}) \leq C_{mon}(\overline{\mathrm{rd}}_p(\Gamma))C(\overline{\mathrm{rd}}_p(\Gamma) - 1),$$

so

$$\nu(\Delta) \leq C_{mon}(\overline{\mathrm{rd}}_p(\Gamma))C(\overline{\mathrm{rd}}_p(\Gamma) - 1).$$

It follows that

$$\dim \rho^{\Gamma^\theta} \leq C_{H1}^{her}(\overline{\mathrm{rd}}_p(\Gamma)) \cdot C_{mon}(\overline{\mathrm{rd}}_p(\Gamma))C(\overline{\mathrm{rd}}_p(\Gamma) - 1) \leq C(\overline{\mathrm{rd}}_p(\Gamma)),$$

as required.

Case 2. $\mathrm{Rad}_p(\Gamma) = \mathrm{Rad}_p(\Delta)$.
In this case, $\overline{\mathrm{rd}}_p(\Delta) \leq \overline{\mathrm{rd}}_p(\Gamma)$, and $\sigma|_{\mathrm{Rad}_p(\Delta)}$ is isotypic. By (3) and Corollary 10.0.2,

$$\begin{aligned}\dim \rho^{\Gamma^\theta} &\leq C_{H1}^{her}(\overline{\mathrm{rd}}_p(\Gamma)) \cdot \nu'(\Delta) \\ &\leq C_{H1}^{her}(\overline{\mathrm{rd}}_p(\Gamma))C_{\nu'}(\overline{\mathrm{rd}}_p(\Delta)) \\ &\leq C_{H1}^{her}(\overline{\mathrm{rd}}_p(\Gamma))C_{\nu'}(\overline{\mathrm{rd}}_p(\Gamma)) \leq C(\overline{\mathrm{rd}}_p(\Gamma)).\end{aligned}$$

□

10.1. Deduction of Theorem A, Corollary B and Corollary D

We will now deduce Theorem A from our main result, first reminding its formulation.

Theorem A. *There is an increasing function $C^{fin} : \mathbb{N} \to \mathbb{N}$ such that, for any*

- *odd prime p,*
- *positive integer d,*
- *finite group Γ,*
- *normal p-subgroup $N \lhd \Gamma$,*
- *an embedding $\Gamma/N \hookrightarrow GL_d(\mathbb{F}_p)$,*
- *an involution θ of Γ,*
- *an irreducible representation ρ of Γ,*

we have $\dim \rho^{\Gamma^\theta} \leq C^{fin}(d)$.

Proof. Set

$$C^{fin}(d) := C_{mon}(d^2)C(d^2).$$

By Corollary 4.1.2, we have a subgroup $\Delta \lhd \Gamma/N$ such that

$$\overline{\mathrm{rd}}(\Delta) \leq \overline{\mathrm{rd}}(GL_d(\mathbb{F}_p)) = d^2$$

and

$$[\Gamma/N : \Delta] \leq C_{mon}(\overline{\mathrm{rd}}(GL_d(\mathbb{F}_p))) = C_{mon}(d^2).$$

Let Γ° be the preimage of Δ under the projection $\Gamma \to \Gamma/N$. We have

$$\overline{\mathrm{rd}}(\Gamma^\circ) = \overline{\mathrm{rd}}(\Delta) \leq d^2.$$

By the main theorem (Theorem 2.3.1),

$$\nu(\Gamma^\circ) \leq C(d^2).$$

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

Lemma 8.0.2(2) implies that

$$\nu(\Gamma) = [\Gamma : \Gamma^\circ]\nu(\Gamma^\circ) = [\Gamma/N : \Delta]\nu(\Gamma^\circ) \leq C_{mon}(d^2)C(d^2) = C^{fin}(d). \qquad \square$$

Proof of Corollary B. Set $\Lambda = C^{fin}(C^{lin}(d))$, where C^{lin} is the function given by Lemma 3.2.2.

Let $\psi : \mathbf{G} \to \mathbf{R}$ be the reductive quotient of $\mathbf{G}$ and let $\varphi : \mathbf{R} \to GL_{C^{lin}(d),F}$ be the embedding given by Lemma 3.2.2. The group $\varphi \circ \psi(K)$ is a compact subgroup of $GL_{C^{lin}(d)}(F)$ and, after conjugation, we may assume that $\varphi \circ \psi(K) \subset GL_{C^{lin}(d)}(O_F)$. Let $K_1 \subset GL_{C^{lin}(d)}(O_F)$ be the first congruence subgroup.

Set $M := K \cap (\varphi \circ \psi)^{-1}(K_1)$, $L := M \cap \ker \rho$, and $P := L \cap \theta(L)$. The claim now follows by applying Theorem A to $\Gamma := K/P$, $N := M/P$, and the embedding $\Gamma/N = K/M \hookrightarrow \mathrm{GL}_{C^{lin}(d)}(O_F)/K_1 = \mathrm{GL}_{C^{lin}(d)}(\mathbb{F}_p)$. $\square$

Proof of Corollary D. There is a constant $C = C(\mathbf{G}, \theta)$ such that, for every prime p, the number of connected components of $\mathbf{G}^\theta \times \mathrm{Spec}(\overline{\mathbb{F}_p})$ is at most C. We claim that, for every p, the set $\mathbf{X}(\mathbb{Z}_p)$ is a union of at most C $\mathbf{G}(\mathbb{Z}_p)$-orbits. Corollary D follows from

- The claim.
- The fact that each $\mathbf{G}(\mathbb{Z}_p)$-orbit has the form $\mathbf{G}(\mathbb{Z}_p)/\mathbf{G}(\mathbb{Z}_p)^{\theta_i}$, for some involutions θ_i of $\mathbf{G}(\mathbb{Z}_p)$.
- $\dim \mathrm{Hom}\big(\rho, C^\infty(\mathbf{G}(O)/\mathbf{G}(O)^{\theta_i})\big) = \dim \rho^{\mathbf{G}(O)^{\theta_i}}$.
- Corollary B.

It remains to prove the claim. For this, it is enough to show that, for every prime p and every natural number n, the number of $\mathbf{G}(\mathbb{Z}/p^n)$-orbits in $\mathbf{X}(\mathbb{Z}/p^n)$ is bounded by C. Recall that the Greenberg functor is a functor from the category of $\mathbb{Z}/p^n$-schemes to the category of $\mathbb{F}_p$-schemes that satisfies that $Gr_n(X)(\mathbb{F}_p) = X(\mathbb{Z}/p^n)$. There is a natural transformation $Gr_n(X) \to X \times \mathrm{Spec}(\mathbb{F}_p)$. For the definition of the Greenberg functor, see, for example, [BLR90, pp. 276].

From the long exact sequence of Galois cohomologies of $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ with coefficients in $Gr_n(\mathbf{G}^\theta)$, $Gr_n(\mathbf{G})$ and $Gr_n(\mathbf{X})$ (see, for example, [Ser02, §5.4, Corollary 1]), the orbit space of $Gr_n(\mathbf{X})(\mathbb{F}_p) = \mathbf{X}(\mathbb{Z}/p^n)$ under $Gr_n(\mathbf{G})(\mathbb{F}_p) = \mathbf{G}(\mathbb{Z}/p^n)$ embeds into $H^1(\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p), Gr_n(\mathbf{G}^\theta))$. The kernel of $\pi : Gr_n(\mathbf{G}^\theta) \to \mathbf{G}^\theta \times \mathrm{Spec}(\mathbb{F}_p)$ is an iterated extension of additive groups, so it is absolutely connected. By Lang's theorem and the long exact sequence of Galois cohomologies with coefficients in $\ker(\pi)$, $Gr_n(\mathbf{G}^\theta)$ and $\mathbf{G}^\theta \times \mathrm{Spec}(\mathbb{F}_p)$, the set $H^1\Big(\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p), Gr_n(\mathbf{G}^\theta)\Big)$ embeds into $H^1\Big(\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p), \mathbf{G}^\theta \times \mathrm{Spec}(\mathbb{F}_p)\Big)$ which itself embeds into $H^1\Big(\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p), \pi_0(\mathbf{G}^\theta)\Big)$. Since $\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p)$ is pro-cyclic, a 1-cocycle is determined by its value at a topological generator, so $H^1\Big(\mathrm{Gal}(\overline{\mathbb{F}_p}/\mathbb{F}_p), \pi_0(\mathbf{G}^\theta)\Big) \leq |\pi_0(\mathbf{G}^\theta)(\overline{\mathbb{F}_p})| \leq C$. $\square$

A. Bounds on twisted multiplicities for spherical spaces of finite groups of Lie type

In this appendix, we prove the following:

Theorem A.0.1. *Let $\mathcal{S}$ be a scheme of finite type, let $\mathcal{G} \to \mathcal{S}$ be a connected reductive group scheme of finite type over $\mathcal{S}$ and let $\mathcal{H} \subseteq \mathcal{G}$ be a closed (not necessarily connected) reductive subgroup scheme. Assume that, for every geometric point s of $\mathcal{S}$, the pair $(\mathcal{G}_s, \mathcal{H}_s)$ is spherical. Then there is a constant C such that, for every finite field F, any $s \in \mathcal{S}(F)$, any irreducible representation ρ of $\mathcal{G}_s(F)$ and any 1-dimensional character θ of $\mathcal{H}_s(F)$,*

$$\dim \mathrm{Hom}_{\mathcal{G}_s(F)}\Big(\rho, \mathrm{Ind}_{\mathcal{H}_s(F)}^{\mathcal{G}_s(F)} \theta\Big) < C.$$

The proof is very similar to the one in [She]. The main additional ingredient is the geometrization of (1-dimensional) characters of finite groups of Lie type.

Given a Weil $\overline{\mathbb{Q}_\ell}$-local system $\mathfrak{L}$ on a scheme X over a finite field F, the sheaf to function correspondence gives a function $X(F) \to \overline{\mathbb{Q}_\ell}$ which we denote by $\chi_{\mathfrak{L}}$.

Lemma A.0.2. *Let $\mathcal{S}$ be a scheme of finite type and let $\mathcal{H} \to \mathcal{S}$ be a (not necessarily connected) reductive group scheme of finite type over $\mathcal{S}$. There is a constant C such that, for every finite field F of size greater then 9, any prime $\ell \neq char(F)$, any $s \in \mathcal{S}(F)$ and any 1-dimensional character $\chi : \mathcal{H}_s(F) \to \overline{\mathbb{Q}_\ell}$, there is a $\overline{\mathbb{Q}_\ell}$-local system $\mathfrak{L}$ over $\mathcal{H}_s$ with a Weil structure of pure weight zero such that $\chi_{\mathfrak{L}}$ is a character of a representation of $\mathcal{H}_s(F)$ of dimension at most C that contains χ as one of its irreducible constituents.*

Proof. For every (not necessarily connected) reductive group $\mathbf{G}$ defined over a field F, let $(\mathbf{G}^\circ)'$ be the derived subgroup of the connected component of $\mathbf{G}$ and let $\widetilde{\mathbf{G}}$ be the the product of the universal cover of $(\mathbf{G}^\circ)'$ and the radical of $\mathbf{G}$. The map $\widetilde{\mathbf{G}}(\bar{F}) \to \mathbf{G}(\bar{F})$ has finite kernel and cokernel.

By a stratification argument, there is a constant c such that, for every field F, any $s \in \mathcal{S}(F)$, the kernel and cokernel of the map $\widetilde{\mathcal{H}_s}(\bar{F}) \to \mathcal{H}_s(\bar{F})$ are bounded by c. By Lemma 3.1.5, if F is a finite field, the kernel and cokernel of the map $\widetilde{\mathcal{H}_s}(F) \to \mathcal{H}_s(F)$ are bounded by c^2. We will show that the lemma holds with $C = c^4$.

Given F, ℓ, s, χ as in the lemma, denote the map $\widetilde{\mathcal{H}_s} \to \mathcal{H}_s$ by φ. Let $R(\mathcal{H}_s)$ be the radical of $\mathcal{H}_s$. By [Lus85, §5], there is a 1-dimensional local system $\mathcal{F}$ on $R(\mathcal{H}_s)$ such that $\chi_{\mathcal{F}} = \chi \restriction_{R(\mathcal{H}_s)}$.

By Theorem 3.1.1(3), the character $\chi \circ \varphi \restriction_{\widetilde{\mathcal{H}'_s}(F)}$ is trivial. Therefore, under the decomposition $\widetilde{\mathcal{H}_s} = \widetilde{\mathcal{H}'_s} \times R(\mathcal{H}_s)$, we have

$$\chi \circ \varphi = 1_{\widetilde{\mathcal{H}'_s}(\mathbb{F}_p)} \boxtimes \chi \restriction_{R(\mathcal{H}_s)} = 1_{\widetilde{\mathcal{H}'_s}(\mathbb{F}_p)} \boxtimes \chi_{\mathcal{F}} = \chi_{\mathbb{1}_{\widetilde{\mathcal{H}'_s}} \boxtimes \mathcal{F}},$$

where $\mathbb{1}_{\widetilde{\mathcal{H}'_s}}$ denotes the 1-dimensional trivial local system on $\widetilde{\mathcal{H}'_s}$

Setting $\mathfrak{M} = \varphi_!(\mathbb{1}_{\widetilde{\mathcal{H}'_s}} \boxtimes \mathcal{F})$, the function $\chi_{\mathfrak{M}}$ is equal to $\varphi_*(\chi \circ \varphi)$. It follows that the restrictions of $\chi_{\mathfrak{M}}$ and $|\ker \varphi(F)|\chi$ to $\varphi(\widetilde{\mathcal{H}_s}(F))$ coincide. Choose coset representatives $g_1, \dots, g_c \in \mathcal{H}_s(F)$ to $\varphi(\widetilde{\mathcal{H}_s}(F))$ and let $\mathfrak{L} = \bigoplus \mathrm{Ad}(g_i)^*(\mathfrak{M})$. We have that

$$\chi_{\mathfrak{L}} = \mathrm{Ind}_{\varphi(\widetilde{\mathcal{H}_s}(F))}^{\mathcal{H}_s(F)} \chi_{\mathfrak{M}} \restriction_{\varphi(\widetilde{\mathcal{H}_s}(F))} = \mathrm{Ind}_{\varphi(\widetilde{\mathcal{H}_s}(F))^{\mathcal{H}_s(F)}} \mathrm{Res}_{\varphi(\widetilde{\mathcal{H}_s}(F))}^{\mathcal{H}_s(F)} |\ker \varphi(F)|\chi,$$

which implies the claim. □

Now we will continue with the original argument of [AA19, She], adapting it to include the character χ and its geometrization $\mathfrak{L}$.

Definition A.0.3. If $\mathbf{G}$ is an algebraic group acting on a variety $\mathbf{X}$, we let $\mathbf{X}_{\mathbf{G}} = \{(x, g) \in X \times \mathbf{G} \mid g \cdot x = x\}$.

Lemma A.0.4. *Let $\mathbf{G}, \mathbf{H}$ be reductive algebraic groups, let $\mathbf{X} = \mathbf{G}/\mathbf{H}$ and consider the diagram*

$$\begin{tikzcd} \mathbf{G} \times \mathbf{H} \arrow[r, "a"] \arrow[d, "p"] & \mathbf{X}_{\mathbf{G}} \\ \mathbf{H} & \end{tikzcd}$$

where $a(g, h) = (g\mathbf{H}, ghg^{-1})$ and $p(g, h) = h$. If $\mathfrak{L}$ is an $\mathbf{H}$-equivariant local system on $\mathbf{H}$, then there is a local system $\mathfrak{M}$ on X_G such that $a^*\mathfrak{M} \cong p^*\mathfrak{L}$.

Proof. We construct $\mathfrak{M}$ using descent. The main point is that $(\mathbf{G} \times \mathbf{H}) \times_{\mathbf{X}_{\mathbf{G}}} (\mathbf{G} \times \mathbf{H}) \cong \mathbf{G} \times \mathbf{H} \times \mathbf{H}$ via the map $((g_1, h_1), (g_2, h_2)) \mapsto (g_1, g_2^{-1} g_1, h_1)$. We get a diagram

$$\begin{tikzcd}
\mathbf{G}\times\mathbf{H}\times\mathbf{H} \arrow[r, shift left, "a_1"] \arrow[r, shift right, "a_2"'] \arrow[d, "p_2"] & \mathbf{G}\times\mathbf{H} \arrow[r, "a"] \arrow[d, "p_1"] & \mathbf{X_G} \\
\mathbf{H}\times\mathbf{H} \arrow[r, shift left, "b_1"] \arrow[r, shift right, "b_2"'] & \mathbf{H} &
\end{tikzcd}$$

where a_1, a_2, p_1, p_2 are the projections, $b_1(x, y) = x$ and $b_2(x, y) = xyx^{-1}$. We have $b_i p_2 = p_1 a_i$ for $i = 1, 2$. The equivariance of $\mathfrak{L}$ gives an identification $\alpha : b_1^*\mathfrak{L} \to b_2^*\mathfrak{L}$, which gives an identification $\beta : a_1^* p_1^* \mathfrak{L} = (b_1 p_2)^*\mathfrak{L} \to (b_2 p_2)^*\mathfrak{L} = a_2^* p_1^* \mathfrak{L}$, and it is easy to check that β satisfies the cocycle identity. By descent, $p_1^*\mathfrak{L}$ is the pullback of a sheaf $\mathfrak{M}$ on $\mathbf{X_G}$. Since a is onto, we get that $\mathfrak{M}$ is a local system. □

In the next lemma, we use the notion of induced character sheaf; see [AA19, Definition 2.2.1].

Lemma A.0.5. *Let $\mathcal{S}$ be a scheme of finite type, let $\mathcal{G} \to \mathcal{S}$ be a connected reductive group scheme of finite type over $\mathcal{S}$ and let $\mathcal{H} \subseteq \mathcal{G}$ be a closed (not necessarily connected) reductive subgroup scheme. Assume that, for every geometric point s of $\mathcal{S}$, the pair $(\mathcal{G}_s, \mathcal{H}_s)$ is spherical. There is a constant C_1 such that, for any finite field F, any $s \in \mathcal{S}(F)$, any induced character sheaf $\mathfrak{K}$ on $\mathcal{G}_s$ and any $\mathcal{H}_s$-equivariant local system $\mathfrak{L}$ on $\mathcal{H}_s$ of weight zero,* $\dim\operatorname{Hom}_{\mathcal{G}_s(F)}\left(\chi_{\mathfrak{K}}, \operatorname{Ind}_{\mathcal{H}_s(F)}^{\mathcal{G}_s(F)} \chi_{\mathfrak{L}}\right) < C_1 \cdot \operatorname{rk}\mathfrak{L}$.

Proof. For every geometric point s of $\mathcal{S}$, let Fl_s be the flag variety of $\mathcal{G}_s$. Let C_1 be such that, for every geometric point s of $\mathcal{S}$, the number of connected components of $(\mathcal{G}_s/\mathcal{H}_s \times \mathrm{Fl}_s)_{\mathcal{G}_s}$ is bounded by C_1.

Let $F, s, \mathfrak{K}, \mathfrak{L}$ be as in the lemma. Denote $\mathbf{G} = \mathcal{G}_s$, $\mathbf{H} = \mathcal{H}_s$, $\mathbf{X} = \mathbf{G}/\mathbf{H}$ and fix a Borel subgroup $\mathbf{B}$ of $\mathbf{G}$ defined over F. Consider the diagram

$$\begin{tikzcd}
 & (\mathbf{X}\times\mathbf{G}/\mathbf{B})_{\mathbf{G}} \arrow[dl, "\widetilde{\pi}"'] \arrow[dr, "\widetilde{f}"] \arrow[dd, "q"] & \\
\mathbf{X_G} \arrow[dr, "f"'] & & (\mathbf{G}/\mathbf{B})_{\mathbf{G}} \arrow[dl, "\pi"] \\
 & \mathbf{G} \arrow[d, "p"] & \\
 & \operatorname{Spec}(F) &
\end{tikzcd}$$

where $f, \pi, \widetilde{f}, \widetilde{\pi}$ are the projections and $q = \pi \circ \widetilde{f} = \widetilde{\pi} \circ f$.

By definition, there is a weight zero local system $\mathfrak{F}$ on $(\mathbf{G}/\mathbf{B})_{\mathbf{G}}$ such that $\mathfrak{K}$ is a direct summand of $R\pi_*\mathfrak{F}$. Applying Lemma A.0.4 to $\mathfrak{L}$, we get a local system $\mathfrak{M}$ on $\mathbf{X_G}$. Since $\mathfrak{L}$ has weight zero, so does $\mathfrak{M}$.

By construction, $\chi_{Rf_!\mathfrak{M}} = \operatorname{Ind}\chi_{\mathfrak{L}}$. Denoting the standard inner product of functions on $G(F)$ by $\langle -, - \rangle$, we get

$$\begin{aligned}
\dim\operatorname{Hom}_{\mathbf{G}(F)}\left(\chi_{\mathfrak{K}}, \operatorname{Ind}_{\mathbf{H}(F)}^{\mathbf{G}(F)} \chi_{\mathfrak{L}}\right) &= \left\langle \chi_{\mathfrak{K}}, \operatorname{Ind}_{\mathbf{H}(F)}^{\mathbf{G}(F)} \chi_{\mathfrak{L}} \right\rangle \\
&= \left\langle \chi_{\mathfrak{K}}, \chi_{f_!\mathfrak{M}} \right\rangle \\
&= \left\langle \chi_{\mathfrak{K}\otimes f_!\mathfrak{M}^\vee}, 1 \right\rangle = \operatorname{trace}\left(Fr_F \mid p_!(\mathfrak{K} \otimes f_!\mathfrak{M}^\vee)\right),
\end{aligned}$$

where Fr_F is induced by the Frobenius map of $\operatorname{Spec}(F)$.

For every n, denote the degree n extension of F by F_n and denote the pullbacks of $\mathfrak{L}, \mathfrak{K}$ to $\mathbf{G}_{F_n}, \mathbf{H}_{F_n}$ by $\mathfrak{L}_n, \mathfrak{K}_n$. From the same reasoning as before, we get

$$\dim\operatorname{Hom}_{\mathbf{G}(F_n)}\left(\chi_{\mathfrak{K}_n}, \operatorname{Ind}_{\mathbf{H}(F_n)}^{\mathbf{G}(F_n)} \chi_{\mathfrak{L}_n}\right) = \operatorname{trace}\left(Fr_F^n \mid p_!(\mathfrak{K} \otimes f_!\mathfrak{M}^\vee)\right).$$

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

The complex $p_!(\mathfrak{K} \otimes f_! \mathfrak{M}^\vee)$ is a direct summand of $p_!(\pi_! \mathfrak{F} \otimes f_! \mathfrak{M}^\vee)$. Since

$$\pi_! \widetilde{f}_! \left(\widetilde{f}^* \mathfrak{F} \otimes \widetilde{\pi}^* \mathfrak{M}^\vee \right) = \pi_! \left(\mathfrak{F} \otimes \widetilde{f}_! \widetilde{\pi}^* \mathfrak{M}^\vee \right) = \pi_! (\mathfrak{F} \otimes \pi^* f_! \mathfrak{M}^\vee) = \pi_! \mathfrak{F} \otimes f_! \mathfrak{M}^\vee,$$

we get that $p_!(\mathfrak{K} \otimes f_! \mathfrak{M}^\vee)$ is a direct summand of $p_! q_! \left(\widetilde{f}^* \mathfrak{F} \otimes \widetilde{\pi}^* \mathfrak{M}^\vee \right)$. Since $\widetilde{f}^* \mathfrak{F} \otimes \widetilde{\pi}^* \mathfrak{M}^\vee$ has weight zero, we get that the complex $p_!(\mathfrak{K} \otimes f_! \mathfrak{M}^\vee)$ has weight zero, is concentrated in degrees $0, \ldots, 2\dim(\mathbf{X} \times \mathbf{G}/\mathbf{B})_G = 2\dim \mathbf{G}$ and

$$\dim H^{2\dim \mathbf{G}} p_!(\mathfrak{K} \otimes f_! \mathfrak{M}^\vee) \leq \dim H^{2\dim \mathbf{G}} p_! q_! \left(\widetilde{f}^* \mathfrak{F} \otimes \widetilde{\pi}^* \mathfrak{M}^\vee \right) \leq c \operatorname{rk} \mathfrak{L}.$$

Thus,

$$\limsup_{n \to \infty} \operatorname{trace}\left(Fr_F^n \mid p_! \mathfrak{K} \otimes f_! \mathfrak{M}^\vee\right) \leq c \operatorname{rk} \mathfrak{L},$$

so, by [AA19, Lemma 2.4.1 and the proof of Theorem 2.1.3],

$$\dim \operatorname{Hom}_{\mathbf{G}(F)}\left(\chi_{\mathfrak{K}}, \operatorname{Ind}_{\mathbf{H}(F)}^{\mathbf{G}(F)} \chi_{\mathfrak{L}}\right) = \operatorname{trace}\left(Fr_F \mid p_! \mathfrak{K} \otimes f_! \mathfrak{M}^\vee\right) \leq c \operatorname{rk} \mathfrak{L} \qquad \square$$

Proposition A.0.6. *For any d, there are integers N, C such that, if*

1. *F is a finite field of size greater than N,*
2. *$\mathbf{G}$ is a reductive group defined over F of dimension at most d,*
3. *χ is an irreducible character of $\mathbf{G}(F)$,*

then there are induced character sheaves $\mathfrak{K}_1, \ldots, \mathfrak{K}_C$ and real numbers $\alpha_1, \ldots, \alpha_C \in [-C, C]$ such that $\sum \alpha_i \chi_{\mathfrak{K}_i} - \chi$ is a non-negative combination of irreducible characters of $\mathbf{G}(F)$.

Proof. [She, Lemma A.1, Theorem 2.2, Theorem 3.3] (the last two are due to Laumon and Lusztig). □

Proof of Theorem A.0.1. Without loss of generality, we may assume that $|F| > 9$. Let ρ be an irreducible representation of $G(F)$ and let θ be a character of $H(F)$. Let $C, \mathfrak{K}_i, \alpha_i$ be as in Lemma A.0.6 (applied to ρ) and let $\mathfrak{L}$ be as in Lemma A.0.2 (applied to θ). By Lemma A.0.5, we have

$$\dim \operatorname{Hom}(\rho, \operatorname{Ind} \theta) \leq \left\langle \sum \alpha_i \chi_{\mathfrak{K}_i}, \operatorname{Ind} \chi_{\mathfrak{L}} \right\rangle \leq \sum |\alpha_i| \cdot \left| \left\langle \chi_{\mathfrak{K}_i}, \operatorname{Ind} \chi_{\mathfrak{L}} \right\rangle \right| < C^2 \cdot C_1 \cdot C. \qquad \square$$

B. A versal family of symmetric pairs of reductive groups over finite fields

In this appendix, we prove Lemma 3.2.2 and construct a family of symmetric pairs of reductive groups that includes all symmetric pairs of reductive groups of a given dimension over all finite fields (Lemma 3.2.1).

B.1. Proof of Lemma 3.2.2

For the proof, we will need the following:

Lemma B.1.1. *There is an increasing function $C^{spt} : \mathbb{N} \to \mathbb{N}$ such that any reductive algebraic group $\mathbf{G}$ over an arbitrary field F splits over an extension F'/F of degree at most $C^{spt}(\dim \mathbf{G})$.*

Proof. Set $C^{spt}(d) := 3^{d^3}$.

There is a maximal torus of $\mathbf{G}$ that is defined over F ([ABD+64, XIV 1.1]), so we can assume that $\mathbf{G}$ is a torus. Denote $d = \dim \mathbf{G}$.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

Since $\mathbf{G}$ is an F-form of $\mathbb{G}_m^d$, we get a continuous homomorphism $\rho : \mathrm{Gal}_F \to \mathrm{Aut}(\mathbb{G}_m^d) = \mathrm{GL}_d(\mathbb{Z})$. The image of ρ is finite. Since the kernel of $\mathrm{GL}_d(\mathbb{Z}) \to \mathrm{GL}_d(\mathbb{Z}/3)$ is torsion-free, $\rho(\mathrm{Gal}_F)$ embeds in $\mathrm{GL}_d(\mathbb{Z}/3)$, so

$$|\rho(\mathrm{Gal}_F)| \leq |\,\mathrm{GL}_d(\mathbb{Z}/3)| < 3^{d^3} = C^{spt}(d). \qquad \square$$

Proof of Lemma 3.2.2. Since there are finitely many split reductive groups of given dimension, there is a function C^{linSpt} such that every split reductive group $\mathbf{H}$ has a faithful representation of dimension $C^{linSpt}(\dim \mathbf{H})$. Given an arbitrary reductive group $\mathbf{G}$, Lemma B.1.1 implies that $\mathbf{G}$ splits over an extension F'/F of degree at most $C^{spt}(\dim \mathbf{G})$. Hence, there is a faithful representation $\mathbf{G} \to \mathrm{Res}_{F'/F}\,\mathrm{GL}_{C^{linSpt}(\dim \mathbf{G})}$, so we can take $C^{lin}(n) = C^{linSpt}(n)C^{spt}(n)$. $\square$

B.2. Sketch of the proof of Lemma 3.2.1

We first show that there are finitely many root data of a given dimension (see Lemma B.3.1 below). Thus, we restrict our attention to a given root datum $\mathfrak{X}$. We denote by $\mathcal{G}$ the split reductive group scheme corresponding to $\mathfrak{X}$. By Lemma B.1.1, there is an integer k such that any reductive group of type $\mathfrak{X}$ over a finite field splits after passing to a field extension of degree k.

We then construct a finite etale map of schemes $\mathcal{E} \to \mathcal{F}$ that forms a family containing all degree k extensions of finite fields. This means that, for any degree k extension of finite fields E/F, we can find an F-point y of $\mathcal{F}$ whose fiber $\mathcal{E}_y$ is $\mathrm{Spec}\, E$. Moreover, we equip $\mathcal{E}$ with an action of the cyclic group C_k such that, if F is a finite field, we can find y as above such that the action of C_k on $\mathcal{E}_y$ is the Frobenius. See Lemma B.4.1 below.

By Lang's theorem, a reductive group of type $\mathfrak{X}$ over a finite field F that splits over a degree k extension E/F is determined by an action of C_k on $\mathfrak{X}$. We show that there are finitely may such actions up to conjugation (see Lemma B.3.2 below). Thus, we can fix one such an action ξ. We can also consider ξ as an action on $\mathcal{G}$.

At this point, we can construct a group scheme $\mathcal{H} \to \mathcal{F}$ containing all groups of type $(\mathfrak{X}, \xi)$ over finite fields. Namely, we first construct a group scheme $\mathcal{H}' \to \mathcal{F}$ whose fiber over $y \in \mathcal{F}(F)$ is the restriction of scalars of $\mathcal{G}_{\mathcal{E}_y}$ to F. Using the two actions of C_k on $\mathcal{E}$ and $\mathcal{G}$, we equip $\mathcal{H}'$ with an action of C_k. Finally, set $\mathcal{H} := (\mathcal{H}')^{C_k}$.

Next, we incorporate all possible involutions. We first note that, up to inner automorphisms, there are only finitely many involutions of $\mathfrak{X}$ commuting with the action of C_k (see Lemma B.3.2 below). Thus, we can restrict our attention to a specific such involution η. We then construct an $\mathcal{F}$-scheme $\mathcal{S}$ whose F-points are pairs (y, t) consisting of a point $y \in \mathcal{F}(F)$ and an involution t of $\mathcal{G}_{\mathcal{E}_y}$ which commutes with ξ and is of outer class η.

Finally, we pull back the group schemes $\mathcal{H}'$ and $\mathcal{H}$ to $\mathcal{S}$ and denote the resulting groups schemes $\mathcal{R}'$ and $\mathcal{R}$. Both $\mathcal{R}$ and $\mathcal{R}'$ are equipped with a natural involution τ. The group scheme $\mathcal{R} \to \mathcal{S}$ with the involution τ gives the required family.

Remark B.2.1. In the proof, below we skip $\mathcal{H}, \mathcal{H}'$ and construct $\mathcal{R}, \mathcal{R}'$ directly.

B.3. Some preparations

Lemma B.3.1. *For any integer $n > 0$, there is a finite number of isomorphism classes of complex connected reductive groups of dimension n.*

Proof. Fix a complex connected reductive group $\mathbf{G}$. Let $\tilde{\mathbf{G}}'$ be the universal cover of its derived group, let $Z^0(\mathbf{G})$ be the connected component of the center of $\mathbf{G}$ and let Γ be the kernel of the multiplication map $\tilde{\mathbf{G}}' \times Z^0(\mathbf{G}) \to \mathbf{G}$.

Let $Z(\tilde{\mathbf{G}}')$ be the center of $\tilde{\mathbf{G}}'$. Note that $Z(\tilde{\mathbf{G}}')$ is finite, that $\Gamma \subset Z(\tilde{\mathbf{G}}') \times Z^0(\mathbf{G})$ and that $\Gamma \cap Z^0(\mathbf{G})$ is trivial. Thus, Γ is a graph of a morphism from subgroup of $Z(\tilde{\mathbf{G}}')$ to $Z^0(\mathbf{G})$. This implies that

$\Gamma < Z(\tilde{\mathbf{G}}') \times Z^0(\mathbf{G})[|Z(\tilde{\mathbf{G}}')|]$, where for an integer k, the group $Z^0(\mathbf{G})[k]$ is the subgroup of elements of order dividing k in $Z^0(\mathbf{G})$.

Any complex connected reductive group $\mathbf{G}$ is uniquely determined (up to isomorphism) by the following:

- the simply conected semi-simple complex group $\tilde{\mathbf{G}}'$.
- the complex algebraic torus $Z^0(\mathbf{G})$.
- the finite subgroup $\Gamma < Z(\tilde{\mathbf{G}}') \times Z^0(\mathbf{G})[|Z(\tilde{\mathbf{G}}')|]$.

Since each of those has only finitely many options given the dimension of $\mathbf{G}$, the claim follows. □

Lemma B.3.2. *For any complex connected reductive group* $\mathbf{G}$ *and any finite abelian group* A*,*

$$\#Mor(A, Out(\mathbf{G}))/Ad(Out(\mathbf{G})) < \infty.$$

Proof. Any automorphism of $\mathbf{G}$ is determined by its restrictions to the derived subgroup $\mathbf{G}'$ and to the connected component $Z^0(\mathbf{G})$ of the center. We first claim that the map $\mathrm{Aut}(\mathbf{G}) \to \mathrm{Aut}(Z^0(\mathbf{G})) \times Aut(\mathbf{G}')$ has finite cokernel. Indeed, let $\mathbf{K}$ be the kernel of the map $\mathbf{G}' \times Z^0(\mathbf{G}) \to \mathbf{G}$. The group $\mathbf{K}$ is finite. Let $\mathbf{M} \subset \mathbf{G}' \times Z^0(\mathbf{G})$ be the product of the center $Z(\mathbf{G}')$ and the finite group of elements of $Z^0(\mathbf{G})$ of order dividing $|\mathbf{K}|$. The group $\mathbf{M}$ is finite, contains $\mathbf{K}$ and is characteristic in $\mathbf{G}' \times Z^0(\mathbf{G})$. It follows that the subgroup of $\mathrm{Aut}(Z^0(\mathbf{G})) \times Aut(\mathbf{G}')$ fixing $\mathbf{K}$ has finite index. Any element in this subgroup extends to an automorphism of $\mathbf{G}$.

Let ϕ be the composition $Aut(\mathbf{G}) \to Aut(Z^0(\mathbf{G})) \times Aut(\mathbf{G}') \to Aut(Z^0(\mathbf{G})) \times Out(\mathbf{G}')$. By the paragraph above, the cokernel of ϕ is finite. Note also that the kernel of ϕ is the subgroup of inner automorphisms. In particular, we have an embedding $Out(\mathbf{G}) \to Aut(Z^0(\mathbf{G})) \times Out(\mathbf{G}')$ with a finite cokernel.

The group $Out(\mathbf{G}')$ is finite. Denote it by Γ. The group $Aut(Z^0(\mathbf{G}))$ is isomorphic to $GL_n(\mathbb{Z})$ for some integer n. We get

$$\begin{aligned}
|Mor(A, Out(\mathbf{G}))/Ad(Out(\mathbf{G}))| &\le |Mor(A, GL_n(\mathbb{Z}) \times \Gamma)/Ad(Out(\mathbf{G}))| \\
&\le [GL_n(\mathbb{Z}) \times \Gamma : Out(\mathbf{G})] \cdot |Mor(A, GL_n(\mathbb{Z}) \times \Gamma)/Ad(GL_n(\mathbb{Z}) \times \Gamma)| \\
&\le [GL_n(\mathbb{Z}) \times \Gamma : Out(\mathbf{G})] \cdot |\Gamma| \cdot |Mor(A, GL_n(\mathbb{Z}))/Ad(GL_n(\mathbb{Z}))|.
\end{aligned}$$

By [PR94, Theorem 4.3], $Mor(A, GL_n(\mathbb{Z}))/Ad(GL_n(\mathbb{Z}))$ is finite, proving the lemma. □

B.4. Construction of the family

Lemma B.4.1. *For any integer* $n > 0$*, there exists a finite etale morphism* $\Psi_n : \mathcal{E}_n \to \mathcal{F}_n$ *of schemes of finite type over* $\mathbb{Z}$ *with an action of* C_n *on* $\mathcal{E}_n$ *over* $\mathcal{F}_n$ *such that, for any degree* n *extension* E/F *of finite fields, there exists* $\nu : \operatorname{Spec} F \to \mathcal{F}_n$ *such that*

$$\operatorname{Spec}(E) \simeq \operatorname{Spec}(F) \times_{\mathcal{F}_n} \mathcal{E}_n$$

as a C_n*-scheme. Here, the action of* C_n *on* E *is the Galois action.*

Proof. For a unital ring A and an integer k, let $A_k[t]$ be the set of polynomials of degree $\le k$ and let $A'_k[t]$ be the set of monic polynomials of degree k. Denote the resultant of two polynomials $f(t), g(t)$ by $res_t(f, g)$. Let

$$\mathcal{F}_n(A) := \{(f, g) \in A'_n[t] \times A_{n-1}[t] \mid res_t(f, f') \in A^\times \text{ and } f \text{ divides } f \circ g \text{ and } g^{\circ n} - t\}$$

and let

$$\mathcal{E}_n(A) := \{(f, g, z) \in A'_n[t] \times A_{n-1}[t] \times A \mid (f, g) \in \mathcal{F}_n \text{ and } f(z) = 0\}.$$

Define an action of C_n on $\mathcal{E}_n(A)$ by

$$k \cdot (f, g, z) \mapsto (f, g, g^{\circ k}(z)).$$

By construction, the assignments $A \mapsto \mathcal{F}_n(A)$ and $A \mapsto \mathcal{E}_n(A)$ give rise to representable functors. We denote the representing schemes by $\mathcal{F}_n$ and $\mathcal{E}_n$. Similarly, the action of C_n on $\mathcal{E}_n(A)$ gives rise to an action of C_n on $\mathcal{E}_n$ over $\mathcal{F}_n$. Denote by $\Psi_n : \mathcal{E}_n \to \mathcal{F}_n$ the projection. The map Ψ_n is an etale map.

Suppose that E/F is a degree n extension of finite fields. Let $\alpha \in E$ be a generator and let $f \in F_n[t]$ be its (monic) minimal polynomial. Let $g \in F_{n-1}[t]$ be the polynomial of degree $< n$ such that $Fr_F(\alpha) = g(\alpha)$. The tuple (f, g) is a point in $\mathcal{F}_n(F)$ (i.e., it defines a morphism $\operatorname{Spec} F \to \mathcal{F}_n$). It is easy to see that

$$\operatorname{Spec}(E) \simeq \operatorname{Spec}(F) \times_{\mathcal{F}_n} \mathcal{E}_n,$$

as required. □

We now prove the main result of this appendix.

Proof of Lemma 3.2.1. Let $\mathfrak{X}$ be a pair consisting of a root datum and a choice of positive roots, and let k be an integer. Let $\alpha : S_2 \times C_k \to Aut(\mathfrak{X})$ be a morphism.

Let $\mathcal{G}_{\mathfrak{X}} \to \operatorname{Spec} \mathbb{Z}$ be the split reductive group scheme corresponding to $\mathfrak{X}$. Let $\alpha_2 : S_2 \times C_k \to Aut(\mathcal{G}_{\mathfrak{X}})$ be the corresponding action.

Let $Aut_{\mathcal{G}_{\mathfrak{X}}/\mathbb{Z}} : Schemes^{op} \to Groups$ be the functor defined by $Aut_{\mathcal{G}_{\mathfrak{X}}/\mathbb{Z}}(S) = Aut_S(\mathcal{G}_{\mathfrak{X}} \times_{\operatorname{Spec}\mathbb{Z}} S)$; cf. [Con, Definition 7.1.3]. By [Con, Theorem 7.1.9], this functor is representable by a (not necessarily finite type) $\mathbb{Z}$-group scheme that we also denote $Aut_{\mathcal{G}_{\mathfrak{X}}/\mathbb{Z}}$.

Denoting $S_2 = \{1, \varepsilon\}$, let $\mathcal{I}_{\mathfrak{X},\alpha} \subset Aut_{\mathcal{G}_{\mathfrak{X}}/\mathbb{Z}}$ be defined by

$$\mathcal{I}_{\mathfrak{X},\alpha}(S) := \left\{ a \in Aut_{\mathcal{G}_{\mathfrak{X}}/\mathbb{Z}}(S) \,\middle|\, \begin{array}{l} a \text{ commutes with } \alpha_2(C_k)_S \text{ and, for every geometric point } s \text{ of } S, \\ \text{the automorphism } a_s \text{ is in the class } \alpha(\varepsilon, 0) \end{array} \right\},$$

where S is an affine scheme. For an automorphism β of $\mathcal{G}_{\mathfrak{X}}$, we denote by β_S its restriction to $\mathcal{G}_{\mathfrak{X}} \times S$. By [Con, Theorem 7.1.9], $\mathcal{I}_{\mathfrak{X},\alpha}$ is of finite type.

Define an action $\alpha_3 : S_2 \times C_k \to Aut_{\mathcal{I}_{\mathfrak{X},\alpha}}(\mathcal{G}_{\mathfrak{X}} \times \mathcal{I}_{\mathfrak{X},\alpha})$ by

$$\alpha_3(\varepsilon^i j)(x, \eta) = (\eta^i \alpha_2(j) x, \eta),$$

where $i \in \mathbb{Z}$, $j \in C_k$ and $(x, \eta) \in \mathcal{G}_{\mathfrak{X}} \times \mathcal{I}_{\mathfrak{X},\alpha}(S)$.

Let $\mathcal{F}_k, \mathcal{E}_k$ be as in Lemma B.4.1 and define $\mathcal{S}_{\mathfrak{X},\alpha} := (\mathcal{I}_{\mathfrak{X},\alpha} \times \mathcal{F}_k)^{\wedge}_{\mathcal{F}_k} \mathcal{E}_k$, where $^\wedge$ denotes the internal morphism space; see, for example, [AA, §§3.1]. An F-point of $\mathcal{S}_{\mathfrak{X},\alpha}$ is a pair (z, y), where $y \in \mathcal{F}_k(F)$ and $z \in \mathcal{I}_{\mathfrak{X},\alpha}((\mathcal{E}_k)_y)$. Let

$$\mathcal{R}'_{\mathfrak{X},\alpha} = (\mathcal{G}_{\mathfrak{X}} \times \mathcal{S}_{\mathfrak{X},\alpha})^{\wedge}_{\mathcal{S}_{\mathfrak{X},\alpha}} (\mathcal{E}_k \times_{\mathcal{F}_k} \mathcal{S}_{\mathfrak{X},\alpha}).$$

Note that $\mathcal{R}'_{\mathfrak{X},\alpha}$ has a natural structure of a group scheme over $\mathcal{S}_{\mathfrak{X},\alpha}$. By their constructions, $\mathcal{E}_k, \mathcal{S}_{\mathfrak{X},\alpha}, \mathcal{R}'_{\mathfrak{X},\alpha}$ all have an action of $S_2 \times C_k$ (S_2 acts trivially on $\mathcal{E}_k$). Denoting the $S_2 \times C_k$-action on $\mathcal{R}'_{\mathfrak{X},\alpha}$ by

$$\alpha_4 : S_2 \times C_k \to Aut_{\mathcal{S}_{\mathfrak{X},\alpha}}(\mathcal{R}'_{\mathfrak{X},\alpha}),$$

let

$$\mathcal{R}_{\mathfrak{X},\alpha} := (\mathcal{R}'_{\mathfrak{X},\alpha})^{\alpha_4(C_k)},$$

and

$$t_{\mathfrak{X},\alpha} := \alpha_4(\varepsilon)|_{\mathcal{R}_{\mathfrak{X},\alpha}}.$$

Denote $n_{\mathfrak{X}} := C^{spt}(\dim_{\operatorname{Spec}\mathbb{Z}}(\mathcal{G}_{\mathfrak{X}}))$, where C^{spt} is the function given by Lemma B.1.1.

Let

$$\Delta_n := \{(\mathfrak{X}, d, \kappa)|\mathfrak{X} \text{ is a root datum of dimension } \leq n; d \leq n_{\mathfrak{X}}; \kappa \in Mor(S_2 \times C_d, \operatorname{Aut}(\mathfrak{X}))/ad(\operatorname{Aut}(\mathfrak{X}))\}.$$

Since there are finitely many root data of a given dimension (Lemma B.3.1) and finitely many actions of $S_2 \times C_d$ ($d \leq n_{\mathfrak{X}}$) on a given root datum (Lemma B.3.2), the set Δ_n is finite. Finally, set

$$\mathcal{S}_n := \bigsqcup_{(\mathfrak{X},d,[\alpha])\in\Delta_n} \mathcal{S}_{\mathfrak{X},\alpha},$$

$$\mathcal{R}_n := \bigsqcup_{(\mathfrak{X},d,[\alpha])\in\Delta_n} \mathcal{R}_{\mathfrak{X},\alpha},$$

and

$$t_n := \bigsqcup_{(\mathfrak{X},d,[\alpha])\in\Delta_n} t_{\mathfrak{X},\alpha}.$$

We claim that $(\mathcal{R}_n, \mathcal{S}_n, t_n)$ satisfies the requirements of the lemma.

Parts (1,3) follow from the fact that, for any geometric point x of $\mathcal{S}_{\mathfrak{X},\alpha}$, the group scheme $(\mathcal{R}_{\mathfrak{X},\alpha})_x$ is reductive and its absolute root system is $\mathfrak{X}$. It remains to show Part (2).

Let n be an integer, let F be a finite field, let $\mathbf{G}$ be a reductive group of dimension $\leq n$ defined over F and let t be an involution of $\mathbf{G}$. We need to find an element $w \in \mathcal{S}_n(F)$ such that

$$(\mathbf{G}, t) \simeq ((\mathcal{R}_n)|_w, t_n|_{(\mathcal{R}_n)|_w}).$$

Let $\mathfrak{X}$ be the absolute root datum of $\mathbf{G}$. By Lemma B.1.1, there is a field extension E/F of degree $d \leq n_{\mathfrak{X}}$ and an isomorphism $\mathbf{G}_E \simeq (\mathcal{G}_{\mathfrak{X}})_E$.

Denoting the group of E-automorphisms of the algebraic group $(\mathcal{G}_{\mathfrak{X}})_E$ by $Aut_E((\mathcal{G}_{\mathfrak{X}})_E)$, we get an element in $H^1(Gal(E/F), Aut_E((\mathcal{G}_{\mathfrak{X}})_E))$. By Lang's theorem, this element comes from an element $H^1(Gal(E/F), Out_E((\mathcal{G}_{\mathfrak{X}})_E))$ via the embedding $Out_E((\mathcal{G}_{\mathfrak{X}})_E) \cong Out(\mathfrak{X}) \subset Aut_E(\mathcal{G}_{\mathfrak{X}})_E$. Since the action of $\operatorname{Gal}(E/F)$ on $Out_E((\mathcal{G}_{\mathfrak{X}})_E)$ is trivial, this element is a homomorphism $\xi : Gal(E/F) \to Out_E((\mathcal{G}_{\mathfrak{X}})_E) = Aut(\mathfrak{X})$.

Let $[t] \in Aut(\mathfrak{X})$ be the involution corresponding to $t \in \operatorname{Aut}(\mathbf{G})$. We get an action $\alpha : S_2 \times C_d \to Aut(\mathfrak{X})$. By Lemma B.4.1, there is an element $y \in \mathcal{F}_d(F)$ such that $(\mathcal{E}_d)|_y = \operatorname{Spec} E$ and the action C_d on this fiber is the Frobenius action.

Let t_E be the automorphism of $\mathbf{G}_E$ corresponding to t. We will consider it as an element in $Aut_{\mathcal{G}_X/\mathbb{Z}}(E) = Aut_E((\mathcal{G}_{\mathfrak{X}})_E)$. By construction, $t \in \mathcal{I}_{\mathfrak{X},\alpha}(F)$. The tuple (y, t) gives a point $w \in \mathcal{S}_{\mathfrak{X},\alpha}(F) \subset \mathcal{S}_n(F)$. Finally,

$$(\mathbf{G}, t) \simeq ((\mathcal{R}_n)|_w, t_n|_{(\mathcal{R}_n)|_w}). \qquad \square$$

Acknowledgements. We thank Uri Bader, Shachar Carmeli, Yoav Segev and Shai Shechter for helpful discussions.

Competing interest. The authors have no competing interest to declare.

Financial support. A.A. was partially supported by ISF grant 249/17 and a Minerva foundation grant. N.A. was partially supported by NSF grant DMS-1902041. We were both partially supported by BSF grant 2018201.

References

[AA] A. Aizenbud and N. Avni, 'Pointwise surjective presentations of stacks', Preprint, 2019, arXiv:1912.11437.

[AA19] A. Aizenbud and N. Avni, 'Bounds on multiplicities of spherical spaces over finite fields', *J. Pure Appl. Algebra* **223**(9) (2019), 3859–3868.

[AAG12] A. Aizenbud, N. Avni and D. Gourevitch, 'Spherical pairs over close local fields', *Comment. Math. Helv.* **87**(4) (2012), 929–962.

[ABD+64] M. Artin, J. E. Bertin, M. Demazure, P. Gabriel, A. Grothendieck, M. Raynaud and J.-P. Serre, *Schémas en groupes. Fasc. 4: Exposés 12 à 14* (Institut des Hautes Études Scientifiques, Paris, 1964) Troisième édition, Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques, 1963/64, dirigé par Michel Demazure et Alexander Grothendieck.

[AG09a] A. Aizenbud and D. Gourevitch, 'Generalized Harish-Chandra descent, Gelfand pairs, and an Archimedean analog of Jacquet-Rallis's theorem', *Duke Math. J.* **149**(3) (2009), 509–567. With an appendix by the authors and Eitan Sayag.

[AG09b] A. Aizenbud and D. Gourevitch, 'Multiplicity one theorem for $(\mathrm{GL}_{n+1}(\mathbb{R}), GL_n(\mathbb{R}))$', *Selecta Math. (N.S.)* **15**(2) (2009), 271–294.

[AG10] A. Aizenbud and D. Gourevitch, 'Some regular symmetric pairs', *Trans. Amer. Math. Soc.* **362**(7) (2010), 3757–3777.

[AG12] A. Aizenbud and D. Gourevitch, 'Multiplicity free Jacquet modules', *Canad. Math. Bull.* **55**(4) (2012), 673–688.

[AGJ09] A. Aizenbud, D. Gourevitch and H. Jacquet, 'Uniqueness of Shalika functionals: the Archimedean case', *Pacific J. Math.* **243**(2) (2009), 201–212.

[AGM16] A. Aizenbud, D. Gourevitch and A. Minchenko, 'Holonomicity of relative characters and applications to multiplicity bounds for spherical pairs', *Selecta Math. (N.S.)* **22**(4) (2016), 2325–2345.

[AGRS10] A. Aizenbud, D. Gourevitch, S. Rallis and G. Schiffmann, 'Multiplicity one theorems', *Ann. of Math. (2)* **172**(2) (2010), 1407–1434.

[AGS08] A. Aizenbud, D. Gourevitch and E. Sayag, '$(\mathrm{GL}_{n+1}(F), \mathrm{GL}_n(F))$ is a Gelfand pair for any local field F', *Compos. Math.* **144**(6) (2008), 1504–1524.

[Aiz] A. Aizenbud, 'The Gelfand-Kazhdan criterion as a necessary and sufficient criterion', Preprint, http://aizenbud.org/4Publications/GK.pdf.

[Aiz13] A. Aizenbud, 'A partial analog of the integrability theorem for distributions on p-adic spaces and applications', *Israel J. Math.* **193**(1) (2013), 233–262.

[AS12] A. Aizenbud and E. Sayag, 'Invariant distributions on non-distinguished nilpotent orbits with application to the Gelfand property of $(GL_{2n}(\mathbb{R}), Sp_{2n}(\mathbb{R}))$', *J. Lie Theory* **22**(1) (2012), 137–153.

[BLR90] S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron Models* (Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]) vol. 21 (Springer-Verlag, Berlin, 1990).

[BvD94] E. P. H. Bosman and G. van Dijk, 'A new class of Gelfand pairs', *Geom. Dedicata* **50**(3) (1994), 261–282.

[Car] S. Carmeli, On the stability and gelfand property of symmetric pairs.

[Con] B. Conrad, Reductive group schemes.

[CS15] F. Chen and B. Sun, 'Uniqueness of Rankin-Selberg periods', *Int. Math. Res. Not. IMRN* 2015(14) (**2015**), 5849–5873.

[Del10] P. Delorme, 'Constant term of smooth H_ψ-spherical functions on a reductive p-adic group', *Trans. Amer. Math. Soc.* **362**(2) (2010), 933–955.

[Fli91] Y. Z. Flicker, 'On distinguished representations', *J. Reine Angew. Math.* **418** (1991), 139–172.

[GK75] I. M. Gel'fand and D. A. Kazhdan, 'Representations of the group (n, K) where K is a local field', in *Lie Groups and Their Representations* (Proc. Summer School, Bolyai János Math. Soc., Budapest, 1971), 95–118.

[Gla18] I. Glazer, 'Representations of reductive groups distinguished by symmetric subgroups', *Math. Z.* **289**(1–2) (2018), 471–489.

[GLS94] D. Gorenstein, R. Lyons and R. Solomon, *The Classification of the Finite Simple Groups* (Mathematical Surveys and Monographs) vol. 40 (American Mathematical Society, Providence, RI, 1994).

[Isa06] I. M. Isaacs, *Character Theory of Finite Groups* (AMS Chelsea Publishing, Providence, RI, 2006). Corrected reprint of the 1976 original [Academic Press, New York; MR0460423].

[JR96] H. Jacquet and S. Rallis, 'Uniqueness of linear periods', *Compos. Math.* **102**(1) (1996), 65–123.

[JSZ10] D. Jiang, B. Sun and C.-B. Zhu, 'Uniqueness of Bessel models: the Archimedean case', *Geom. Funct. Anal.* **20**(3) (2010), 690–709.

[JSZ11] D. Jiang, B. Sun and C.-B. Zhu, 'Uniqueness of Ginzburg-Rallis models: the Archimedean case', *Trans. Amer. Math. Soc.* **363**(5) (2011), 2763–2802.

[KO13] T. Kobayashi and T. Oshima, 'Finite multiplicity theorems for induction and restriction', *Adv. Math.* **248** (2013), 921–944.

[KS16] B. Krötz and H. Schlichtkrull, 'Finite orbit decomposition of real flag manifolds', *J. Eur. Math. Soc. (JEMS)* **18**(6) (2016), 1391–1403.

[LP11] M. J. Larsen and R. Pink, 'Finite subgroups of algebraic groups', *J. Amer. Math. Soc.* **24**(4) (2011), 1105–1158.

[Lus85] G. Lusztig, 'Character sheaves. I', *Adv. Math.* **56**(3) (1985), 193–237.

[Mar91] G. A. Margulis, *Discrete Subgroups of Semisimple Lie Groups* (Ergebnisse der Mathematik und ihrer Grenzgebiete (3) [Results in Mathematics and Related Areas (3)]) vol. 17 (Springer-Verlag, Berlin, 1991).

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press

[Moo68] C. C. Moore, 'Group extensions of p-adic and adelic linear groups', *Inst. Hautes Études Sci. Publ. Math.* 1968(35) (**1968**), 157–222.

[Nie06] C. Nien, 'Models of representations of general linear groups over p-adic fields', PhD Thesis, University of Minnesota (ProQuest LLC, Ann Arbor, MI, 2006).

[Nor87] M. V. Nori, 'On subgroups of GLn(Fp)', *Invent. Math.* **88**(2) (1987), 257–275.

[OS08] O. Offen and E. Sayag, 'Uniqueness and disjointness of Klyachko models', *J. Funct. Anal.* **254**(11) (2008), 2846–2865.

[PR94] V. Platonov and A. Rapinchuk, *Algebraic Groups and Number Theory* (Pure and Applied Mathematics) vol. 139 (Academic Press, Inc., Boston, MA, 1994). Translated from the 1991 Russian original by Rachel Rowen.

[Pra] D. Prasad, 'A "relative" local langlands correspondence', Preprint, 2015, arXiv:1512.04347.

[Rub] R. Rubio, 'On the Gelfand property for complex symmetric pairs', Preprint, 2022, arXiv:1905.11820.

[Ser02] J.-P. Serre, *Galois Cohomology* (Springer Monographs in Mathematics) English edn. (Springer-Verlag, Berlin, 2002). Translated from the French by Patrick Ion and revised by the author.

[Sha74] J. A. Shalika, 'The multiplicity one theorem for GLn', *Ann. of Math. (2)* **100** (1974), 171–193.

[She] S. Shechter, 'Bounds on multiplicities of spherical spaces over finite fields – the general case', Preprint, 2019, arXiv:1912.03694.

[Ste60] R. Steinberg, 'Automorphisms of finite linear groups', *Canad. J. Math.* **12** (1960), 606–615.

[Ste68] R. Steinberg, *Endomorphisms of Linear Algebraic Groups* (Memoirs of the American Mathematical Society) no. 80. (American Mathematical Society, Providence, RI, 1968).

[SV17] Y. Sakellaridis and A. Venkatesh, 'Periods and harmonic analysis on spherical varieties', *Astérisque* **396** (2017), viii+360.

[SZ12] B. Sun and C.-B. Zhu, 'Multiplicity one theorems: the Archimedean case', *Ann. of Math. (2)* **175**(1) (2012), 23–44.

[vD86] G. van Dijk, 'On a class of generalized Gel'fand pairs', *Math. Z.* **193**(4) (1986), 581–593.

[vdB87] E. P. van den Ban, 'Asymptotic behaviour of matrix coefficients related to reductive symmetric spaces', *Nederl. Akad. Wetensch. Indag. Math.* **49**(3) (1987), 225–249.

[Yak05] O. Yakimova, *Gelfand Pairs* (Bonner Mathematische Schriften [Bonn Mathematical Publications]) vol. 374 (Universität Bonn, Mathematisches Institut, Bonn, 2005. Dissertation, Rheinische Friedrich-Wilhelms- Universität Bonn, Bonn, 2004).

[Zha10] L. Zhang, 'Gelfand pairs $(\mathrm{Sp}_{4n}(F), \mathrm{Sp}_{2n}(E))$', *J. Number Theory* **130**(11) (2010), 2428–2441.

https://doi.org/10.1017/fms.2024.58 Published online by Cambridge University Press