

# FUNCTORIALITY AND THE INVERSE GALOIS PROBLEM

CHANDRASHEKHAR KHARE, MICHAEL LARSEN, AND GORDAN SAVIN

ABSTRACT. We prove that for any prime  $\ell$  and any even integer  $n$ , there are infinitely many exponents  $k$  for which  $\mathrm{PSP}_n(\mathbb{F}_{\ell^k})$  appears as a Galois group over  $\mathbb{Q}$ . This generalizes a result of Wiese [Wiese], which inspired this paper.

**MSC numbers:** 11F, 11R

## 1. INTRODUCTION

The inverse Galois problem asserts that every finite group  $G$  occurs as  $\mathrm{Gal}(K/\mathbb{Q})$  for  $K/\mathbb{Q}$  a finite Galois extension of  $\mathbb{Q}$ . This has received much attention. It is natural to focus first on simple groups  $G$ . The first infinite family of non-abelian finite simple groups for which the problem was solved was the family of alternating groups. Hilbert proved his irreducibility theorem for this purpose, thus showing that it suffices to prove that  $A_n$  occurs as the Galois group of a finite regular extension of  $\mathbb{Q}(T)$ .

The main advance on this problem in recent decades is the rigidity method. This method has solved the problem for most of the sporadic groups: it realizes all sporadic groups with the exception of the Mathieu groups  $M_{23}$  and  $M_{24}$  as Galois groups of regular extensions of  $\mathbb{Q}(T)$ . We refer to [Det], and the references therein, for results towards the inverse Galois problem that are proved by the rigidity method and its variants.

For classical groups, rigidity-type methods have met with only sporadic success. Typically these methods seem to work for  $G(\mathbb{F}_{\ell^k})$ , with  $G$  a Chevalley group over the prime field  $\mathbb{F}_{\ell}$ , when  $k$  is *small* as compared to the rank of  $G$ .

Recently, Wiese [Wiese] proved a result of the opposite kind:

**Theorem 1.1.** *Let  $\ell$  be any prime. Then there exist infinitely many integers  $k$  such that at least one of  $\mathrm{PSL}_2(\mathbb{F}_{\ell^k})$  and  $\mathrm{PGL}_2(\mathbb{F}_{\ell^k})$  can be*

---

CK was partially supported by NSF grants DMS 0355528 and DMS 0653821, and the Miller Institute for Basic Research in Science, University of California Berkeley.

GS was partially supported by NSF grant DMS 0551846.

realized as a Galois group over  $\mathbb{Q}$ . In particular, there are infinitely many integers  $k$  for which the finite simple group  $L_2(2^k) = \mathrm{PSL}_2(\mathbb{F}_{2^k}) = \mathrm{PGL}_2(\mathbb{F}_{2^k})$  can be realized.

This paper generalizes Wiese's result to finite simple groups of symplectic type.

**Theorem 1.2.** *If we fix a prime  $\ell$  and integers  $n, t \geq 1$  with  $n = 2m$  even, the finite simple group  $\mathrm{PSp}_n(\mathbb{F}_{\ell^k})$  occurs as a Galois group over  $\mathbb{Q}$  for some integer  $k$  divisible by  $t$ .*

The method of [Wiese] relies on results in [KW]. In particular it relies on [KW, Lemma 6.3], which asserts that if one ensures certain ramification properties of a compatible system of 2-dimensional representations of  $G_{\mathbb{Q}}$ , then its residual representations for small residue characteristics are large. Wiese uses this lemma and some other techniques and results from [KW]. One may remark, however, that given some constructions of automorphic forms, the only result from [KW] one really needs to use is the simple but crucial [KW, Lemma 6.3].

To prove our theorem we construct a continuous irreducible representation  $\rho : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_{\ell})$  that is unramified outside  $\ell$ , the infinite place  $\infty$ , and another auxiliary prime  $q$ , and whose image is contained in either the orthogonal or symplectic similitudes. The representation  $\rho$  is constructed so that the image of  $\rho(D_q)$ , with  $D_q$  a decomposition group at  $q$  in  $G_{\mathbb{Q}}$ , is a metacyclic group, which acts irreducibly on  $\overline{\mathbb{Q}}_{\ell}^n$  and preserves an alternating form, up to a multiplier. Thus one knows that the image of  $\rho$  is contained in fact in the symplectic similitudes. We ensure that the order of  $\rho(I_q)$ , with  $I_q$  an inertia group at  $q$  of  $G_{\mathbb{Q}}$ , is a prime  $p \neq \ell$  that is sufficiently large. The representation  $\rho$  has the property that all open subgroups  $H$  of index  $\leq N$  contain the image of  $\rho(D_q)$ . (The  $N$  here is larger than  $\max(p(n), d(n))$  with  $p(n), d(n)$  as in Theorem 2.2 and  $p$  is chosen to be larger than  $N$ .) This is ensured by choosing  $q$  to split in all extensions of  $\mathbb{Q}$  of degree at most  $N$  that are unramified outside  $\ell$  and  $\infty$ , and observing that by construction the extensions of  $\mathbb{Q}$  corresponding to the subgroups  $H$  of  $\mathrm{im}(\rho)$  of index at most  $N$  have this property. Such a  $q$  exists as a consequence of the theorems of Hermite-Minkowski and Čebotarev. Then by choice of  $N, q, p$ , using Theorem 2.2 and Corollary 2.6, one sees that the projective image of the image of a reduction of  $\rho$  is either  $\mathrm{PSp}_n(\mathbb{F}_{\ell^k})$  or  $\mathrm{PGSp}_n(\mathbb{F}_{\ell^k})$  for some integer  $k$ . By choosing  $p$  appropriately we may ensure that the former possibility obtains, and that  $k$  is divisible by an integer  $t$  chosen in advance.

It is in practise impossible to construct such Galois representations with controlled ramification properties directly. Instead one constructs

certain automorphic forms and relies crucially on the work of Kottwitz, Clozel and Harris-Taylor which associates Galois representations to these, and proves that they have the required ramification properties. We recall this more precisely below.

The observations that if:

- a finite subgroup  $G$  of  $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$  contains *deeply* embedded within it a certain metacyclic subgroup, then  $G$  is forced to be *large*, and
- the image of a global Galois representation can be made to contain such a metacyclic subgroup by means of the Hermite-Minkowski theorem

we owe to [KW] in the case of  $n = 2$ . Theorem 2.2 of this work generalizes the first observation to all  $n$ . The second observation can then be used in conjunction with automorphic methods to construct the required global Galois representations.

The main steps to the proof of Theorem 1.2 are:

- (1) A generalization of Lemma 6.3 of loc. cit. to any dimension (Theorem 2.2), and
- (2) Construction of self-dual, algebraic, regular cuspidal automorphic representations  $\Pi$  on  $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ , with  $\mathbb{A}_\mathbb{Q}$  the adèles of  $\mathbb{Q}$ , with certain ramification properties: see Section 5.3. The reader may consult [Cl] for the definition of regular and algebraic which is a condition on  $\Pi_\infty$ .

Theorem 2.2 might be of independent interest and be useful when extending the results of [KW].

We indicate how we construct the  $\Pi$ 's: this also allows us to introduce some necessary notation.

An expected source of  $\mathrm{PSp}_n(\overline{\mathbb{F}}_\ell)$ -valued representations of  $G_\mathbb{Q}$  are self-dual automorphic representations  $\Pi$  of  $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$  which are regular algebraic at infinity and for which the exterior square  $L$ -function,  $L(s, \Lambda^2, \Pi)$ , has a pole at  $s = 1$ .

For each place  $v$  of  $\mathbb{Q}$  we may attach to  $\Pi_v$  its complex Langlands parameter  $\sigma(\Pi_v)$  (we use the normalization of [Cl]) which is a representation of the Weil-Deligne group  $WD_v$  of  $\mathbb{Q}_v$  with values in  $\mathrm{GL}_n(\mathbb{C})$ . We may regard this as valued in  $\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$  by choosing an isomorphism  $\mathbb{C} \simeq \overline{\mathbb{Q}}_\ell$ . When  $\Pi_v$  is unramified or supercuspidal,  $\sigma(\Pi_v)$  may be regarded as a representation of the Weil group  $W_{\mathbb{Q}_v} \subset WD_v$  of  $\mathbb{Q}_v$ ; in fact, this will be the case at all finite places for the representations we construct.

The work in [Kot], [Cl], [HT] attaches Galois representations to many such  $\Pi$ . More precisely, if there is a finite place  $v$  such that  $\Pi_v$  is

discrete series, and  $\Pi_\infty$  is regular and algebraic, for every prime  $\ell$ , there is an  $\ell$ -adic Galois representation  $\rho_\Pi : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$  such that the Frobenius-semisimplification of  $\rho_\Pi|_{D_q}$  is isomorphic to  $\sigma(\Pi_v) \otimes |\cdot|^{-\frac{1-n}{2}}$  for all primes  $q \neq p$  at which  $\Pi_q$  is unramified or supercuspidal.

We need to ensure certain ramification properties of  $\Pi$  for this Galois representation to be of use to us. For this we give ourselves the data of certain supercuspidal representations  $\pi_v$  of  $\mathrm{GL}_n(\mathbb{Q}_v)$  for  $v \in S$  a finite set of finite places and a discrete series representation  $\pi_\infty$  at  $\infty$  with regular algebraic parameter. Then we have to construct a cuspidal automorphic representation  $\Pi$  that is self-dual on  $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ , such that  $\Pi$  is unramified outside  $S$  and another place  $w$  (which will typically be  $\ell$ ), and  $\Pi_v \simeq \pi_v$  for  $v \in S \cup \{\infty\}$ .

To construct representations of  $G_{\mathbb{Q}}$  with values in symplectic groups, one is led by the predictions of Langlands to construct automorphic forms on orthogonal groups which are their dual. On the other hand, the work recalled above of attaching Galois representations to automorphic forms is available for automorphic forms that are on groups more closely related to  $\mathrm{GL}_{2m}$ . Thus we first construct appropriate generic cuspidal automorphic representations on  $\mathrm{SO}_{2m+1}(\mathbb{A}_{\mathbb{Q}})$  using Poincaré series (see Theorem 4.5) and then transfer them to  $\mathrm{GL}_{2m}(\mathbb{A}_{\mathbb{Q}})$  using a known case of Langlands' principle of functoriality, namely the forward lifting of Cogdell, Kim, Piatetski-Shapiro and Shahidi [C.K.PS.S] that uses converse theorems. This accounts for the functoriality of the title (functoriality is used in some more of our references, e.g. [CI]). The results of Jiang and Soudry [JS1], [JS2] which prove the local Langlands correspondence for generic supercuspidal representations of  $\mathrm{SO}_{2m+1}(\mathbb{Q}_p)$ , and that the lifts from  $\mathrm{SO}_{2m+1}(\mathbb{A}_{\mathbb{Q}})$  to  $\mathrm{GL}_{2m}(\mathbb{A}_{\mathbb{Q}})$  constructed in [C.K.PS.S] are functorial at all places, are crucial to us.

The  $\ell$ -adic representations  $\rho_\Pi$  which arise this way from automorphic representations  $\Pi$  on  $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$  that are lifted from  $\mathrm{SO}_{2m+1}(\mathbb{A}_{\mathbb{Q}})$  come with a pairing

$$\rho \otimes \rho \rightarrow \mathbb{Q}_\ell(1 - n).$$

It is expected, but probably not known in general, that this pairing can be chosen to be symplectic. It is also expected, but again not known in general, that if  $\Pi$  is cuspidal,  $\rho_\Pi$  is irreducible. We use the fact that the  $\Pi$  we consider is such that  $\sigma(\Pi_q)$  is an *irreducible* representation that preserves an *alternating* form on  $\overline{\mathbb{Q}}_\ell^n$ , at some finite prime  $q$ , to check this in the cases considered in this paper.

To summarize: we begin with a subgroup of  $\mathrm{Sp}_{2m}(\overline{\mathbb{F}}_\ell)$  which can be realized as a Galois group over  $\mathbb{Q}_q$  for a prime  $q$  satisfying a certain condition of Čebotarev type. We take the corresponding Weil group

representation and use local Langlands for  $GL_n$  to construct a representation of  $GL_n(\mathbb{Q}_q)$ . We use inverse lifting to get a representation of  $SO_{2m+1}(\mathbb{Q}_q)$ . This becomes the factor at  $q$  of an automorphic representation of  $SO_{2m+1}(\mathbb{A}_{\mathbb{Q}})$ . We then lift this to a self-dual representation on  $GL_{2m}(\mathbb{A}_{\mathbb{Q}})$ , to which we associate a symplectic  $\ell$ -adic representation of  $G_{\mathbb{Q}}$ . Thanks to known compatibilities, the restriction to  $G_{\mathbb{Q}_q}$  of the reduction of this representation gives our original representation up to a twist. Then a group theory argument (depending on the condition satisfied by  $q$ ) can be used to show that any subgroup of  $GSp_{2m}(\overline{\mathbb{F}}_{\ell})$  which contains the image of the specified image of  $G_{\mathbb{Q}_q}$  is (up to conjugation and issues of center) of the form  $Sp_{2m}(\mathbb{F}_{\ell^k})$  for some  $k$  divisible by  $t$ .

Some variant of this basic method might be made to work for other families of finite simple groups of Lie type. It appears, however, that our poor control over which values of  $k$  can be achieved is an unavoidable limitation of our technique, at least in its present form. We construct Galois representations by constructing cuspidal automorphic representations  $\pi$  on  $GL_n(\mathbb{A}_{\mathbb{Q}})$  using Poincaré series and the results of [C.K.P.S.S]. Thus this allows no control on the field of definition of  $\pi$ . On the other hand by explicitly computing Hecke eigenvalues of cuspidal automorphic representations on  $SO_{2n+1}(\mathbb{A}_{\mathbb{Q}})$ , and choosing  $\rho_q$  carefully, one could in principle realize  $PSp_n(\mathbb{F}_{\ell^k})$  for specific values of  $k$ .

On the positive side, this method does give good control of ramification. In fact, all the Galois extensions of  $\mathbb{Q}$  constructed in this paper can be ramified only at  $\ell$ ,  $q$ , and  $\infty$ .

We end our paper by proving that the  $\ell$ -adic Galois representations we construct, whose reductions mod  $\ell$  enable us to prove Theorem 1.2, also have large images; namely their Zariski closure is  $GSp_n$ .

We itemize the contents of the paper. In Section 2 we prove the group theoretic result Theorem 2.2 that is key for us. In Section 3 we fix the local Galois theoretic data that we need to realize as arising from a global Galois representation to prove Theorem 1.2. In Section 4 we prove Theorem 4.5 which yields existence of generic cuspidal representations  $\pi$  of a quasi-split group over  $\mathbb{Q}$ , with some control on the ramification of  $\pi$ , that interpolate finitely many given local representations that are generic, integrable discrete series representations. In Section 5 we combine all the earlier work to prove Theorem 1.2. We end with Section 6 that determines the Zariski closures of the images of the  $\ell$ -adic Galois representations we construct.

## 2. SOME GROUP THEORY

Let  $\Gamma$  be a group and  $d \geq 2$  an integer. We define  $\Gamma^d$  as the intersection of all normal subgroups of  $\Gamma$  of index  $\leq d$ .

Let  $n \geq 2$  be an integer and  $p$  a prime congruent to 1 (mod  $n$ ). By a group of type  $(n, p)$ , we mean any non-abelian homomorphic image of any extension of  $\mathbb{Z}/n\mathbb{Z}$  by  $\mathbb{Z}/2p\mathbb{Z}$  such that  $\mathbb{Z}/n\mathbb{Z}$  acts faithfully on  $\mathbb{Z}/p\mathbb{Z} \subset \mathbb{Z}/2p\mathbb{Z}$ .

These groups have the following property:

**Lemma 2.1.** *If  $G$  is a group of type  $(n, p)$  and  $\ell$  is a prime distinct from  $p$ , then every representation  $V$  of  $G$  over  $\overline{\mathbb{F}}_\ell$  on which  $G$  does not act through an abelian quotient has dimension  $\geq n$ . Thus every faithful representation of  $G$  over  $\overline{\mathbb{F}}_\ell$  has dimension  $\geq n$ .*

*Furthermore if the representation is  $n$ -dimensional, and the action of  $G$  is faithful, then  $G$  acts irreducibly on  $V$ .*

*Proof.* For the first part, it suffices to prove that if

$$0 \rightarrow \mathbb{Z}/2p\mathbb{Z} \rightarrow G \rightarrow \mathbb{Z}/n\mathbb{Z} \rightarrow 0$$

and  $\mathbb{Z}/n\mathbb{Z}$  acts faithfully on  $\mathbb{Z}/p\mathbb{Z}$ , then every irreducible representation of  $G$  has dimension 1 or dimension  $\geq n$ . The restriction of any such representation to  $\mathbb{Z}/p\mathbb{Z}$  is a direct sum of characters since  $\ell \neq p$ . If every character is trivial, then the original representation factors through an extension of  $\mathbb{Z}/n\mathbb{Z}$  by  $\mathbb{Z}/2\mathbb{Z}$ , and such an extension is always abelian. Otherwise, a non-trivial character  $\chi$  of  $\mathbb{Z}/p\mathbb{Z}$  appears, so every character obtained by composing  $\chi$  with an automorphism of  $\mathbb{Z}/p\mathbb{Z}$  coming from the action of  $\mathbb{Z}/n\mathbb{Z}$  likewise appears. As there are  $n$  such distinct characters, say  $\chi_1 = \chi, \dots, \chi_n$ , the original representation must have degree  $\geq n$ . If, furthermore,  $V$  is  $n$ -dimensional and  $G$  acts faithfully on  $V$ , and hence not through an abelian quotient, then the restriction of  $V$  to  $\mathbb{Z}/p\mathbb{Z}$  is  $\bigoplus_{i=1}^n \chi_i$  and  $\mathbb{Z}/n\mathbb{Z}$  acts transitively on  $\{\chi_i\}$ , justifying the last sentence.  $\square$

We recall that if  $n \geq 2$  is an integer and  $\mathbb{F}$  is a finite field, then  $\Omega_n^\pm(\mathbb{F})$  denotes the image of  $\text{Spin}_n^\pm(\mathbb{F})$  in  $\text{SO}_n^\pm(\mathbb{F})$ . (Here  $\text{Spin}_n^\pm$  and  $\text{SO}_n^\pm$  denote split or non-split spin and orthogonal groups as the superscript has a positive or negative sign; the negative sign can only appear when  $n$  is even.)

We can now state the theorem:

**Theorem 2.2.** *Let  $n \geq 2$  be an integer. There exist constants  $d(n)$  and  $p(n)$  that depend only on  $n$  such that if  $d > d(n)$  is an integer,  $p > p(n)$  and  $\ell$  are distinct primes, and  $\Gamma \subset \text{GL}_n(\overline{\mathbb{F}}_\ell)$  is a finite group such that*

$\Gamma^d$  contains a group of type  $(n, p)$ , then there exist  $g \in \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$  and  $k \geq 1$  such that  $g^{-1}\Gamma g$  is one of the following:

- (1) A group containing  $\mathrm{SL}_n(\mathbb{F}_{\ell^k})$  or  $\mathrm{SU}_n(\mathbb{F}_{\ell^k})$  and contained in its normalizer.
- (2) A group containing  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$  and contained in its normalizer.
- (3) A group containing  $\Omega_n^\pm(\mathbb{F}_{\ell^k})$  and contained in its normalizer.

*Proof.* By the main theorem of [LP], there exists a constant  $J(n)$  depending only on  $n$  such that every  $\Gamma \subset \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$  has normal subgroups  $\Gamma_1 \subset \Gamma_2 \subset \Gamma_3$  with the following properties:

- (a)  $\Gamma_1$  is an  $\ell$ -group.
- (b)  $\Gamma_2/\Gamma_1$  is an abelian group of prime-to- $\ell$  order
- (c)  $\Gamma_3/\Gamma_2$  is isomorphic to a product  $\Delta_1 \times \cdots \times \Delta_r$  of finite simple groups of Lie type in characteristic  $\ell$ .
- (d)  $\Gamma/\Gamma_3$  is of order  $\leq J(n)$ .

If  $\Gamma^d$  contains a subgroup of type  $(n, p)$  for  $d > J(n)$ , then  $\Gamma_3$  contains such a subgroup. Thus by Lemma 2.1, the action of  $\Gamma_3$  on  $\overline{\mathbb{F}}_\ell^n$  is irreducible. It follows that  $\Gamma_1 = \{1\}$ , as  $\Gamma_3$  preserves the non-trivial subspace of invariants of the  $\ell$ -group  $\Gamma_1$  acting on  $\overline{\mathbb{F}}_\ell^n$ . We conclude that  $\Gamma_3$  is an abelian extension of  $\Delta_1 \times \cdots \times \Delta_r$ . This implies  $r \geq 1$ .

We have the following lemma:

**Lemma 2.3.** *If  $q \neq \ell$  is a prime,  $\Delta$  is isomorphic to a product of finite simple groups of Lie type in characteristic  $\ell$ , and  $\phi: \Delta \rightarrow \mathrm{GL}_n(\overline{\mathbb{F}}_q)$  is a homomorphism, then*

$$|\phi(\Delta)| \leq \max(J(n), 25920)^{n/2}.$$

*Proof.* In the proof we use implicitly the fact that the normal subgroups of a product of  $r$  nonabelian simple groups are exactly the  $2^r$  obvious ones. The image  $\phi(\Delta)$  is again a product  $\Delta_1 \times \cdots \times \Delta_s$  of simple groups of Lie type in characteristic  $\ell$ . Applying [LP] to  $\phi(\Delta)$ , and renumbering the  $\Delta_i$  if necessary, we may assume that there exists  $t \leq s$  so that

$$|\Delta_1| \cdots |\Delta_t| \leq J(n)$$

and  $\Delta_{t+1}, \dots, \Delta_s$  are all of Lie type in characteristic  $q$ . There are finitely many finite simple groups which are of Lie type in two different characteristics, and the largest is  $U_4(\mathbb{F}_2) \cong \mathrm{PSp}_4(\mathbb{F}_3)$  [Atlas, p. xv], which is of order 25920. Thus,

$$|\phi(\Delta)| \leq \max(J(n), 25920)^s.$$

To bound  $s$ , we use the fact that every (faithful) irreducible representation of a product of  $k$  finite groups is an external tensor product of (faithful) representations of these groups and therefore of degree  $\geq 2^k$ .

Every faithful representation of  $\Delta_1 \times \cdots \times \Delta_s$  has, for each  $i$  from 1 to  $s$ , at least one irreducible factor which is faithful on  $\Delta_i$ . Thus the dimension of such a representation has degree at least  $2^{k_1} + \cdots + 2^{k_u}$  where  $k_1 + \cdots + k_u = s$ . It follows that  $2s \leq n$ .  $\square$

From this we can deduce the following:

**Lemma 2.4.** *Let*

$$d(n) = J(n) \max(J(n), 25920)^{n/2}$$

and  $d > d(n)$ . *There exist normal subgroups  $\{1\} = \Gamma'_1 \subset \Gamma'_2 \subset \Gamma'_3$  of  $\Gamma$  satisfying conditions (a)–(c) above together with two additional conditions:  $\Gamma'_2$  lies in the center of  $\Gamma'_3$  and  $\Gamma^d \subset \Gamma'_3$ .*

*Proof.* We know that  $\Gamma_3/\Gamma_2$  is non-trivial, and hence a non-trivial product of groups of Lie type in characteristic  $\ell$ . Let  $q$  denote a prime dividing the order of  $\Gamma_2$ . Thus  $q \neq \ell$ . Let  $\Gamma_2[q]$  and  $\Gamma_2[q^\infty]$  denote the kernel of multiplication by  $q$  and the  $q$ -Sylow subgroup respectively. As  $\Gamma_2[q]$  is an elementary abelian  $q$ -group contained in  $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ , its dimension as  $\mathbb{F}_q$ -vector space is  $\leq n$ . By the preceding lemma, the image of the homomorphism

$$\phi: \Gamma_3/\Gamma_2 \rightarrow \mathrm{Aut} \Gamma_2[q] \subset \mathrm{GL}_n(\mathbb{F}_q)$$

giving the action of  $\Gamma_3/\Gamma_2$  on  $\Gamma_2[q]$  has order bounded above by  $\max(J(n), 25920)^{n/2}$ . Let  $\Gamma_{3,q}$  denote the preimage in  $\Gamma_3$  of  $\ker \phi$ . As  $\Gamma_2[q]$  is normal in  $\Gamma$ , we see that  $\Gamma_{3,q}$  is a normal subgroup of  $\Gamma$  of index  $\leq J(n)|\mathrm{im} \phi| < d$ . Let  $\Gamma'_3$  denote the intersection of  $\Gamma_{3,q}$  over all primes  $q$  dividing the order of  $\Gamma_2$ . Then  $\Gamma^d \subset \Gamma'_3$ , and  $\Gamma'_3/\Gamma_2$  is a normal subgroup of a product of groups of Lie type in characteristic  $\ell$  and is therefore again such a product. Its action on each  $\Gamma_2[q^\infty]$  is trivial since  $\ker \mathrm{Aut} \Gamma_2[q^\infty] \rightarrow \mathrm{Aut} \Gamma_2[q]$  is a  $q$ -group. Therefore, its action on  $\Gamma_2$  is trivial. Setting  $\Gamma'_2 = \Gamma_2$ , we get the lemma.  $\square$

Redefining  $\Gamma_i := \Gamma'_i$ , we may assume that (a)–(c) hold together with the condition  $\Gamma^d \subset \Gamma_3$ , and we proceed on the hypothesis that  $\Gamma^d$  contains a subgroup of type  $(n, p)$ . Let  $\tilde{\Delta}_i$  denote the universal central extension of the simple (and therefore perfect) group  $\Delta_i$ . Then  $\tilde{\Delta}_1 \times \cdots \times \tilde{\Delta}_r$  is the universal central extension of  $\Gamma_3$  modulo its center and therefore admits a homomorphism  $\psi$  to  $\Gamma_3$ . The image of  $\psi$  together with the center of  $\Gamma_3$  generates  $\Gamma_3$ . If  $r \geq 2$ , then the composition of  $\psi$  and the inclusion  $\Gamma_3 \subset \mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$  must give an irreducible  $n$ -dimensional representation of  $\tilde{\Delta}_1 \times \cdots \times \tilde{\Delta}_r$ , which can be written as a tensor product  $V_1 \otimes V_2$  of two representations  $V_1, V_2$  with  $\dim(V_i) < n$  for  $i = 1, 2$ . This would mean that the image of  $\psi$  is contained, up to

conjugation, in the image  $I_{a,b}$  of  $\mathrm{GL}_a \times \mathrm{GL}_b$  in  $\mathrm{GL}_n$ , for some  $ab = n$ ,  $a, b > 1$ . As all scalars belong to  $I_{a,b}$ ,  $\Gamma_3$  is contained in a conjugate of  $I_{a,b}$ , which means that  $\Gamma_3 \rightarrow \mathrm{GL}_n$ , and therefore its restriction to a subgroup  $H \subset \Gamma_3$  isomorphic to a group of type  $(n, p)$ , arises from the tensor product of representations over  $\bar{\mathbb{F}}_\ell$  of dimension  $< n$ . This contradicts Lemma 2.1, and it follows that  $r = 1$ . As  $\Delta_1$  is a group of Lie type in characteristic  $\ell$ , there exists a simply connected almost simple algebraic group  $D/\bar{\mathbb{F}}_\ell$  and a Frobenius map  $F: D \rightarrow D$  such that  $\Delta_1$  is isomorphic to the quotient of  $D(\bar{\mathbb{F}}_\ell)^F$  by its center. Moreover,  $D(\bar{\mathbb{F}}_\ell)^F$  is the universal central extension of  $\Delta_1$ , so the projective representation  $\Delta_1 \rightarrow \mathrm{PGL}_n(\bar{\mathbb{F}}_\ell)$  lifts to an irreducible linear representation  $D(\bar{\mathbb{F}}_\ell)^F \rightarrow \mathrm{GL}_n(\bar{\mathbb{F}}_\ell)$ . By a well-known theorem of Steinberg [St, 13.1], the irreducible representations of  $D(\bar{\mathbb{F}}_\ell)^F$  over  $\bar{\mathbb{F}}_\ell$  extend to irreducible representations of the algebraic group  $D$ . Thus we have a non-trivial representation  $\rho: D \rightarrow \mathrm{GL}_n$ . In particular,  $\dim D \leq n^2$  and the center of  $D$  can be bounded by a function  $p(n)$  that depends only on  $n$ .

Next, we need the following lemma:

**Lemma 2.5.** *Let  $G$  be an semisimple algebraic group over an algebraically closed field  $F$ . Then there exists a constant  $N$  depending only on  $\dim G$  such that if  $p > N$  is prime and  $p \neq 0$  in  $F$ , then for any two elements  $x_1, x_2 \in G(F)$  of order  $p$  whose commutator lies in the center of  $G$  there exists a maximal torus  $T$  such that  $x_1, x_2 \in T(F)$ .*

*Proof.* We use induction on  $\dim G$ . Without loss of generality we assume that  $x_1$  is not central. If  $\tilde{x}_i$  denotes a preimage of  $x_i$  in  $\tilde{G}(F)$ , where  $\tilde{G}$  is the universal cover of  $G$ , then  $\tilde{x}_1\tilde{x}_2 = z(x_1, x_2)\tilde{x}_2\tilde{x}_1$ , where  $z(x_1, x_2)$  lies in the center of  $\tilde{G}$ . If  $p$  is greater than the order of the center of  $\tilde{G}$ , this implies that  $\tilde{x}_1$  and  $\tilde{x}_2$  commute, so  $x_1$  and  $x_2$  lie in the image  $H$  in  $G$  of the centralizer  $Z_{\tilde{G}}(\tilde{x}_1)$ . Note that  $x_1$  is semisimple due to its order, so  $\tilde{x}_1$  is semisimple, and by Steinberg's theorem,  $Z_{\tilde{G}}(\tilde{x}_1)$  is a connected reductive group. As  $H$  is connected and reductive, it can be written  $H = H'Z$ , where the derived group  $H'$  of  $H$  is semisimple and  $Z$  is the identity component of the center of  $H$ , which is a torus. Let  $x_i = x'_i z_i$  for  $i = 1, 2$  chosen so the order of  $x'_i$  is  $p$ . By the induction hypothesis,  $x'_1$  and  $x'_2$  lie in a common maximal torus  $T'$  of  $H'$ , and setting  $T = T'Z$ , the lemma follows by induction.  $\square$

We choose  $p$  greater than  $p(n)$ ,  $p \neq \ell$ , so that Lemma 2.5 applies. As  $\Gamma_3$  contains a group of type  $(n, p)$  it contains an element  $x$  of order  $p$  and an element  $y$  such that  $y^{-1}xy = x^a$ , where  $a \in (\mathbb{Z}/p\mathbb{Z})^*$  is an element of order  $n$ . Thus  $x$  and  $y^{-1}xy$  are commuting elements of order  $p$ . As we have chosen  $p$  that is prime to the order of center of  $D$ , we

may choose elements  $\tilde{x}, \tilde{y} \in D(\overline{\mathbb{F}}_\ell)$  that lie over  $x, y \in \Delta_1$  and have order  $p$ . Let  $x_1 = \tilde{x}$  and  $x_2 = \tilde{y}^{-1}\tilde{x}\tilde{y}$ . Thus  $x_2$  lies over  $x^a$ . It follows that the commutator of  $x_1$  and  $x_2$  lies in the center of  $D$ .

Applying Lemma 2.5 to  $x_1, x_2$ , we conclude that there exists a maximal torus  $T$  in  $D$  such that  $x_1$  and  $x_2$  both lie in  $T(\overline{\mathbb{F}}_\ell)$ . By a well-known theorem [Hu, §3.1], there exists  $w$  in the normalizer of  $T$  such that

$$w^{-1}x_1w = x_2 = x_1^a z.$$

As  $x_1$  and  $x$  have the same image in  $\mathrm{PGL}_n(\overline{\mathbb{F}}_\ell)$ ,

$$\rho(x_1) \sim \omega \begin{pmatrix} \lambda & 0 & \cdots & 0 \\ 0 & \lambda^a & \cdots & 0 \\ \vdots & \vdots & \ddots & 0 \\ 0 & 0 & \cdots & \lambda^{a^{n-1}} \end{pmatrix}$$

for some  $\omega$ . This implies that the characters of  $\rho$  with respect to  $T$  are pairwise distinct.

Conjugation by  $w$  permutes the weights of  $\rho$  cyclically. In particular, the Weyl group acts transitively on the weights, so  $\rho$  is miniscule. By the classification of miniscule representations [Se, Annexe], one of the following must hold:

- (1)  $D = \mathrm{SL}_m$  and  $\rho$  is a fundamental representation.
- (2)  $D = \mathrm{Sp}_n$ , and  $\rho$  is the natural representation.
- (3)  $D = \mathrm{Spin}_n$ ,  $n$  is even, and  $\rho$  is the natural representation of  $\mathrm{SO}_n$ .
- (4)  $D = \mathrm{Spin}_{2m}$ ,  $n = 2^{m-1}$ , and  $\rho$  is a semispin representation.
- (5)  $D = \mathrm{Spin}_{2m+1}$ ,  $n = 2^m$ , and  $\rho$  is the spin representation.
- (6)  $D = E_6$  and  $n = 27$ .
- (7)  $D = E_7$  and  $n = 56$ .

In case (1),  $\rho$  must be the natural representation or its dual because no permutation of an  $m$ -element set  $S$  generates a group acting transitively on the set of  $k$ -element subsets of  $S$  when  $2 \leq k \leq m-2$ . Cases (4) to (7) can be treated by observing that an integral  $r \times r$  matrix and its powers can act transitively on an  $n$ -element set only if  $\phi(n) \leq r$ . For  $m \geq 5$ ,  $\phi(2^{m-1}) = 2^{m-2} > m$ , and for  $m \geq 3$ ,  $\phi(2^m) = 2^{m-1} > m$ . This takes care of case (4) and case (5); we can ignore the semispin representations of  $\mathrm{Spin}_6$  and  $\mathrm{Spin}_8$  and the spin representation of  $\mathrm{Spin}_5$  because, up to outer automorphisms, they are duplicates of subcases of (1)–(3). Finally,  $\phi(27) = 18 > 6$ , and  $\phi(56) = 24 > 7$ .

We conclude that it suffices to consider the cases

- (1)  $D = \mathrm{SL}_n$  and  $\rho$  is the natural representation.
- (2)  $D = \mathrm{Sp}_n$  and  $\rho$  is the natural representation.

(3)  $D = \mathrm{Spin}_n$  and  $\rho$  is the natural representation of  $\mathrm{SO}_n$ .

In case (1),  $D(\overline{\mathbb{F}}_\ell)^F$  is of the form  $\mathrm{SL}_n(\mathbb{F}_{\ell^k})$  or  $\mathrm{SU}_n(\mathbb{F}_{\ell^k})$ . In case (2),  $D(\overline{\mathbb{F}}_\ell)^F = \mathrm{Sp}_n(\mathbb{F}_{\ell^k})$ . In case (3),  $D(\overline{\mathbb{F}}_\ell)^F = \mathrm{Spin}_n^\pm(\mathbb{F}_{\ell^k})$ .

Now,

$$[\Gamma_3, \Gamma_3] = [\rho(D(\overline{\mathbb{F}}_\ell)^F), \rho(D(\overline{\mathbb{F}}_\ell)^F)] = \rho(D(\overline{\mathbb{F}}_\ell)^F).$$

The possibilities for  $\rho(D(\overline{\mathbb{F}}_\ell)^F)$  are  $\mathrm{SL}_n(\mathbb{F}_{\ell^k})$ ,  $\mathrm{SU}_n(\mathbb{F}_{\ell^k})$ ,  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$ , and  $\Omega_n^\pm(\mathbb{F}_{\ell^k})$ . As

$$[\Gamma_3, \Gamma_3] \subset \Gamma \subset \mathrm{Norm}_{\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)}(\Gamma_3),$$

we have the theorem.  $\square$

**Corollary 2.6.** *Under the hypotheses of Theorem 2.2, if  $\Gamma \subset \mathrm{GSp}_n(\overline{\mathbb{F}}_\ell)$ , and  $\bar{\Gamma}$  denotes the image of  $\Gamma$  in  $\mathrm{PGL}_n(\overline{\mathbb{F}}_\ell)$ , then there exists  $\bar{g} \in \mathrm{PGL}_n(\overline{\mathbb{F}}_\ell)$  and a positive integer  $k$  such that*

$$\bar{g}^{-1}\bar{\Gamma}\bar{g} \in \{\mathrm{PSp}_n(\mathbb{F}_{\ell^k}), \mathrm{GSp}_n(\mathbb{F}_{\ell^k})/\mathbb{F}_{\ell^k}^\times\}.$$

*If, in addition,  $\det(\Gamma) \subset (\mathbb{F}_{\ell^k}^\times)^n$ , then  $\bar{g}^{-1}\bar{\Gamma}\bar{g} = \mathrm{PSp}_n(\mathbb{F}_{\ell^k})$ .*

*Proof.* If  $g^{-1}\Gamma g$  contains  $\mathrm{SL}_n(\mathbb{F}_{\ell^k})$ ,  $\mathrm{SU}_n(\mathbb{F}_{\ell^k})$ , or  $\Omega_n^\pm(\mathbb{F}_{\ell^k})$ , then one of these groups has an  $n$ -dimensional symplectic representation. When  $n = 2$ ,  $\mathrm{SL}_n$ ,  $\mathrm{SU}_n$ , and  $\mathrm{Sp}_n$  all coincide and there are no groups  $\Omega_2^\pm$  (at least no such group is a central extension of a simple non-abelian group), so  $g^{-1}\Gamma g$  contains  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$ . For  $n \geq 3$ , from Steinberg's theorem, it follows that the algebraic group  $\mathrm{SL}_n$  or  $\mathrm{SO}_n$  has a non-trivial self-dual  $n$ -dimensional representation defined over  $\overline{\mathbb{F}}_\ell$  which maps the fixed points of a Frobenius map into  $\mathrm{Sp}_n(\overline{\mathbb{F}}_\ell)$ . Of course  $\mathrm{SL}_n$  has no non-trivial self-dual representation of dimension  $n$  when  $n \geq 3$ . As for  $\mathrm{SO}_n$ , an irreducible  $n$ -dimensional representation of  $\Omega_n^\pm(\mathbb{F}_{\ell^k})$  cannot preserve a symplectic form, since it already preserves a symmetric form.

In any case, by Theorem 2.2,  $g^{-1}\Gamma g$  is trapped between  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$  and its normalizer in  $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$ . To compute the normalizer, we first note that  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$  has no non-trivial graph automorphisms, so its outer automorphism group is the semidirect product of the group of diagonal automorphisms  $\mathbb{Z}/k\mathbb{Z}$  (or  $\{0\}$  if  $\ell = 2$ ) by the group of field automorphisms  $\mathbb{Z}/2\mathbb{Z}$ .

Non-trivial field automorphisms never preserve the character of the  $n$ -dimensional representation of  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$ . For  $\ell^k \neq 4$ , we can see this by noting that, by a counting argument,  $\mathbb{F}_{\ell^k}$  contains an element  $\alpha$  such that  $\alpha + \alpha^{-1}$  is not contained in any proper subfield, and there exists an element of  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$  with eigenvalues  $1, 1, \dots, 1, \alpha, \alpha^{-1}$ . For  $n \geq 4$ , there exists an element  $\alpha$ , of  $\overline{\mathbb{F}}_4$  of order 17 and an element of  $\mathrm{Sp}_n(\mathbb{F}_4)$  with eigenvalues  $1, 1, \dots, 1, \alpha, \alpha^4, \alpha^{-4}, \alpha^{-1}$  and therefore with

trace in  $\mathbb{F}_4 \setminus \mathbb{F}_2$ . Finally,  $\mathrm{SL}_2(\mathbb{F}_4)$  contains the element  $\begin{pmatrix} 1 & \omega \\ & 1 \end{pmatrix}$  with trace  $\omega \notin \mathbb{F}_2$ . Thus,

$$[N_{\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)} \mathrm{Sp}_n(\mathbb{F}_{\ell^k}) : \mathrm{Sp}_n(\mathbb{F}_{\ell^k}) \overline{\mathbb{F}}_\ell^\times] \leq \begin{cases} 2 & \text{if } \ell \text{ is odd,} \\ 1 & \text{if } \ell = 2. \end{cases}$$

On the other hand, when  $\ell$  is odd,  $\mathrm{GSp}_n(\mathbb{F}_{\ell^k}) \subset \mathrm{Sp}_n(\mathbb{F}_{\ell^k})$  contains elements which act on  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$  by the non-trivial diagonal automorphism. By Schur's lemma, the normalizer of  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$  in  $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$  is therefore  $\mathrm{GSp}_n(\mathbb{F}_{\ell^k}) \overline{\mathbb{F}}_\ell^\times$ . This implies the first claim of the corollary.

Finally, if  $\det \Gamma \subset (\mathbb{F}_{\ell^k}^\times)^n$ , then  $g^{-1} \Gamma g \subset \mathrm{Sp}_n(\mathbb{F}_{\ell^k}) \mathbb{F}_{\ell^k}^\times$ . Taking images in  $\mathrm{PGL}_n(\overline{\mathbb{F}}_\ell)$ , we obtain the second claim of the corollary.  $\square$

**Remark:** We indicate how the proof of Theorem 2.2 is related to that of Lemma 6.3 of [KW]. There it is proved that every subgroup  $G$  of  $\mathrm{GL}_2(\overline{\mathbb{F}}_\ell)$  with the property that every index 2 subgroup of  $G$  contains the dihedral group of order  $2p$  with  $p > 5, p \neq \ell$  a prime, has projective image that is conjugate to a subgroup that is trapped between  $\mathrm{PSL}_2(\mathbb{F}_{\ell^k})$  and  $\mathrm{PGL}_2(\mathbb{F}_{\ell^k})$  for some integer  $k$ . This is proved using Dickson's theorem. The role of Dickson's theorem here is played by the results of [LP].

### 3. A FEW PRELIMINARIES FOR THE PROOF OF THEOREM 1.2

**3.1. A tamely ramified symplectic local parameter at  $q$  of dimension  $n$ .** Let  $p, q > n$  be distinct odd primes, such that the order of  $q \bmod p$  is  $n = 2m$ . Consider the degree  $n$  unramified extension  $\mathbb{Q}_{q^n}$  of  $\mathbb{Q}_q$ . We consider a character  $\chi : \mathbb{Q}_{q^n}^\times \simeq \mu_{q^n-1} \times U_1 \times q^\mathbb{Z} \rightarrow \overline{\mathbb{Q}}_\ell^\times$  such that

- the order of  $\chi$  is  $2p$
- $\chi|_{\mu_{q^n-1} \times U_1}$  is of order  $p$
- $\chi(q) = -1$ .

We call such a  $\chi$  a tame symplectic character of  $\mathbb{Q}_q$  of degree  $n$  and order  $2p$ . By local class field theory, we can regard  $\chi$  as a character of  $G_{\mathbb{Q}_{q^n}}$ . (We normalize the isomorphism of class field theory by sending a uniformizer to an arithmetic Frobenius.)

Consider  $\rho_q : G_{\mathbb{Q}_q} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$  that is given by  $\mathrm{Ind}_{\mathbb{Q}_{q^n}}^{\mathbb{Q}_q} \chi$ .

The following is easily deduced from Theorem 1 of [Moy]:

**Proposition 3.1.** *The representation  $\rho_q$  is irreducible and symplectic, and thus it can be conjugated to take values in  $\mathrm{Sp}_n(\overline{\mathbb{Q}}_\ell)$ .*

*Proof.* The irreducibility follows from the fact that the order of  $\chi$  is  $2p$  and the order of  $q \bmod 2p$  is  $n$ . This ensures that the characters

$\chi, \chi^q, \chi^{q^2}, \dots, \chi^{q^{n-1}}$  are all distinct. Also note that  $\chi|_{\mathbb{Q}_{q^m}^\times}$  is unramified (i.e., trivial on the units of  $\mathbb{Q}_{q^m}$ ) and of order 2. Then Theorem 1 of [Moy] proves that  $\rho_q$  is symplectic.  $\square$

We assume  $p \neq \ell$ . The image of the reduction of  $\rho_q$  in  $\mathrm{GL}_n(\overline{\mathbb{F}}_\ell)$  is a group of type  $(n, p)$ . It acts irreducibly on  $\overline{\mathbb{F}}_\ell^n$  and preserves up to scalars a unique bilinear form which is necessarily non-degenerate and alternating.

**3.2. Some lemmas.** Next we recall some well-known facts concerning the values of cyclotomic polynomials. Let  $R_n$  denote the set of primitive complex  $n$ th roots of unity, and

$$\Phi_n(x) = \prod_{\zeta \in R_n} (x - \zeta).$$

If  $a$  is an integer,  $n$  a positive integer, and  $p$  a prime dividing  $\Phi_n(a)$ , then either the class of  $a$  in  $\mathbb{F}_p^\times$  has order exactly  $n$  or  $p$  divides  $n$  [Was, Lemma 2.9]. In the former case,  $p$  cannot divide  $\Phi_d(a)$  for any proper divisor  $d$  of  $n$ . In the latter case, we have the following result:

**Lemma 3.2.** *If  $n \geq 3$ ,  $a \in \mathbb{Z}$ , and  $p$  is a prime dividing  $n$ , then  $p^2$  does not divide  $\Phi_n(a)$ .*

*Proof.* Suppose first that  $p = 2$  and  $n = 2^k$  for  $k \geq 2$  an integer. Then

$$\Phi_n(a) = a^{2^{k-1}} + 1 = (a^{2^{k-2}})^2 + 1 \not\equiv 0 \pmod{4}.$$

If  $p = 2$  and  $n$  has an odd prime divisor  $q$ , then  $\Phi_n(x)$  divides  $\Phi_q(x^{n/q})$  in  $\mathbb{Z}[x]$ , so  $\Phi_n(a)$  divides

$$1 + a^{\frac{n}{q}} + a^{\frac{2n}{q}} + \dots + a^{\frac{(q-1)n}{q}} \equiv 1 \pmod{2}.$$

Finally, if  $p$  is odd,  $\Phi_n(a)$  divides  $\Phi_p(a^{n/p})$ . As  $\Phi_p(x+1)$  is an Eisenstein polynomial, evaluating  $\Phi_p$  at an integer cannot give a multiple of  $p^2$ .  $\square$

From this we easily deduce the following:

**Lemma 3.3.** *If  $a \geq 3$  and  $n \geq 3$  or  $a = 2$  and  $n \geq 7$ , then  $\Phi_n(a)$  has a prime divisor  $q$  such that the class of  $a$  in  $\mathbb{F}_q^\times$  has order exactly  $n$ .*

*Proof.* It suffices to prove that  $|\Phi_n(a)| > n$  as then by Lemma 3.2 it has a prime divisor which is prime to  $n$ . We first consider the case  $a \geq 3$ . Then  $|a - \zeta| > 2$  for every  $\zeta \in R_n$ , so we have  $|\Phi_n(a)| > 2^{\phi(n)}$ . For every prime power  $P$  except for  $P = 2$ , we have  $\phi(P) \geq \sqrt{P}$ . As  $\phi$  is multiplicative, for all  $n \geq 1$ , we have  $\phi(n) \geq \sqrt{n/2}$ . For  $x > 2$ ,  $\log_2(x) < \sqrt{x/2}$ , so  $2^{\phi(n)} > n$  for all  $n \geq 3$ .

For  $a = 2$ , we write

$$\log \Phi_n(x) = \sum_{d|n} \mu\left(\frac{n}{d}\right) \log(x^d - 1).$$

As

$$|\log(2^d - 1) - d \log 2| \leq 2^{-d}(1 - 2^{-d})^{-1} \leq 2^{1-d},$$

we have

$$|\log \Phi_n(2) - \phi(n) \log 2| \leq \sum_{d=1}^{\infty} 2^{1-d} = 2.$$

For  $n \geq 181$ , we have

$$\phi(n) - 2 \geq \sqrt{n/2} - 2 > \log_2(n),$$

so we need only check  $n \leq 180$ . The only values  $n \geq 7$  for which  $\phi(n) - 2 \leq \log_2(n)$  are  $n = 8, 10, 12, 18$  for which  $\Phi_n(2)$  has prime divisor 17, 11, 13, 19 respectively.  $\square$

Now we can construct the primes  $p$  and  $q$  needed for the main theorem.

**Lemma 3.4.** *Given an even integer  $n \geq 2$ , a prime  $\ell$ , a finite Galois extension  $K/\mathbb{Q}$ , and positive integers  $t$  and  $N$ , there exist primes  $p$  and  $q$  with the following properties:*

- (1) *The primes  $p$ ,  $q$ , and  $\ell$  are all distinct.*
- (2) *The prime  $p$  is greater than  $N$ .*
- (3) *If  $\mathbb{F}$  is any finite field in characteristic  $\ell$  and  $\mathrm{GSp}_n(\mathbb{F})$  contains an element of order  $p$ , then  $\mathbb{F}$  contains  $\mathbb{F}_{\ell^t}$ .*
- (4) *The prime  $q$  splits in  $K$ .*
- (5) *The order of the image of  $q$  in  $\mathbb{F}_p^\times$  is exactly  $n$ .*

*Proof.* Let  $n = 2m$ . Let  $u > 0$  denote a multiple of  $t \cdot (m - 1)!$ . Using Lemma 3.3, choose  $p$  to be a prime dividing  $\Phi_{nu}(\ell)$  and therefore  $\Phi_n(\ell^u)$ , and such that the order of  $\ell \bmod p$  is  $nu$ . We can make  $p$  as large as we please by choosing  $u$  sufficiently large. We may therefore assume that  $p > \max(n, \ell, N)$  and  $K/\mathbb{Q}$  is not ramified at  $p$ . For the third property, we note that

$$|\mathrm{GSp}_n(\mathbb{F}_{\ell^k})| = (\ell^k - 1) \ell^{km^2} \prod_{i=1}^m (\ell^{2ik} - 1).$$

If  $\mathrm{GSp}_n(\mathbb{F}_{\ell^k})$  has an element of order  $p$ , then  $p$  divides  $\ell^{2ik} - 1$  for some  $i$  between 1 and  $m$ , which means that the order of  $\ell$  in  $\mathbb{F}_p^\times$  divides  $2ki$  for some  $i \leq m$  and therefore divides  $2k \cdot m!$ . We know that the order is in fact  $nu$ , which is an integral multiple of  $2t \cdot m!$ , so  $t$  divides  $k$ , as claimed.

Let  $q \neq \ell$  be a prime congruent to  $\ell^u \pmod{p}$ , split in  $K$ , and greater than  $n$ . As  $\mathbb{Q}(\zeta_p)$  and  $K$  are linearly disjoint over  $\mathbb{Q}$ , the Čebotarev density theorem guarantees the existence of such a prime. As  $p \neq q$ , the first property is satisfied. The second and fourth properties are built into the definitions of  $p$  and  $q$  respectively. As  $p$  does not divide  $n$  and

$$\Phi_n(q) \equiv \Phi_n(\ell^u) \equiv 0 \pmod{p},$$

the fifth property is satisfied. □

**Remark:** The referee has remarked that instead of Lemmas 3.2 and 3.3 we may use the following: For any nonzero positive integers  $a$  and  $n$ , the set of primes dividing an element of the sequence  $\{\Phi_n(a^d), d > 0\}$  is infinite.

**3.3. Fixing Galois-theoretic data.** Let  $t$  be a given positive integer. We may freely replace  $t$  by any positive multiple, so without loss of generality we assume that  $t$  is divisible by  $n$ . We define  $N$  to be  $\max(d(n), p(n))$  using the notation of Theorem 2.2, and let  $K$  denote the compositum of all extensions of  $\mathbb{Q}$  inside an algebraic closure of degree  $\leq N$  which are ramified only over  $\ell$  and  $\infty$ . By the Hermite-Minkowski theorem,  $K$  is a number field. We define  $p$  and  $q$  via Lemma 3.4 and consider the representation  $\rho_q = \text{Ind}_{\mathbb{Q}_q^n}^{\mathbb{Q}_q} \chi : G_{\mathbb{Q}_q} \rightarrow \text{Sp}_n(\overline{\mathbb{Q}_\ell})$  for  $\chi$  a tame, symplectic character of  $\mathbb{Q}_q$  of degree  $n$  and order  $2p$ . Note that  $\chi(I_q)$  has order  $p$ .

#### 4. GLOBALIZING DISCRETE SERIES

In this section we show how to construct a global, generic cuspidal representation with desired local components. A precise result is contained in Theorem 4.5. We consider Poincaré series constructed from matrix coefficients of integrable discrete series representations. A new result here is that the Poincaré series are globally generic under certain conditions. The series considered in this paper are not constructed from compactly supported functions and are, therefore, considerably different from those used by Henniart and Vigneras. See [Sha], Section 5, and references there.

**4.1. Poincaré Series.** Let  $G$  be a quasi-split almost simple algebraic group over  $\mathbb{Q}$ . The group  $K_p = G(\mathbb{Z}_p)$  is a hyperspecial maximal compact subgroup in  $G(\mathbb{Q}_p)$  for almost all primes. We assume that the Lie group  $G(\mathbb{R})$  has discrete series representations. This condition determines the quasi-split  $G(\mathbb{R})$ , up to an isogeny. We fix an invariant

measure on  $G(\mathbb{R})$  and on  $G(\mathbb{Q}_p)$ . If  $G(\mathbb{Q}_p)$  contains a hyperspecial subgroup, we normalize the measure so that the volume of the hyperspecial subgroup is 1. Since  $G$  has a hyperspecial maximal compact subgroup for almost all primes, we have also fixed a product measure on  $G(\mathbb{A})$ .

Let  $(\pi, H)$  be an integrable discrete series of  $G(\mathbb{R})$  on a Hilbert space  $H$ . Fix  $K$ , a maximal compact subgroup in  $G(\mathbb{R})$ . The space  $H_K$  of  $K$ -finite vectors in  $H$  is an irreducible  $(\mathfrak{g}, K)$ -module. Let  $f = f_\infty \otimes_p f_p$  be a function on  $G(\mathbb{A})$  such that  $f_p$  is compactly supported for every prime  $p$  and  $f_p$  is equal to the characteristic function of  $K_p$  for almost all primes. Moreover,  $f_\infty$  is a matrix coefficient of the integrable discrete series. More precisely, let  $\langle v, w \rangle$  denote the inner product on  $H$ . For our purposes the matrix coefficient  $f_\infty$  is a function

$$f_\infty(g) = \langle \pi(g)w, \pi(g_1)v \rangle$$

where  $v$  and  $w$  are  $K$ -finite vectors in  $H$  and  $g_1$  is an element in  $G(\mathbb{R})$ . Let  $Z(\mathfrak{g})$  be the center of the enveloping algebra of  $\mathfrak{g}$ . The function  $f$  satisfies:

- $f$  is in  $L^1(G(\mathbb{A}))$ .
- $f$  is right  $K$ -finite.
- $f$  is an eigenfunction of  $Z(\mathfrak{g})$ .

We define the Poincaré series to be the sum

$$P_f(g) = \sum_{\gamma \in G(\mathbb{Q})} f(\gamma g).$$

Convergence properties of this series were established by an elegant argument of Harish-Chandra. See [Bo2], Theorem 9.1. (The statement in our, adelic, language follows by the same proof.) In any case,  $P_f(g)$  converges absolutely and in the  $C^\infty$ -topology to a smooth function on  $G(\mathbb{Q}) \backslash G(\mathbb{A})$ . In particular, the series converges uniformly on compact sets in  $G(\mathbb{A})$ . This function is cuspidal. That is, for every parabolic subgroup  $P = MN$  defined over  $\mathbb{Q}$ , the constant term

$$c_N(P_f)(g) = \int_{N(\mathbb{Q}) \backslash N(\mathbb{A})} P_f(ng) \, dn$$

vanishes. This is easy to verify. Indeed, since  $\pi$  is a discrete series representation, a classical result of Harish-Chandra says that matrix coefficient  $f_\infty$  lies in the sub-space of cusp forms  $\mathcal{C}_0(G(\mathbb{R}))$  in the Schwarz space  $\mathcal{C}(G(\mathbb{R}))$  on  $G(\mathbb{R})$ . This means

$$\int_{N(\mathbb{R})} f_\infty(g'ng) \, dn = 0$$

for any two elements  $g'$  and  $g$  in  $G(\mathbb{R})$ . (See the first book of Wallach [Wal].) Since the Poincaré series is uniformly convergent on compact sets and the integral defining the constant term is taken over a compact set, we can switch the order of integration and summation to obtain

$$c_N(P_f)(g) = \sum_{\gamma \in G(\mathbb{Q})/N(\mathbb{Q})} \prod_v \int_{N_v} f_v(\gamma n g_v) dn,$$

where we have abbreviated  $N_v = N(\mathbb{Q}_p)$  if  $v = p$  and  $N_v = N(\mathbb{R})$  if  $v = \infty$ . It follows that  $c_N(P_f) = 0$  since the local integral vanishes for  $v = \infty$ .

For every  $X$  in the Lie algebra  $\mathfrak{g}$  let  $R_X$  denote the natural right action of  $X$  on smooth functions on  $G(\mathbb{R})$ . Since the Poincaré series converges in  $C^\infty$  topology,

$$R_X(P_f) = P_{Xf}$$

where  $Xf(g) = \langle \pi(g)\pi(X)w, \pi(g_1)v \rangle$ . It follows that, by fixing a  $K$ -finite  $v$  in  $H$ , the map

$$w \mapsto P_f$$

is an intertwining map—in the sense of  $(\mathfrak{g}, K)$ -modules—from  $H_K$  into  $C_0^\infty(G(\mathbb{Q}) \backslash G(\mathbb{A}))_K$ . (Here the subscript  $K$  means  $K$ -finite.) In addition, for any prime  $q$ , the local factor  $f_q$  can be taken to be a matrix coefficient of a supercuspidal representation  $\pi_q$  of  $G(\mathbb{Q}_q)$ . Then the Poincaré series, if non-vanishing, will generate a finite sum of cuspidal automorphic representation which has the integrable discrete series at the real place, the supercuspidal representation  $\pi_q$  as a local factor at the prime  $q$  and is unramified for all  $p$  such that  $K_p$  is hyperspecial.

**4.2. Genericity of Poincaré series.** Let  $N$  be the unipotent radical of a Borel subgroup  $B$  of  $G$ , defined over  $\mathbb{Q}$ . Fix  $\psi$  a Whittaker character of  $N(\mathbb{A})$  trivial on  $N(\mathbb{Q})$ . Note that the character  $\psi$  is necessarily unitary since  $N(\mathbb{A})/N(\mathbb{Q})$  is compact. In this section  $\pi$  shall denote an automorphic representation of  $G(\mathbb{A})$ . Recall that  $\pi$  is  $\psi$ -generic if

$$W_\psi(\phi) = \int_{N(\mathbb{Q}) \backslash N(\mathbb{A})} \phi(n)\psi(n) dn \neq 0$$

for some (smooth) function  $\phi$  in  $\pi$ . Again, the convergence of this integral is clear since  $N(\mathbb{A})/N(\mathbb{Q})$  is compact.

Fix two finite and disjoint sets of places:  $D$ , containing  $\infty$  and perhaps nothing else, and  $S$ , a non-empty set of primes such that  $G$  is unramified at all primes  $p$  not in  $D \cup S$ . This means that  $K_p = G(\mathbb{Z}_p)$  is a hyperspecial maximal compact subgroup of  $G(\mathbb{Q}_p)$ . For  $G$  split,  $S$  could consist of only one prime. In this section we shall show how

Poincaré series gives a globally  $\psi$ -generic (and thus non-zero) cuspidal automorphic representation  $\pi$  such that

- $\pi_\infty$  is a (given) generic integrable discrete series representation.
- $\pi_q$  is a (given) generic supercuspidal representation for every prime  $q$  in  $D$ .
- $\pi_p$  is unramified for all  $p$  not in  $S \cup D$ .

We assume, as we can, that  $\psi$  is trivial on  $N_p \cap K_p$  for every prime  $p$  not in  $S$ .

The Poincaré series is constructed as follows: Let  $f = \otimes_v f_v$  be a function on  $G(\mathbb{A})$  such that:

- $f_\infty$  is a matrix coefficient of the generic integrable discrete series  $\pi_\infty$ .
- $f_q$  is a (compactly supported) matrix coefficient of the generic supercuspidal representation  $\pi_q$  for every prime  $q$  in  $D$ .
- $f_p$  is the characteristic function of  $K_p = G(\mathbb{Z}_p)$  for all  $p$  not in  $S \cup D$ .

We shall specify the local components  $f_\ell$  for  $\ell$  in  $S$  in a moment. The idea is to show that for some choice of  $f_\ell$ , the Poincaré series is generic. Let  $B^-$  be a Borel subgroup opposite to  $B$ . For every prime  $\ell$  in  $S$  pick a decreasing sequence  $K_\ell^m$  of open compact subgroups  $K_\ell$  such that

- $K_\ell^m \cap N_\ell$  is independent of  $m$  and  $\psi$  is trivial on it.
- $K_\ell^m$  admits a parahoric factorization

$$K_\ell^m = (K_\ell^m \cap B_\ell^-)(K_\ell^m \cap N_\ell).$$

- $\lim_{m \rightarrow \infty} K_\ell^m \cap B_\ell^- = 1$  meaning that

$$\bigcap_{m=1}^{\infty} (K_\ell^m \cap B_\ell^-) = \{1\}.$$

It is easy to see that such sequence of groups  $K_m$  exists. For example, if  $G = \mathrm{SL}_2(\mathbb{Q}_p)$  then we can pick  $K_m$  to be a congruence subgroup of  $\mathrm{SL}_2(\mathbb{Z}_p)$  consisting of elements

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that  $a, d \equiv 1 \pmod{p^m}$  and  $c \equiv 0 \pmod{p^m}$ . An analogous definition can be given in general, for example, using a Chevalley basis consisting of eigenvectors for the adjoint action of the maximal torus  $B^- \cap B$ .

Let  $f^m$  be the function on  $G(\mathbb{A})$  which has the local factors outside  $S$  independent of  $m$  and as specified above, and  $f_\ell^m$  the characteristic function of  $K_\ell^m$  for all  $\ell$  in  $S$ . We shall show that  $W_\psi(P_{f^m})(g) \neq 0$  for

a sufficiently large  $m$ . In fact we can accomplish this with  $g$  in  $G(\mathbb{A})$  such that  $g_p = 1$  for all  $p$  not in  $D$ . Now to the proof. In order to save notation, assume that  $S$  contains only one prime:  $S = \{\ell\}$ . Since the Poincaré series  $P_{f^m}$  is uniformly convergent on compact sets, and  $W_\psi(P_{f^m})$  is obtained by integrating over a compact set  $N(\mathbb{A})/N(\mathbb{Q})$ , we can switch the order of integration to obtain an absolutely convergent series

$$W_\psi(P_{f^m})(g) = \sum_{\gamma \in G(\mathbb{Q})/N(\mathbb{Q})} \prod_v \int_{N_v} f_v^m(\gamma n g_v) \psi(n) \, dn.$$

Let  $\Phi(f_v^m, \gamma)$  denote the local integral over  $N_v$  in the above product. For a given  $\gamma$  in  $G(\mathbb{Q})$ , as  $m$  varies, only the factor at  $v = \ell$  could possibly change.

**Lemma 4.1.** *Let  $\gamma$  in  $G(\mathbb{Q})$  such that  $\Phi(f_\ell^m, \gamma) \neq 0$ . Then*

$$\Phi(f_\ell^m, \gamma) = \Phi(f_\ell^1, \gamma).$$

*Proof.* Recall first that  $g_\ell = 1$ . If  $\Phi(f_\ell^m, \gamma) \neq 0$  then  $\gamma n \in K_\ell^m$  for some  $n$  in  $N_\ell$ . This implies that  $\gamma$  can be written as

$$\gamma = k_\gamma n_\gamma$$

for some  $k_\gamma$  in  $K_\ell^m \cap B_\ell^-$  and  $n_\gamma$  in  $N_\ell$ . A trivial computation now shows that

$$\Phi(f_\ell^1, \gamma) = \text{vol}(K_\ell^1 \cap N_\ell) \cdot \psi(n_\gamma)^{-1} = \text{vol}(K_\ell^m \cap N_\ell) \cdot \psi(n_\gamma)^{-1} = \Phi(f_\ell^m, \gamma).$$

□

The above lemma shows that the terms in the series  $W_\psi(P_{f^m})(g)$  ( $g$  is here fixed and trivial at all finite places outside  $D$ ) are the same as the terms in the series  $W_\psi(P_{f^1})(g)$  except we take only  $\gamma$  contained in

$$(K_\ell^m \cap B_\ell^-) \cdot N_\ell.$$

As  $m$  goes to infinity, we are reduced to  $\gamma$  which sit in  $N_\ell$ , that is, in  $N(\mathbb{Q})$ . Since  $\gamma$  is a coset in  $G(\mathbb{Q})/N(\mathbb{Q})$ , we can take  $\gamma = 1$  and the limit is equal to

$$\lim_{m \rightarrow \infty} W_\psi(P_{f^m})(g) = \text{vol}(K_\ell^1 \cap N_\ell) \prod_{v \in D} \int_{N_v} f_v(n g_v) \psi(n) \, dn.$$

The local factors for  $p$  not in  $S \cup D$  are all equal to 1 since  $g_p = 1$ ,  $f_p$  is the characteristic function of  $K_p$  and, we assumed,  $\psi$  is trivial when restricted to  $K_p \cap N_p$ .

Thus, in order to show that the Poincaré series is generic for some level  $m$ , it remains to show that the integral on the right is non-zero

for some matrix coefficient and some  $g_v$ . This is done in the following section.

**4.3. Some results of Wallach.** In this section  $G = G(\mathbb{R})$ , except at the end of the section. Let  $K$  be a maximal compact subgroup in  $G$ . Let  $(\pi, H)$  be a discrete series representation on a Hilbert space  $H$ . Let  $\langle v, w \rangle$  denote the inner product on  $H$ . Let  $v$  be a non-zero vector in  $H_K$ , the space of  $K$ -finite vectors in  $H$ , and consider the matrix coefficient  $c_{v,w}(g) = \langle \pi(g)v, w \rangle$ . It will be important for us that the function  $c_{v,w}$  belongs to the (Harish-Chandra) Schwarz space  $\mathcal{C}(G)$ .

Assume now that  $\pi$  is a generic representation with respect to a regular unitary character  $\psi$  of  $N$ . The Whittaker functional  $W_\psi$  is not defined on  $H$ . Instead, the Whittaker functional is defined on a space of smooth vectors  $H^\infty$  and continuous with respect to a certain topology on  $H^\infty$ . Note that  $H_K$ , the space of  $K$ -finite vectors, is contained in  $H^\infty$ . For every vector  $v$  in  $H_K$  we can define a generalized matrix coefficient

$$\ell_{\psi,v}(g) = W_\psi(\pi(g)v).$$

Of course,  $\ell_{\psi,v}(ng) = \psi(n)\ell_{\psi,v}(g)$  for every  $N$ . Moreover, the following important property of  $\ell_{\psi,v}$  has been established by Wallach in Theorem 15.3.4 in [Wal], Section 15: The function  $\ell_{\psi,v}$  belongs to the space of Schwarz functions  $\mathcal{C}(N \backslash G, \psi)$ . This space is described using the Iwasawa decomposition  $G = NAK$ . Here  $A = \exp(\mathfrak{a})$  where  $\mathfrak{a}$  is a maximal split Cartan subalgebra of the Lie algebra  $\mathfrak{g}$  of  $G$ . A smooth function  $f$  on  $G$  belongs to  $\mathcal{C}(N \backslash G, \psi)$  if  $f/ng) = \psi(n)f(g)$  and for every  $X$  in the enveloping algebra of  $\mathfrak{g}$  and every positive integer  $d$  there is a constant  $C$  such that for all  $a$  in  $A$  and  $k$  in  $K$

$$|R_X f(ak)| \leq C\rho(a)(1 + \|\log(a)\|)^{-d}$$

where  $R_X f$  is obtained by differentiating  $f$  by  $X$  from the right. Note that this definition says, in essence, that the restriction of  $f$  to  $A$  is a usual Schwarz function on  $A$  multiplied by the modular character  $\rho(a)$ . The Haar measure  $dg$  on the group  $G$  can be decomposed as

$$dg = dn \rho^{-2}(a) da dk.$$

It follows that the space  $\mathcal{C}(N \backslash G, \psi)$  admits a natural  $G$ -invariant inner product

$$(\varphi_1, \varphi_2) = \int_{AK} \varphi_1(ak) \overline{\varphi_2(ak)} \rho^{-2}(a) da dk.$$

The absolute convergence of this integral is clear. In fact, as we shall need this observation in a moment, if  $\varphi_1$  is in the Schwarz space, so  $\varphi_1(ak) \leq C_{2,d}\rho(a)(1 + \|\log(a)\|)^{-d}$  for any  $d$ , and  $\varphi_2(ak) \leq C_2\rho(a)$

then the integral is still absolutely convergent. Indeed, up to a non-zero factor, the integral is bounded by

$$\int_A (1 + \|\log(a)\|)^{-d} da$$

which is absolutely convergent for a sufficiently large  $d$ .

The map  $v \mapsto \ell_{\psi,v}$  from  $H_K$  to  $\mathcal{C}(N \backslash G, \psi)$  is an intertwining map preserving inner products. In particular the matrix coefficient  $c_{v,w}$  can be written as

$$c_{v,w}(g) = (R(g)\ell_{\psi,v}, \ell_{\psi,w})$$

where  $R$  denotes the action of  $G$  on  $\mathcal{C}(N \backslash G, \psi)$  by right translations.

**Proposition 4.2.** *Let  $\psi$  be a regular (generic) unitary character of  $N$ . Let  $(\pi, H_K)$  be a  $\psi$ -generic discrete series. For every  $v \neq 0$  in  $H_K$  there are  $g$  and  $g_1$  in  $G$  such that*

$$\int_N c_{v,\pi(g_1)v}(ng)\psi(n) dn \neq 0.$$

*Proof.* The proof is based on the following lemma:

**Lemma 4.3.** *Let  $\alpha$  be a function in  $\mathcal{C}(G)$  and  $\varphi$  a function in  $\mathcal{C}(N \backslash G, \psi)$ . Then there exists a constant  $C$  such that*

$$\int_G |\alpha(g)| \cdot |\varphi(g_1g)| dg \leq C\rho(a_1)$$

for every  $g_1 = n_1a_1k_1$  in  $G$ .

We shall postpone the proof of this lemma in order to finish the proof of proposition, first. If we take  $\alpha = c_{v,v}$  and  $\varphi = \ell_{\psi,v}$ , then the lemma assures that the integral

$$\int_{N \backslash G} \int_G c_{v,v}(g)\ell_{\psi,v}(g_1g)\overline{\ell_{\psi,v}(g_1)} dg dg_1$$

converges absolutely. Reversing the order of integration, we can rewrite this integral as

$$\int_G c_{v,v}(g)\overline{(R(g)\ell_{\psi,v}, \ell_{\psi,v})} = \|c_{v,v}\|_{L^2(G)}^2 \neq 0$$

since, as we have remarked before,  $(R(g)\ell_{\psi,v}, \ell_{\psi,v}) = c_{v,v}(g)$ . By Fubini's theorem, it follows that for some  $g_1$  in  $G$ ,

$$0 \neq \int_G c_{v,v}(g)\ell_{\psi,v}(g_1g) dg.$$

The substitution  $g := g_1^{-1}g$  gives

$$0 \neq \int_G c_{v,\pi(g_1)v}(g) \ell_{\psi,v}(g) dg.$$

Since this is an absolutely convergent integral over  $G$ , it can be written as a double integral over  $N \backslash G \times N$ . Then, by Fubini's theorem, there exists  $g$  in  $N \backslash G$  such that

$$0 \neq \ell_{\psi,v}(g) \int_N c_{v,\pi(g_1)v}(ng) \psi(n) dn.$$

(Here we used that  $\ell_{\psi,v}(ng) = \psi(n) \ell_{\psi,v}(g)$ .)

It remains to prove Lemma 4.3. We first recall some basic facts about Harish-Chandra's space  $\mathcal{C}(G)$ , see Section 8.3.7 in [War]. If  $\alpha$  is in  $\mathcal{C}(G)$  then, for every positive integer  $d$ , there exists a constant  $c$  such that

$$|\alpha(g)| \leq c \cdot \Xi(g)(1 + \sigma(g))^{-d}$$

for every  $g$  in  $G$ . This is essentially a definition of  $\mathcal{C}(G)$ . Here  $\Xi$  is a zonal spherical function of  $G$  (in particular, it is  $K$ -biinvariant) and  $\sigma(g)$  is a  $K$ -biinvariant function such that  $\sigma(a) = \|\log(a)\|$  if  $a$  is in  $A$ . We have the following result of Harish-Chandra:

**Lemma 4.4.** *For a sufficiently large positive integer  $d$ ,*

$$\int_N \Xi(na)(1 + \sigma(na))^{-d} dn \leq \rho(a).$$

*Proof.* This is precisely Theorem 8.5.2.1 in [War], the case  $s = 0$ . Note that the zonal spherical function for  $A$  is 1.  $\square$

The proof of Lemma 4.3 is now a simple manipulation of the integral. Substituting  $g := g_1^{-1}g$  and writing  $g = nak$  the integral (in the statement of Lemma 4.3) can be written as

$$\int_{NAK} |\alpha(k_1^{-1}a_1^{-1}n_1^{-1}nak)| \cdot |\varphi(nak)| dn \rho^{-2}(a) da dk.$$

Note that  $|\varphi(nak)| = |\varphi(ak)|$  since  $\psi$  is unitary. We can use a substitution  $n := n_1n$  to rewrite the integral as

$$\int_{NAK} |\alpha(k_1^{-1}a_1^{-1}nak)| \cdot |\varphi(ak)| dn \rho^{-2}(a) da dk.$$

Next, substituting  $n := a_1na_1^{-1}$  (this change of variable in  $N$  contributes a factor  $\rho^2(a_1)$ ), the integral further becomes

$$\rho^2(a_1) \int_{NAK} |\alpha(k_1^{-1}na_1^{-1}ak)| \cdot |\varphi(ak)| dn \rho^{-2}(a) da dk.$$

Since  $\alpha$  is in  $\mathcal{C}(G)$ , by Lemma 4.4, there exists a constant  $c$  such that

$$\int_N |\alpha(k_1^{-1}na_1^{-1}ak)| dn \leq c\rho(a_1^{-1}a)$$

for all  $(k_1, k)$  in  $K \times K$ . It follows that the integral is bounded by

$$c\rho(a_1) \int_{AK} \rho(a)^{-1} |\varphi(ak)| da dk \leq C\rho(a_1),$$

for some constant  $C$ , exactly what we wanted. Lemma 4.3 is proved.  $\square$

Of course, our discussion is valid in the case of  $p$ -adic fields, provided that for every positive integer  $d$ , there exists a constant  $C$  such that

$$|\ell_{\psi,v}(nak)| \leq C\rho(a)(1 + \|\log(a)\|)^{-d}.$$

This may not be known in general, but if the discrete series is supercuspidal, then  $\ell_{\psi,v}$  is compactly supported, so Proposition 4.2 holds in this case, as well. Summarizing, we have shown the following:

**Theorem 4.5.** *Let  $G$  be an almost simple, quasi-split algebraic group defined over  $\mathbb{Q}$ . Fix two finite and disjoint sets of places:  $D$  containing  $\infty$  and perhaps nothing else, and  $S$  a non-empty set of primes such that  $G$  is unramified at all primes  $p$  not in  $D \cup S$ . (This means that  $G(\mathbb{Q}_p)$  contains a hyperspecial maximal subgroup.) Let  $\psi$  be a regular (generic) character of  $N(\mathbb{A})$  trivial on  $N(\mathbb{Q})$ . Note that  $\psi$  is unitary, since  $N(\mathbb{A})/N(\mathbb{Q})$  is compact. Assume that we are given a  $\psi$ -generic integrable discrete series representation of  $G(\mathbb{R})$ , and a  $\psi$ -generic supercuspidal representation  $\pi_q$  for every  $q$  in  $D$ . Then there exists a global  $\psi$ -generic cuspidal representation  $\pi$  such that  $\pi_\infty$  is the given integrable discrete series,  $\pi_q$  is the given supercuspidal representation for every  $q$  in  $D$  and  $\pi_p$  is unramified for every  $p$  outside  $D \cup S$ .*

## 5. PROOF OF THEOREM 1.2

We first reduce the proof of Theorem 1.2 to the construction of certain self-dual cuspidal automorphic representations on  $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ . Then we carry out the construction combining Theorem 4.5 with the results in [C.K.P.S.S].

But to begin with, to apply Theorem 4.5 to construct generic cuspidal representations with a given integral integrable discrete series at the infinite place on certain orthogonal groups, we need a description of generic, integrable discrete series representations of the real group  $\mathrm{SO}(m, m+1)$ .

**5.1. Generic discrete series of  $\mathrm{SO}(m, m+1)$ .** The Lie group  $\mathrm{SO}(m+1, m)$  has two connected components. Let  $G_0$  be the connected component containing the identity and  $K_0$  a maximal compact subgroup of  $G_0$ . Note that

$$K_0 \cong \mathrm{SO}(m+1) \times \mathrm{SO}(m).$$

The necessary and sufficient condition for  $G_0$  to have discrete series representations is that the rank of  $G_0$  is equal to the rank of  $K_0$ . This clearly holds here. We shall now describe discrete series representations of  $G_0$  and specify which of them are  $\psi$ -generic for a choice of a regular (generic) character  $\psi$  of  $N(\mathbb{R})$ , the unipotent radical of a Borel subgroup. (The difference between generic discrete series for  $\mathrm{SO}(m+1, m)$  and  $G_0$  is easy to explain. Any two generic characters of  $N(\mathbb{R})$  are conjugate by an element in  $\mathrm{SO}(m+1, m)$ , whereas there are two conjugacy classes of generic characters for  $G_0$ . Any generic discrete series representation of  $\mathrm{SO}(m+1, m)$ , when restricted to  $G_0$ , breaks up as a sum of two discrete series representation of  $G_0$ , each generic with respect to precisely one of the two classes of characters.)

Let  $\mathfrak{g}$  be the real Lie algebra of  $G_0$  and  $\mathfrak{k}$  the real Lie algebra of  $K_0$ . Let  $\mathfrak{h}$  be a maximal Cartan subalgebra of  $\mathfrak{g}$  contained in  $\mathfrak{k}$ . Let  $\Phi$  and  $\Phi_K$  be the sets of roots for the action of  $\mathfrak{h}$  on  $\mathfrak{g}$  and  $\mathfrak{k}$ , respectively. The roots in  $\Phi_K$  are called *compact* roots. The root system  $\Phi$  is of type  $B_m$ . We can identify  $i\mathfrak{h}^* \cong \mathbb{R}^m$ . Let  $(\cdot|\cdot)$  be the usual inner product on  $\mathbb{R}^m$  such that the standard basis  $e_i$ ,  $1 \leq i \leq m$  is orthonormal. Then

$$\Phi = \{\pm e_i \pm e_j, \text{ with } i \neq j \text{ and } \pm e_i \text{ for all } i\}.$$

The Langlands parameter [Lan, §3] defining an  $L$ -packet of discrete series representation of  $\mathrm{SO}(m+1, m)$  is a homomorphism  $\sigma_\infty : W_{\mathbb{R}} \rightarrow \mathrm{Sp}_{2m}(\mathbb{C})$  described as follows. Recall that  $W_{\mathbb{R}}$  is the non-split extension of  $\mathbb{Z}/2\mathbb{Z}$  by  $\mathbb{C}^\times$  given by  $W_{\mathbb{R}} = \mathbb{C}^\times \cup t\mathbb{C}^\times$  where  $t^2 = -1$  and  $tzt^{-1} = \bar{z}$ . The representation  $\sigma_\infty$  is a direct sum of 2-dimensional symplectic representations  $\rho_{i,\infty}$  ( $1 \leq i \leq m$ ) which, when restricted to  $\mathbb{C}^\times$ , are of the form  $(\frac{z}{\bar{z}})^{\frac{1-2\lambda_i}{2}} \oplus (\frac{z}{\bar{z}})^{-\frac{1-2\lambda_i}{2}}$ , for some non-zero integers  $\lambda_i$  such that  $\lambda_i \neq \pm\lambda_j$  if  $i \neq j$ , and  $\rho_m(t)$  is the matrix

$$\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}.$$

The infinitesimal character of all representations in the  $L$ -packet of  $\sigma_\infty$  is

$$\lambda = (\lambda_1, \lambda_2, \dots, \lambda_m) \in i\mathfrak{h}^*.$$

In fact, the  $L$ -packet consists of all discrete series representations with this infinitesimal character. More precisely, for every non-singular and

integral  $\lambda$  in  $i\mathfrak{h}^*$ , there exists a discrete series representation  $\pi_\lambda$  of  $G_0$  with the infinitesimal character  $\lambda$ . Furthermore,  $\pi_\lambda \cong \pi_{\lambda'}$  if and only if  $\lambda$  and  $\lambda'$  are conjugated by  $W_K$ , the Weyl group of  $\Phi_K$ . Of course,  $\pi_\lambda$  and  $\pi_{\lambda'}$  have the same infinitesimal character if and only if  $\lambda$  and  $\lambda'$  are conjugated by  $W$ , the Weyl group of  $\Phi$ . In particular, the number of representations in the  $L$ -packet (for  $G_0$ ) is equal to the index of  $W_K$  in  $W$ . The representation  $\pi_\lambda$  is  $\psi$ -generic for some choice of a regular character  $\psi$  of  $N(\mathbb{R})$  if and only if all walls of the Weyl chamber containing  $\lambda$  are defined by non-compact roots (see [Vo, §6] and [Kos]). The existence of one such chamber, in fact precisely two up to the action of  $W_K$ , can be shown as follows. Instead of fixing an embedding  $\Phi_K \subseteq \Phi$  we shall fix a Weyl chamber  $\mathcal{C}$  containing  $\lambda$ , and then look for ways how to put  $\Phi_K$  into  $\Phi$  so that it misses the roots defining the Walls of  $\mathcal{C}$ . We pick the Weyl chamber  $\mathcal{C}$  containing  $\lambda$ , so that  $\lambda = (\lambda_1, \lambda_2, \dots, \lambda_m)$  where  $\lambda_i$  are positive integers such that  $\lambda_1 > \dots > \lambda_m$ . In particular, the walls of the Weyl chamber are given by

$$e_1 - e_2, e_2 - e_3, \dots, e_{m-1} - e_m \text{ and } e_m.$$

Then  $\pi_\lambda$  is  $\psi$ -generic for some choice of  $\psi$  if and only if these roots are not compact. Thus, we need to show that we can embed  $\Phi_K$  into  $\Phi$  so that it does not contain any of these roots. To this end, break up the set of indices  $\{1, 2, \dots, m\}$  into a disjoint union  $E \cup O$  where  $E = \{m, m-2, \dots\}$  and  $O = \{m-1, m-3, \dots\}$ . Then we can pick  $\Phi_K$  so that it contains  $\pm e_i \pm e_j$  where *both*  $i$  and  $j$  are either in  $E$  or in  $O$ , and  $\pm e_i$  with  $i$  in  $O$ . With this choice of  $\Phi_K$ , the discrete series  $\pi_\lambda$  is generic. The other Weyl chamber without ‘‘compact’’ walls is  $-\mathcal{C}$ . These two are not  $W_K$ -conjugated since  $-1$  is not contained in  $W_K$ . We put

$$\pi_\infty = \text{Ind}_{G_0}^{\text{SO}(m+1, m)} \pi_\lambda.$$

This is the unique generic discrete series representation of  $\text{SO}(m+1, m)$  with the infinitesimal character  $\lambda$ . In order to make this representation a local component of a global automorphic representation, we need that its matrix coefficients are integrable, as well. Integrability conditions on matrix coefficients are given as follows (see [Mi]):

**Proposition 5.1.** *Let  $W$  be the Weyl group of  $\Phi$ . Fix a positive  $W$ -invariant inner product  $(\cdot | \cdot)$  on  $i\mathfrak{h}^*$ . The discrete series representation  $\pi_\lambda$  has integrable matrix coefficients if*

$$|(\lambda | \alpha)| > k(\alpha) = \frac{1}{4} \sum_{\beta \in \Phi} |(\alpha | \beta)|.$$

for every non-compact root  $\alpha$ .

In practical terms this simply means that  $\lambda$  is at a certain distance from all walls corresponding to non-compact roots. We can determine whether the discrete series  $\pi_\lambda$  is integrable or not since one easily computes that

$$k(\alpha) = \begin{cases} m - \frac{1}{2} & \text{if } \alpha \text{ is short} \\ 2m & \text{if } \alpha \text{ is long.} \end{cases}$$

In particular, if  $\lambda_m \geq m$  and  $\lambda_i - \lambda_{i+1} > 2m$  for all  $i = 1, \dots, m-1$  then  $\pi_\lambda$  has integrable matrix coefficients.

**5.2. Reduction of Theorem 1.2 to existence of certain cuspidal automorphic representations of  $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$ .** Throughout this section we use the notation of §3.3, and the primes  $p, q$ , the representation  $\rho_q$ , and integer  $N$  are as in that section.

Let  $\Pi$  be a cuspidal automorphic representation of  $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$  which is unramified or supercuspidal at each finite place  $v$  of  $\mathbb{Q}$ . There is attached to  $\Pi_v$  a representation  $\sigma(\Pi_v): W_{\mathbb{Q}_v} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}_\ell})$ . This arises from the local Langlands correspondence of [HT] (for finite places, for infinite places these are the results of Harish-Chandra and Langlands, see [Lan], [Bo1]), and depends on choosing an isomorphism  $\mathbb{C} \simeq \overline{\mathbb{Q}_\ell}$ .

Let  $\Pi$  be a cuspidal automorphic representation of  $\mathrm{GL}_n(\mathbb{A}_\mathbb{Q})$  with the following properties:

- (a)  $\Pi$  is self-dual, i.e.,  $\Pi^\vee \simeq \Pi$
- (b)  $\Pi_\infty$  has a regular symplectic parameter  $\sigma_\infty$  described in the Section 5.1. Recall that  $\sigma_\infty$  is a direct sum of 2-dimensional representations  $\rho_{i,\infty}$  ( $1 \leq i \leq m$ ) which, when restricted to  $\mathbb{C}^\times$ , are of the form  $(\frac{z}{\bar{z}})^{\frac{1-2\lambda_i}{2}} \oplus (\frac{z}{\bar{z}})^{-\frac{1-2\lambda_i}{2}}$ . We require that  $\lambda_i$  be positive integers such that  $\lambda_m \geq m$  and  $\lambda_i - \lambda_{i+1} > 2m$  for all  $i = 1, \dots, m-1$ . This technical condition on the  $\lambda_i$ 's assures us that  $\Pi_\infty$  is a local lift of an integrable discrete series representation  $\pi_\infty$  of  $\mathrm{SO}(m+1, m)$ .
- (c)  $\Pi$  is unramified outside  $\{\ell, q\}$ , and  $\sigma(\Pi_q)$  is isomorphic to the  $\rho_q$  fixed in §3.3.

The results of [Kot], [Cl], [HT], see Theorem 3.6 of [Tay] (applied to a twist of  $\Pi$  by the  $\frac{1-n}{2}$  power of the norm character), ensure that there is a continuous semisimple representation  $\rho_\Pi: G_\mathbb{Q} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}_\ell})$  attached to  $\Pi$  such that for the finite places  $v \neq \ell$ , the Frobenius semisimplification of  $\rho_\Pi|_{D_v}$  is isomorphic to  $\sigma(\Pi_v) \otimes |\cdot|^{\frac{1-n}{2}}$ . Here  $|\cdot|^{\frac{1}{2}}: G_{\mathbb{Q}_q} \rightarrow \overline{\mathbb{Q}_\ell}$  is the unramified character of  $\mathbb{Q}_q^\times$  that takes  $q \rightarrow \sqrt{q}$  ( $\sqrt{q}$  positive). For any integer  $r$ , we may also analogously define a character

$| \cdot |^r$  of  $G_{\mathbb{Q}}$  with values in  $\overline{\mathbb{Q}}_{\ell}^*$  which is the  $r$ th power of the  $\ell$ -adic cyclotomic character.

From the fact that  $\Pi$  is self-dual we see by Čebotarev density that  $\rho_{\Pi}^{\vee} \simeq \rho_{\Pi} | \cdot |^{n-1}$  and thus  $\rho_{\Pi}$  acts either by orthogonal or symplectic similitudes on  $\overline{\mathbb{Q}}_{\ell}^n$  with similitude factor  $| \cdot |^{n-1}$ . Although it is possible for an irreducible representation to act by both orthogonal and symplectic similitudes, this is not possible if the factors of similitude are the same. As  $\rho_{\Pi}|_{D_q} \simeq \rho_q \otimes | \cdot |^{\frac{1-n}{2}}$ , and  $\rho_q$  is an irreducible symplectic representation, it follows that  $\rho_{\Pi}$  is irreducible, and that the self-duality of  $\rho_{\Pi}$  with similitude factor  $| \cdot |^{n-1}$  is symplectic. Therefore, the image of  $\rho_{\Pi}$  may be conjugated to land inside  $\mathrm{GSp}_n(\overline{\mathbb{Q}}_{\ell})$ , and in fact by the compactness of  $G_{\mathbb{Q}}$ , inside  $\mathrm{GSp}_n(\overline{\mathbb{Z}}_{\ell})$ .

We consider the reduction mod  $\ell$  of  $\rho_{\Pi}$ , and denote the resulting representation by  $\bar{\rho} : G_{\mathbb{Q}} \rightarrow \mathrm{GSp}_n(\overline{\mathbb{F}}_{\ell})$ , and note that its determinant is valued in  $\mathbb{F}_{\ell}^{\times}$ . Let  $\Gamma$  denote  $\mathrm{im}(\bar{\rho})$ . Then we see that  $\Gamma$  satisfies the conditions of Theorem 2.2, by construction, namely the choice of  $q$  and the parameter  $\rho_q$ . We expand on this. We see that any subgroup of  $\Gamma$  of index  $\leq N$  cuts out an extension  $L$  of  $\mathbb{Q}$  of degree  $\leq N$  that is unramified outside  $\{\ell, q, \infty\}$ . In fact as the image of  $\rho_q(I_q)$  is of order  $p$  and  $p > N$  we see that  $L$  is unramified at  $q$ . (To see this note that as  $p > N$ , the degree of the normal closure of  $L$  over  $\mathbb{Q}$  is prime to  $p$ .) Thus  $L$  is unramified outside  $\{\ell, \infty\}$ . Hence by choice of  $q$ , it splits in  $L$ . Furthermore, by construction  $\mathrm{im}(\bar{\rho}(D_q))$  is a group of type  $(n, p)$  (note that by choice  $p \neq \ell$ ) of Section 2, and it is contained in  $\Gamma^{d(n)}$ .

Thus Theorem 2.2 implies that after conjugation by an element in  $\mathrm{GL}_n(\overline{\mathbb{F}}_{\ell})$  we may conclude that  $\Gamma$  contains  $\mathrm{Sp}_n(\mathbb{F}_{\ell^k})$  for some integer  $k$  and is contained in its normalizer. Thus by Corollary 2.6 we know that the image of  $\Gamma$  in  $\mathrm{PGL}_n(\overline{\mathbb{F}}_{\ell})$  is isomorphic to  $\mathrm{PSp}_n(\mathbb{F}_{\ell^k})$  or  $\mathrm{GSp}_n(\mathbb{F}_{\ell^k})/\mathbb{F}_{\ell^k}^{\times}$ . As the order of this group is divisible by  $p$  (as the order of  $\bar{\rho}(I_q)$  is  $p$ ), it follows using Lemma 3.4(3) that  $k$  is divisible by  $t$ .

Recall that we are assuming that  $n|t$ , and we also know that  $\det(\bar{\rho}) \subset \mathbb{F}_{\ell}^{\times}$ . Note that for each prime  $\ell$  and integers  $n$  and  $t$ ,  $\mathbb{F}_{\ell}^*$  is a subgroup of  $(\mathbb{F}_{\ell^t}^*)^n$  if  $n$  divides  $t$ . Thus we know further, by the last part of Corollary 2.6, that the image of  $\Gamma$  in  $\mathrm{PGL}_n(\overline{\mathbb{F}}_{\ell})$  is isomorphic to  $\mathrm{PSp}_n(\mathbb{F}_{\ell^k})$ .

**5.3. Construction of certain cuspidal automorphic representations of  $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$ .** In order to construct the  $\Pi$  of the previous section we construct generic cuspidal automorphic representations  $\pi$  of the split  $\mathrm{SO}_{2m+1}(\mathbb{A}_{\mathbb{Q}})$  using Theorem 4.5 and lift them to  $\mathrm{GL}_{2m}(\mathbb{A}_{\mathbb{Q}})$  using the results of [C.K.P.S.S], [JS1], [JS2]. We use the terminology of these papers below. There is work of Chenevier and Clozel [CC] which uses related, but more elaborate, constructions to improve the results in

[Che], which Chenevier had mentioned to the first named author. The relevance of  $\mathrm{SO}_{2m+1}$  to our work is that the connected component of its L-group is  $\mathrm{Sp}_{2m}$ .

We consider the split group  $\mathrm{SO}_{2m+1}$  of rank  $m$  defined over  $\mathbb{Q}$  (defined by the form  $\sum_{i=1}^n x_i x_{n+i} + x_{2n+1}^2$ ), and consider  $\mathrm{SO}_{2m+1}(\mathbb{Q}_v)$  for each place  $v$  of  $\mathbb{Q}$ , and  $\mathrm{SO}_{2m+1}(\mathbb{A}_{\mathbb{Q}})$ . We note that the notion of genericity for these groups is independent of choice of (local or global) Whittaker character  $\psi$ , and thus we call the  $\psi$ -generic forms, or  $\psi$ -generic local representations, of Section 4 simply generic.

We need the following theorem which is a combination of the work of [C.K.P.S.S] and [JS2]: see [C.K.P.S.S, Theorem 7.1] and [JS2, Theorem E].

**Theorem 5.2.** *There is a lifting from equivalence classes of irreducible generic cuspidal automorphic representations of  $\mathrm{SO}_{2m+1}(\mathbb{A}_{\mathbb{Q}})$  to equivalence classes of irreducible automorphic representations of  $\mathrm{GL}_{2m}(\mathbb{A}_{\mathbb{Q}})$  such that this lifting is functorial at all places. Further a cuspidal automorphic representation  $\Pi$  of  $\mathrm{GL}_{2m}(\mathbb{A}_{\mathbb{Q}})$  which is in the image of this lift is self-dual (and  $L(s, \Lambda^2, \Pi)$  has a simple pole at  $s = 1$ ).*

We refer to the cited papers for the exact notion of functoriality used, but will spell it out in the cases used below.

In order to construct the generic cuspidal representation  $\pi$  we need to specify what we want at the local places. We start with the following theorem of Jiang-Soudry: [JS1, Theorem 6.4] and [JS2, Theorem 2.1].

**Theorem 5.3.** *Let  $q$  be finite prime of  $\mathbb{Q}$ . There is a bijection between irreducible generic discrete series representations of  $\mathrm{SO}_{2m+1}(\mathbb{Q}_q)$  and irreducible generic representations of  $\mathrm{GL}_{2m}(\mathbb{Q}_q)$  with Langlands parameter of the form  $\sigma = \Sigma \sigma_i$  with  $\sigma_i$  irreducible symplectic representations of  $WD_{\mathbb{Q}_q}$  which are pairwise non-isomorphic.*

Thus in particular there is a generic supercuspidal representation  $\pi_q$  of  $\mathrm{SO}_{2m+1}(\mathbb{Q}_q)$  that corresponds to the Langlands parameter  $\rho_q$  (and thus to a supercuspidal representation of  $\mathrm{GL}_{2m}(\mathbb{Q}_q)$  with this parameter). This correspondence is also known at the Archimedean places as recalled in Section 5.1. From this we deduce there is a generic, integrable discrete series representation  $\pi_{\infty}$  on  $\mathrm{SO}_{2m+1}(\mathbb{R})$  which corresponds (under the correspondence of [C.K.P.S.S, Section 5.1]) to the representation  $\Pi_{\infty}$  fixed in Section 5.2 with Langlands parameter  $\sigma_{\infty}$ .

By Theorem 4.5 (with  $D = \{\infty, q\}$  and  $S = \{\ell\}$ ) there exists a generic cuspidal automorphic representation  $\pi$  on  $\mathrm{SO}_{2m+1}(\mathbb{A}_{\mathbb{Q}})$  such that:

- Under the Jiang-Soudry correspondence of Theorem 5.3,  $\pi_q$  has parameter  $\rho_q$ .
- $\pi$  is unramified outside  $\{\ell, q\}$
- $\pi_\infty$  is a generic integrable discrete series with Langlands parameter  $\sigma_\infty$ .

Using Theorem 5.2 we can transfer  $\pi$  to  $\Pi$  to get an irreducible automorphic representation  $\Pi$  on  $\mathrm{GL}_{2m}(\mathbb{A}_{\mathbb{Q}})$  such that

- $\Pi_\infty$  has the regular algebraic parameter  $\sigma_\infty$ ,  $\Pi$  is unramified outside  $\{\ell, q\}$ , and  $\sigma(\Pi_q) \simeq \rho_q$ . (this for us is the implication of the *functorial at all places* assertion in Theorem 5.2).
- $\Pi$  is cuspidal (as  $\Pi_q$  is supercuspidal) and self-dual.

**Remarks:**

- To directly construct self-dual representations of  $\mathrm{GL}_n(\mathbb{A}_{\mathbb{Q}})$  interpolating finitely many specified self-dual supercuspidal representations at finitely many places is a subtle matter, and has been addressed recently in [CC]. As pointed out in [PR], one of the difficulties is that an obstruction to this is that the corresponding local Langlands parameters should either be all symplectic or all orthogonal, and proofs using the trace formula might not see this obstruction. We duck this issue by constructing  $\pi$  on  $\mathrm{SO}_{2m+1}(\mathbb{A}_{\mathbb{Q}})$  and then transferring it to  $\mathrm{GL}_{2m}(\mathbb{A}_{\mathbb{Q}})$  using the results of [C.K.P.S.S].
- The case  $n = 2$  corresponds to the result of [Wiese]. In that case the lifting proved in [C.K.P.S.S] is trivial: it is the lifting of cuspidal automorphic representations of  $\mathrm{PGL}_2(\mathbb{A}_{\mathbb{Q}})$  to cuspidal automorphic representations of  $\mathrm{GL}_2(\mathbb{A}_{\mathbb{Q}})$  with trivial central character.
- Curiously enough as we lack control of the field of definition of the  $\bar{\rho}$  we get, we don't see using this method how to realize  $\mathrm{PGL}_2(\mathbb{F}_{\ell^k})$  as a Galois group over  $\mathbb{Q}$  for infinitely many  $k$ . The limitations of our method do not allow us to prove that given an integer  $t > 1$  there are infinitely many  $k$  prime to  $t$  (or even one such  $k$ ) such that  $\mathrm{PSp}_n(\mathbb{F}_{\ell^k})$  appears as a Galois group over  $\mathbb{Q}$ .
- In the  $n = 2$  case, we may prove the result of [Wiese] for  $\ell > 2$  by imposing in addition to large dihedral ramification at a prime  $q$ , also  $A_4/S_4$ -type ramification at another prime (necessarily 2!). This works for  $\ell > 2$  to ensure that we get some large image representations, but does not work for  $\ell = 2$ . This is because by our methods it is not possible to ensure that a non-trivial unipotent is in the image of the mod  $\ell$  Galois representation

being considered. A similar remark applies for higher dimensions  $n$ . Further it seems of interest to us to force large images of global Galois representations by dint of properties of the representation at a *single* prime  $q$ .

- In an earlier version of the paper (see <http://front.math.ucdavis.edu/math.NT/0610860>) it had been erroneously asserted that the existence of generic cuspidal forms as in Theorem 4.5 follows from the literature, in particular the methods of [PS]. But it turns out that the methods of [PS] using the relative trace formula are not able to prove results like Theorem 4.5 where one of the local representations sought to be interpolated into a global generic representation is a generic discrete series representation of a real group.

## 6. ZARISKI DENSITY

We conclude with a group-theoretic proposition which shows that if  $t \gg 0$ , the  $\ell$ -adic representations  $\rho_{\Pi} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_{\ell})$  constructed in Section 5 have Zariski-dense image in  $\mathrm{GSp}_n$ .

Before stating it, we first prove the following lemma:

**Lemma 6.1.** *Given a positive even integer  $n$  and a prime  $\ell$  there exists a constant  $M$  such that for all  $m > M$ , and all almost simple algebraic groups  $G/\overline{\mathbb{F}}_{\ell}$  of rank  $< n/2$ , the finite simple group  $\mathrm{PSp}_n(\mathbb{F}_{\ell^m})$  is not a subquotient of  $G(\overline{\mathbb{F}}_{\ell})$ .*

*Proof.* Up to isomorphism there are only finitely many possibilities for  $G$ , so we may pick one. Let  $r < n/2$  denote the rank of  $G$ , and  $e_1 < e_2 < \dots < e_r$  the exponents. Let  $p > e_r$  be any prime and  $\mathbb{F}$  a finite field in characteristic  $\ell$  such that  $G$  is defined and split over  $\mathbb{F}$  and  $p$  divides the order of  $\mathbb{F}^{\times}$ . Let  $T$  be an  $\mathbb{F}$ -split maximal torus of  $G$ . We have

$$\mathrm{ord}_p |T(\mathbb{F})| = r \mathrm{ord}_p (|\mathbb{F}| - 1) = \sum_{i=1}^r \mathrm{ord}_p (|\mathbb{F}|^{e_i} - 1) = \mathrm{ord}_p |G(\mathbb{F})|,$$

so any  $p$ -Sylow subgroup of  $T(\mathbb{F})$  is a  $p$ -Sylow subgroup of  $G(\mathbb{F})$ . It follows that every  $p$ -Sylow of  $G(\mathbb{F})$  is abelian and generated by  $\leq r$  elements, and these properties are inherited by any finite  $p$ -subgroup of  $G(\mathbb{F})$  and therefore (letting  $\mathbb{F}$  grow) of  $G(\overline{\mathbb{F}}_{\ell})$ . It follows that no finite subgroup of  $G(\overline{\mathbb{F}}_{\ell})$  has a subquotient isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^{n/2}$ . By Lemma 3.3, for  $m$  sufficiently large,  $\ell^m - 1$  has a prime divisor  $p > e_r$ , so  $\mathrm{PSp}_n(\mathbb{F}_{\ell^m})$  has a subgroup isomorphic to  $(\mathbb{Z}/p\mathbb{Z})^{n/2}$ . It cannot, therefore, be a subquotient of  $G(\overline{\mathbb{F}}_{\ell})$ . □

Let  $\Gamma = \rho_{\Pi}(G_{\mathbb{Q}})$ . The image of  $\Gamma$  lies in  $\mathrm{GL}_n(K)$  for some  $\ell$ -adic field  $K$ . Since  $\rho_{\Pi}$  has positive weight, in order to prove that the Zariski-closure of  $\Gamma$  is  $\mathrm{GSp}_n$ , it suffices to prove that the closure contains  $\mathrm{Sp}_n$ . This follows from the following proposition:

**Proposition 6.2.** *Let  $K$  be a finite extension of  $\mathbb{Q}_{\ell}$  with residue field  $k$  and  $\Gamma$  denote a compact subgroup of  $\mathrm{GSp}_n(K) \subset \mathrm{GL}_n(K)$ . Suppose that some quotient of  $\Gamma$  is isomorphic to  $\mathrm{PSP}_n(\mathbb{F}_{\ell^m})$ . If  $m$  is sufficiently large, then the Zariski-closure of  $\Gamma$  contains  $\mathrm{Sp}_n$ .*

*Proof.* Let  $G$  denote the Zariski-closure of  $\Gamma$  in  $\mathrm{GL}_n$ . Let  $G^{\circ}$  denote the identity component of  $G$ . The following version of Jordan's theorem for algebraic groups seems to be well-known, but lacking a reference, we sketch the proof.

**Lemma 6.3.** *There exists a function  $J: \mathbb{N} \rightarrow \mathbb{N}$  such that every integer  $n > 0$  and every algebraic subgroup  $G \subset \mathrm{GL}_n$  over a field of characteristic zero, the component group  $H := G/G^{\circ}$  has a normal abelian subgroup of index  $\leq J(n)$ .*

*Proof.* We may (and do) assume without loss of generality that we are working over  $\mathbb{C}$ .

If  $\tilde{H}$  is an extension of  $H$  by a finite group, and  $\tilde{H}$  has a normal abelian subgroup  $\tilde{A}$  of index at most  $J(n)$ , then the image  $A$  of  $\tilde{A}$  in  $H$  is a normal abelian subgroup of index at most  $J(n)$ . It suffices to prove that for some finite extension  $\tilde{H}$  of  $H$ , the homomorphism  $\tilde{H} \rightarrow H$  lifts to  $\tilde{H} \rightarrow \mathrm{GL}_n(\mathbb{C})$ . Indeed Jordan's theorem for finite subgroups of  $\mathrm{GL}_n(\mathbb{C})$  then applies to  $\tilde{H}$ , and therefore to  $H$ . Lifting by stages, it suffices to prove this first in the case that  $G^{\circ}$  is adjoint semisimple, next when  $G^{\circ}$  is diagonal, and last when  $G^{\circ}$  is commutative and unipotent. For the first case, we note that the center of  $G^{\circ}(\mathbb{C})$  is trivial, so every extension of  $H$  by  $G^{\circ}(\mathbb{C})$  is a semidirect product. For the second, we note that  $H^2(H, D(\mathbb{C}))$  is annihilated by  $|H|$ , and therefore lies in the image of  $H^2(H, D(\mathbb{C})[[H]])$ . Any class in this latter cohomology group defines an extension of  $H$  by the finite abelian group  $D(\mathbb{C})[[H]]$ . Thus, every cohomology class in  $H^2(H, D(\mathbb{C}))$  can be trivialized by pullback to a finite abelian extension  $\tilde{H}$  of  $H$ . For the third, we note that  $H^2(H, V) = 0$  for every complex representation  $V$  of  $H$ , so there is no obstruction to lifting. □

Now, if  $0 \rightarrow G_1 \rightarrow G_2 \rightarrow G_3 \rightarrow 0$  is any short exact sequence of groups and  $G_2$  admits a surjective homomorphism to a finite simple group  $\Delta$ , then  $G_1$  maps to a normal subgroup of  $\Delta$ ; thus either  $G_1$  or  $G_3$

maps onto  $\Delta$ . Setting  $\Delta = \mathrm{PSp}_n(\mathbb{F}_{\ell^k})$  and assuming  $|\Delta| > J(n)$ , we see that the component group  $H$  cannot map to  $\Delta$ , and therefore  $G^\circ(K) \cap \Gamma$  must. Without loss of generality, therefore, we may assume that  $G$  is connected. If  $R$  denotes the radical of  $G$ , then  $R(K) \cap \Gamma$  is a normal solvable subgroup of  $\Gamma$ , so its image in  $\Delta$  is trivial. It follows that there exists a semisimple quotient  $G_s$  of  $G$  such that  $G_s(K)$  contains a compact subgroup  $\Gamma_s$  which admits a surjective homomorphism to  $\Delta$ . Replacing  $K$  with a finite extension  $L$ , we may assume that  $\Gamma_s$  stabilizes a hyperspecial vertex of the building of  $G_s$  over  $L$  ([Se2, Prop. 8], [Lar, Lemma 2.4]). It follows that there exists a smooth group scheme  $\mathcal{G}_s$  over the ring of integers  $\mathcal{O}_L$  of  $L$  with connected semisimple fibers such that  $\Gamma_s \subset \mathcal{G}_s(\mathcal{O}_L)$  and the generic fiber of  $\mathcal{G}_s$  is isomorphic to  $G_s$ . The kernel of the reduction map on  $\Gamma_s$  is a normal pro- $\ell$ -group of  $\Gamma_s$  whose image in  $\Delta$  must again be trivial. We conclude that the image of  $\Gamma_s$  under the reduction map admits a surjective homomorphism to  $\Delta$ . Let  $G_s^\ell$  denote the special fiber of  $\mathcal{G}_s$ . It is connected and semisimple, with the same Dynkin diagram as  $G_s$ . Moreover  $G_s^\ell(\overline{\mathbb{F}}_\ell)$  contains a subgroup which maps onto  $\Delta$ .

We assume that  $G_s$ , or equivalently  $G_s^\ell$ , is not symplectic of rank  $n/2$ . If the rank of  $G_s$  is  $n/2$  but  $G_s \neq \mathrm{Sp}_n$ , then by the classification of equal rank subgroups of  $\mathrm{Sp}_n$ ,  $G_s$  fails to be almost simple. In this case, we can replace  $G_s^\ell$  by an almost simple subquotient, whose rank is strictly less than  $n/2$ . In any case, as long as  $G_s \neq \mathrm{Sp}_n$ , we can find  $G_s^\ell$  with rank less than  $n/2$  such that  $G_s^\ell(\overline{\mathbb{F}}_\ell)$  contains a finite subgroup which maps onto  $\Delta = \mathrm{PSp}_n(\mathbb{F}_{\ell^m})$ . By Lemma 6.1, this cannot happen for  $m \gg 0$ . □

## 7. ACKNOWLEDGEMENTS

We are much indebted to Dragan Milićić, Dipendra Prasad, Peter Trapa and Nolan Wallach for their assistance, especially with real groups. We thank Michael Dettweiler for some helpful correspondence. We are indebted to Don Blasius and the anonymous referee for helpful feedback on the manuscript.

## REFERENCES

- [Atlas] Conway, J. H.; Curtis, R. T.; Norton, S. P.; Parker, R. A.; Wilson, R. A.: Atlas of finite groups. Maximal subgroups and ordinary characters for simple groups. With computational assistance from J. G. Thackray. Oxford University Press, Eynsham, 1985.

- [Bo1] A. Borel. Automorphic  $L$ -functions. Automorphic forms, representations and  $L$ -functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, pp. 27–61, Proc. Sympos. Pure Math., XXXIII, Amer. Math. Soc., Providence, R.I., 1979.
- [Bo2] Introduction to automorphic forms. Algebraic groups and discontinuous subgroups (Proc. Sympos. Pure Math., Boulder, 1965), pp. 199–210, Proc. Sympos. Pure Math., IX, Amer. Math. Soc., Providence, R.I., 1966.
- [Che] Gaëtan Chenevier. On number fields with given ramification. preprint.
- [Cl] Laurent Clozel. Représentations galoisiennes associées aux représentations automorphes autoduales de  $GL(n)$ . Inst. Hautes Études Sci. Publ. Math. No. 73 (1991), 97–145.
- [CC] Gaëtan Chenevier and Laurent Clozel. Corps de nombres peu ramifiés et formes automorphes autoduales. preprint.
- [C.K.P.S.] J. Cogdell, H. Kim, I.I. Piatetski-Shapiro, F. Shahidi. Functoriality for the classical groups. Publ. Math. Inst. Hautes Études Sci. No. 99 (2004), 163–233.
- [Det] M. Dettweiler. Galois realizations of classical groups and the middle convolution. preprint available at [math.NT/0605381](http://math.NT/0605381).
- [HT] M. Harris, R. Taylor. The geometry and cohomology of some simple Shimura varieties. Annals of Mathematics Studies, 151. Princeton University Press, Princeton, NJ, 2001. viii+276 pp.
- [Hu] James E. Humphreys: Conjugacy classes in semisimple algebraic groups. Mathematical Surveys and Monographs, **43**. American Mathematical Society, Providence, RI, 1995.
- [JS1] D. Jiang, D. Soudry. The local converse theorem for  $SO(2n + 1)$  and applications. *Ann. of Math. (2)* **157** (2003), no. 3, 743–806.
- [JS2] D. Jiang, D. Soudry. Generic representations and local Langlands reciprocity law for  $p$ -adic  $SO_{2n+1}$ . Contributions to automorphic forms, geometry, and number theory, 457–519, Johns Hopkins Univ. Press, Baltimore, MD, 2004.
- [Kos] B. Kostant: On Whittaker vectors and representation theory. *Invent. Math.* **48** (1978), 101–184.
- [Kot] R. Kottwitz. On the  $\lambda$ -adic representations associated to some simple Shimura varieties. *Invent. Math.* **108** (1992), no. 3, 653–665.
- [KW] Chandrashekhara Khare and Jean-Pierre Wintenberger: *Serre’s modularity conjecture (I)* preprint available at <http://www.math.utah.edu/~shekhar/papers.html>.
- [Lan] R. P. Langlands: On the classification of irreducible representations of real algebraic groups. *Representation theory and harmonic analysis on semisimple Lie groups*, 101–170, Math. Surveys Monogr., 31, Amer. Math. Soc., Providence, RI, 1989.
- [Lar] Michael Larsen: Maximality of Galois actions for compatible systems. *Duke Math. J.* **80** (1995), no. 3, 601–630.
- [LP] Michael Larsen and Richard Pink: Finite subgroups of algebraic groups. preprint available at <http://www.math.ethz.ch/~pink/publications.html>
- [Mi] D. Miličević, *Asymptotic behavior of matrix coefficients of the discrete series*, Duke Math. Journal, **44** (1977), 59 - 88.

- [Moy] Allen Moy. The irreducible orthogonal and symplectic Galois representations of a  $p$ -adic field (the tame case). *Journal of Number Theory* **10** (1984), 341–344.
- [PR] D. Prasad, D. Ramakrishnan. On the self-dual representations of division algebras over local field. preprint available at <http://www.math.tifr.res.in/~dprasad>
- [PS] D. Prasad, R. Schulze-Pillot. Generalised form of a conjecture of Jacquet and a local consequence. preprint available at <http://www.math.tifr.res.in/~dprasad>
- [Se] J-P. Serre: Groupes algébriques associés aux modules de Hodge-Tate. Journées de Géométrie Algébrique de Rennes, Astérisque **65** (1979), 155–188.
- [Se2] J-P. Serre: Exemples de plongements des groupes  $\mathrm{PSL}_2(\mathbb{F}_p)$  dans des groupes de Lie simples. *Invent. Math.* **124** (1996), no. 1-3, 525–562.
- [Sha] Freydoon Shahidi. A proof of Langlands’ conjecture on Plancherel measures; complementary series for  $p$ -adic groups. *Ann. Fac. Sci. Toulouse Math.* **132** (1990), no. 2, 273–330.
- [St] Robert Steinberg: Endomorphisms of linear algebraic groups. Memoirs of the American Mathematical Society, No. 80 American Mathematical Society, Providence, R.I., 1968.
- [Tay] Richard Taylor. Galois representations. *Ann. Fac. Sci. Toulouse Math.* **13** (2004), 73–119.
- [Vo] David Vogan: Gel’fand-Kirillov dimension for Harish-Chandra modules. *Invent. Math.* **48** (1978), no. 1, 75–98.
- [Wal] N. Wallach, *Real reductive Groups, I and II*. Pure and Applied Mathematics 132. Academic Press, San Diego, 1992.
- [War] G. Warner, *Harmonic Analysis on Semi-Simple Lie Groups II*, Springer-Verlag, New York, 1972.
- [Was] Lawrence C. Washington: *Introduction to cyclotomic fields*. Graduate Texts in Mathematics, 83. Springer-Verlag, New York, 1982.
- [Wiese] Gabor Wiese. On projective linear groups over finite fields as Galois groups over the rational numbers. preprint available at <http://xxx.lanl.gov/abs/math.NT/0606732>

*E-mail address:* shekhar@math.ucla.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF UTAH, 155 SOUTH 1400 EAST, ROOM 233, SALT LAKE CITY, UT 84112-0090, U.S.A., AND DEPARTMENT OF MATHEMATICS, UCLA, LOS ANGELES, CA 90095-1555, U.S.A.

*E-mail address:* larsen@math.indiana.edu

DEPARTMENT OF MATHEMATICS, INDIANA UNIVERSITY, BLOOMINGTON, IN 47405, U.S.A.

*E-mail address:* savin@math.utah.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF UTAH, 155 SOUTH 1400 EAST, ROOM 233, SALT LAKE CITY, UT 84112-0090, U.S.A.