

# JOURNAL

de Théorie des Nombres  
de BORDEAUX

*anciennement Séminaire de Théorie des Nombres de Bordeaux*

Alexandru GHITZA et Takuya YAMAUCHI

**Automorphy of mod 2 Galois representations associated to certain genus 2 curves over totally real fields**

Tome 36, n° 2 (2024), p. 637-660.

<https://doi.org/10.5802/jtnb.1291>

© Les auteurs, 2024.



Cet article est mis à disposition selon les termes de la licence  
CREATIVE COMMONS ATTRIBUTION – PAS DE MODIFICATION 4.0 FRANCE.  
<http://creativecommons.org/licenses/by-nd/4.0/fr/>



*Le Journal de Théorie des Nombres de Bordeaux est membre du  
Centre Mersenne pour l'édition scientifique ouverte*

<http://www.centre-mersenne.org/>

e-ISSN : 2118-8572

# Automorphy of mod 2 Galois representations associated to certain genus 2 curves over totally real fields

par ALEXANDRU GHITZA et TAKUYA YAMAUCHI

RÉSUMÉ. Soit  $C$  une courbe hyperelliptique de genre 2 sur un corps totalement réel  $F$ . Nous montrons que la représentation galoisienne modulo 2,  $\bar{\rho}_{C,2}: \text{Gal}(\bar{F}/F) \rightarrow \text{GSp}_4(\mathbb{F}_2)$ , associée à  $C$  est résiduellement automorphe lorsque l'image de  $\bar{\rho}_{C,2}$  est un groupe isomorphe à  $S_5$  et transitif par rapport à un isomorphisme fixé  $\text{GSp}_4(\mathbb{F}_2) \simeq S_6$ . Plus précisément, il existe une forme parabolique  $h$  de Hilbert–Siegel sur  $\text{GSp}_4(\mathbb{A}_F)$  de poids parallèle 2, propre pour les opérateurs de Hecke, dont la représentation galoisienne  $\bar{\rho}_{h,2}$  est isomorphe à  $\bar{\rho}_{C,2}$ .

ABSTRACT. Given a genus two hyperelliptic curve  $C$  over a totally real field  $F$ , we show that the mod 2 Galois representation  $\bar{\rho}_{C,2}: \text{Gal}(\bar{F}/F) \rightarrow \text{GSp}_4(\mathbb{F}_2)$  attached to  $C$  is residually automorphic when the image of  $\bar{\rho}_{C,2}$  is isomorphic to  $S_5$  and it is also a transitive subgroup under a fixed isomorphism  $\text{GSp}_4(\mathbb{F}_2) \simeq S_6$ . More precisely, there exists a Hilbert–Siegel Hecke eigen cusp form  $h$  on  $\text{GSp}_4(\mathbb{A}_F)$  of parallel weight two whose mod 2 Galois representation  $\bar{\rho}_{h,2}$  is isomorphic to  $\bar{\rho}_{C,2}$ .

## 1. Introduction

Let  $K$  be a number field in an algebraic closure  $\bar{\mathbb{Q}}$  of  $\mathbb{Q}$  and  $p$  be a prime number. In proving automorphy of a given geometric  $p$ -adic Galois representation

$$\rho: G_K := \text{Gal}(\bar{\mathbb{Q}}/K) \longrightarrow \text{GL}_n(\bar{\mathbb{Q}}_p),$$

a first step would be, typically, to observe residual automorphy of its mod  $p$  reduction

$$\bar{\rho}: G_K \longrightarrow \text{GL}_n(\bar{\mathbb{F}}_p)$$

obtained after choosing a suitable integral lattice. However, proving residual automorphy of  $\bar{\rho}$  is hard unless the image of  $\bar{\rho}$  is reasonable so that one can apply the current results in the theory of automorphic representations. For instance, if the image is solvable, one can use the Langlands base change

---

Manuscrit reçu le 27 décembre 2022, révisé le 29 juin 2023, accepté le 12 juillet 2023.

2020 *Mathematics Subject Classification*. 11F, 11F33, 11F80.

*Mots-clefs*. genus 2 curves, mod 2 Galois representations, automorphy.

The second author is partially supported by JSPS KAKENHI Grant Number (B) No.19H01778.

argument to find an automorphic cuspidal representation as is done in many known cases (cf. [11, 29, 35, 42, 45]). Another natural problem is to find geometric objects whose residual Galois representations have suitably small images in question so that one can apply the various known results for automorphy of Galois representations.

In this paper, we study residual automorphy of mod 2 Galois representations associated to certain hyperelliptic curves of genus 2. Let us fix some notation to explain our results. Let  $F$  be a totally real field and fix an embedding  $F \subset \overline{\mathbb{Q}}$ . Let us consider the hyperelliptic curve over  $F$  of genus 2 defined by

$$(1.1) \quad C: \quad y^2 = f(x) := x^6 + a_1x^5 + \cdots + a_5x + a_6, \quad a_1, \dots, a_6 \in F.$$

Let  $D_f$  be the discriminant of  $f$ . If we write  $f(x) = \prod_{i=1}^6(x - \alpha_i)$  over  $\overline{\mathbb{Q}}$ , then  $D_f = \prod_{1 \leq i < j \leq 6}(\alpha_i - \alpha_j)^2$ . By abusing the notation, we also denote by  $C$  a unique smooth completion of the above hyperelliptic curve. Let  $J = \text{Jac}(C)$  be the Jacobian variety of  $C$  and for each positive integer  $n$ , let  $J[n]$  be the group scheme of  $n$ -torsion points. Let  $T_{J,2}$  be the 2-adic Tate module over  $\mathbb{Z}_2$  associated to  $J$ . Let  $\langle *, * \rangle: T_{J,2} \times T_{J,2} \rightarrow \mathbb{Z}_2(1)$  be the Weil pairing, which is  $G_F$ -equivariant, perfect, and alternating. It yields an integral 2-adic Galois representation

$$\rho_{C,2}: G_F \longrightarrow \text{GSp}(T_{J,2}, \langle *, * \rangle) \simeq \text{GSp}_4(\mathbb{Z}_2)$$

where the algebraic group  $\text{GSp}_4 = \text{GSp}_J$  is the symplectic similitude group in  $\text{GL}_4$  associated to  $\begin{pmatrix} 0_2 & s \\ -s & 0_2 \end{pmatrix}$ ,  $s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Put

$$\overline{T}_{J,2} = T_{J,2} \otimes_{\mathbb{Z}_2} \mathbb{F}_2 = J[2](\overline{\mathbb{Q}}).$$

This yields a mod 2 Galois representation

$$(1.2) \quad \overline{\rho}_{C,2}: G_F \longrightarrow \text{GSp}(\overline{T}_{J,2}, \langle *, * \rangle_{\mathbb{F}_2}) \simeq \text{GSp}_4(\mathbb{F}_2).$$

On the other hand, we can embed the Galois group  $\text{Gal}(F_f/F)$  of the splitting field of  $f$  over  $F$  into  $S_6$  by permutation of the roots of  $f(x)$ ; we denote this embedding by  $\iota_f: \text{Gal}(F_f/F) \hookrightarrow S_6$ . Here  $S_n$  stands for the  $n$ -th symmetric group. Since  $\overline{T}_{J,2}$  is generated (cf. [33]) by divisors associated to the points  $(x, 0)$  in  $C(\overline{\mathbb{Q}})$ ,  $\overline{\rho}_{C,2}$  factors through  $\text{Gal}(F_f/F)$ ; we denote it by  $\overline{\rho}_{C,2}: \text{Gal}(F_f/F) \hookrightarrow \text{GSp}_4(\mathbb{F}_2)$  again. A subgroup  $H$  of  $S_6$  is transitive if it acts on the set  $\{1, 2, 3, 4, 5, 6\}$  transitively. Let us fix an isomorphism  $\text{GSp}_4(\mathbb{F}_2) \simeq S_6$  commuting with  $\overline{\rho}_{C,2}$  and  $\iota_f$ .

In this situation we will prove the following:

**Theorem 1.1.** *Keep the notation as above. Suppose that  $\text{Im}(\overline{\rho}_{C,2}) \simeq S_5$  and it is a transitive subgroup of  $S_6$  via the fixed isomorphism between  $\text{GSp}_4(\mathbb{F}_2)$  and  $S_6$ . Further assume that for any complex conjugation  $c$  in  $G_F$ ,  $\overline{\rho}_{C,2}(c)$  is of type  $(2, 2)$  as an element of  $S_5$ . Then there exists a Hilbert–Siegel Hecke*

eigen cusp form  $h$  on  $\mathrm{GSp}_4(\mathbb{A}_F)$  of parallel weight 2 such that  $\bar{\rho}_{h,2} \simeq \bar{\rho}_{C,2}$  as a representation to  $\mathrm{GL}_4(\overline{\mathbb{F}}_2)$ , where  $\bar{\rho}_{h,2}$  is the reduction modulo 2 of the 2-adic representation  $\rho_{h,2}$  associated to  $h$  (see Section 3.1 for  $\rho_{h,2}$ ).

We give some remarks on the above theorem. The transitivity of the image implies  $f(x)$  is irreducible over  $F$ . Put  $L = F(\sqrt{D_f})$ . It is corresponding to the kernel of  $\mathrm{sgn} \circ \iota_f \circ \bar{\rho}_{C,2}: G_F \rightarrow \{\pm 1\}$  where  $\mathrm{sgn}: S_6 \rightarrow \{\pm 1\}$  is the usual sign character. The assumption on  $\bar{\rho}_{C,2}(c)$  shows  $f(x)$  has only two real roots and the other four complex roots are permuted by an element of type  $(2, 2)$  in  $S_6$ . Therefore,  $D_f \in F$  is totally real and it is not a square element since  $\mathrm{Im}(\bar{\rho}_{C,2}) \simeq S_5$ . In conclusion,  $L/F$  is a totally real quadratic extension. Then it will turn out that  $\bar{\rho}_{C,2}$  is an induced representation to  $G_F$  of a certain totally odd 2-dimensional mod 2 Galois representation  $\bar{\tau}: G_L \rightarrow \mathrm{GL}_2(\overline{\mathbb{F}}_2)$  whose image is isomorphic to  $A_5$ . Applying Sasaki’s result [34] (or Pilloni–Stroh’s result [28]), the Jacquet–Langlands correspondence, and a suitable congruence method, one can find a Hilbert cusp form  $g$  of parallel weight 2 on  $\mathrm{GL}_2(\mathbb{A}_L)$  whose corresponding mod 2 Galois representation  $\bar{\rho}_{g,2}$  is isomorphic to  $\bar{\tau}$ . Then the theta lift of the corresponding automorphic representation  $\pi_g$  to  $\mathrm{GSp}_4(\mathbb{A}_F)$  yields a cuspidal automorphic representation  $\Pi$  of  $\mathrm{GSp}_4(\mathbb{A}_F)$  which is generated by a Hilbert–Siegel Hecke eigen cusp form  $h$  of parallel weight 2 on  $\mathrm{GSp}_4(\mathbb{A}_F)$ . By Theorem 1.1 of [44], for each  $p$  in a set of primes of Dirichlet density one, the Hodge–Tate weights at  $p$  of the  $p$ -adic Galois representation attached to  $\Pi$  are  $\{0, 0, 1, 1\}$ . It is also true for  $p = 2$  when  $\Pi_2$  is unramified and the roots of the 2-nd Hecke polynomial of  $\Pi$  are pairwise distinct (see Theorem 3.3 of [44]). On the other hand, the Hodge–Tate weights of  $\rho_{C,2}$  at the place dividing 2 are always  $\{0, 0, 1, 1\}$  and this is why we seek a form  $h$  of such weight.

We note that  $J$  is potentially automorphic by Theorem 1.1.3 of [7] and the potential version of Theorem 1.1 is already known in a more general setting.

**Remark 1.2.**

- (1) The construction of Hilbert–Siegel modular forms in Theorem 1.1 is similar to the one in [41]. However, to apply theta lifting to  $\mathrm{GSp}_4$ , we need to carefully look at the central characters after a congruence method (see Proposition 3.8).
- (2) In the main theorem, we do not specify the levels of the Hilbert–Siegel forms because of the lack of level-lowering results (see Remark 3.9). However,  $h$  could be a paramodular form by using the method of [22] at least when  $F = \mathbb{Q}$  so that the situation is compatible with the paramodular conjecture [8, Conjecture 1.4].

- (3) In the course of the proof for the main theorem, we do not use the results in [17] to associate a form with a Galois representation though it is necessary to state Theorem 3.1. Instead, we apply the unconditional result in [30] to construct a corresponding automorphic cuspidal representation. Hence Theorem 1.1 is true unconditionally.
- (4) The central character of  $h$  can be read off from Theorem 3.6 and Proposition 3.8.
- (5) We can weaken the condition on the image of  $\bar{\rho}_{C,2}$  by requiring that the image be isomorphic to  $F_{20} := C_4 \times C_5$ , or isomorphic to  $A_5$  with  $F/\mathbb{Q}$  of even degree. In the  $F_{20}$  case, we have a similar cuspidal representation. In the  $A_5$  case,  $\bar{\rho}_{C,2}$  is reducible so we can naively attach a non-cuspidal automorphic representation. By using a congruence method, we may hope to obtain a cuspidal representation in either case but we do not pursue it in this article.

This paper is organized as follows. In Section 2, we consider some basic facts about mod 2 Galois representations to  $\mathrm{GSp}_4(\mathbb{F}_2)$ . We devote Section 3 to the study of the automorphic forms in question and to various congruences between several types automorphic forms, and apply this to the proof of automorphy of our representations in 3.3. Finally, in Section 4 we describe how to obtain explicit families of examples using two constructions: the first coming from a classical result of Hermite, and the second from 5-division points on elliptic curves following Goins [19].

## 2. Certain mod 2 Galois representations to $\mathrm{GSp}_4(\mathbb{F}_2)$

In this section, we study some properties of mod 2 Galois representations to  $\mathrm{GSp}_4(\mathbb{F}_2)$ . We refer to [9, Section 5] and [41, Section 3]. We denote by  $S_n$  the  $n$ -th symmetric group, by  $A_n$  the  $n$ -th alternating group, and by  $C_n$  the cyclic group of order  $n$ .

**2.1.  $\mathrm{GSp}_4$ .** Let us introduce the smooth group scheme  $\mathrm{GSp}_4 = \mathrm{GSp}_J$  over  $\mathbb{Z}$  which is defined as the symplectic similitude group in  $\mathrm{GL}_4$  associated to  $J := \begin{pmatrix} 0_2 & s \\ -s & 0_2 \end{pmatrix}$ ,  $s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ . Explicitly,

$$\mathrm{GSp}_4 = \left\{ X \in \mathrm{GL}_4 \mid {}^t X J X = \nu(X) J, \exists \nu(X) \in \mathrm{GL}_1 \right\}.$$

Put  $\mathrm{Sp}_4 = \mathrm{Ker}(\nu: \mathrm{GSp}_4 \rightarrow \mathrm{GL}_1, X \mapsto \nu(X))$ .

**2.2. An identification between  $\mathrm{GSp}_4(\mathbb{F}_2)$  and  $S_6$ .** Let  $s: \mathbb{F}_2^6 \rightarrow \mathbb{F}_2$  be the linear functional defined by  $s(x_1, \dots, x_6) = x_1 + \dots + x_6$ . Put  $V = \{x \in \mathbb{F}_2^6 \mid s(x) = 0\}$  and  $W = V/U$  where  $U = \langle (1, 1, 1, 1, 1, 1) \rangle$ . Let us consider the bilinear form on  $\mathbb{F}_2^6$  given by the formula

$$\langle x, y \rangle = x_1 y_1 + \dots + x_6 y_6, \quad x, y \in \mathbb{F}_2^6.$$

It induces a non-degenerate, alternating pairing  $\langle *, * \rangle_W$  on  $W$ , where being alternating means that  $\langle x, x \rangle_W = 0$  for each  $x \in W$ . The symmetric group  $S_6$  acts naturally on  $\mathbb{F}_2^6$  and it yields a group homomorphism

$$\varphi: S_6 \longrightarrow \mathrm{GSp}_{\mathbb{F}_2}(W, \langle *, * \rangle_W) \simeq \mathrm{GSp}_4(\mathbb{F}_2).$$

The action of  $S_6$  on  $W$  is faithful. In fact, we can check it only for (12) and (123456) generating  $S_6$ . By direct computation,

$$|\mathrm{GSp}_4(\mathbb{F}_2)| = \mathrm{Sp}_4(\mathbb{F}_2) = 720 = |S_6|$$

and therefore,  $\varphi$  is an isomorphism.

It is easy to find a basis of  $W$ . For instance, we see that

$$(2.1) \quad \begin{aligned} e_1 &= (1, 1, 0, 0, 0, 0), & e_2 &= (0, 0, 0, 1, 1, 0), \\ e_3 &= (0, 0, 0, 1, 0, 1), & e_4 &= (1, 0, 1, 0, 0, 0) \end{aligned}$$

form a basis of  $W$ . The representation matrices with respect to the above basis for the generators (12) and (123456) of  $S_6$  are given respectively as follows:

$$(2.2) \quad \left( \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right), \quad \left( \begin{array}{cccc} 1 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{array} \right).$$

**2.3.  $S_5$ -representations to  $\mathrm{GSp}_4(\mathbb{F}_2)$ .** It follows from [9, Section 5] (in particular, the table in Lemma 5.1.7 in loc. cit.) that, up to conjugacy, there are two embeddings from  $S_5$  to  $\mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$  which are absolutely irreducible as representations to  $\mathrm{GL}_4(\overline{\mathbb{F}}_2)$ . We denote the images by  $S_5(a), S_5(b)$  respectively; they are characterized in terms of the trace as follows:

- (1) (type  $S_5(a)$ ) the elements of order 3 have trace 0 and are of type (3, 3),
- (2) (type  $S_5(b)$ ) the elements of order 3 have trace 1 and are of type (3).

Under the identification  $\mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$ , these subgroups are given explicitly as

$$(2.3) \quad \begin{aligned} S_5(a) &= \langle \sigma_6 := (12346), \sigma_{23} := (12)(34)(56) \rangle, \\ S_5(b) &= \{ \sigma \in S_6 \mid \sigma(6) = 6 \}. \end{aligned}$$

Notice that  $\sigma_{23}(\sigma_6\sigma_{23}\sigma_6^{-1})$  is of type (3, 3) and  $(\sigma_6\sigma_{23})^2 = (16)(35)$  is obviously of type (2, 2) which is explicitly given by  $\begin{pmatrix} 0 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 \end{pmatrix}$  with respect to the basis (2.1). By direct computation, one can check it is conjugate to  $J$  by  $\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \in \mathrm{GSp}_4(\mathbb{F}_2)$ .

Let  $G$  be a group and  $\bar{\rho}: G \rightarrow \mathrm{GSp}_4(\mathbb{F}_2)$  a representation of  $G$ . Since any element of  $\mathrm{GSp}_4(\mathbb{F}_2) = \mathrm{Sp}_4(\mathbb{F}_2)$  has determinant one,  $\bar{\rho}$  is automatically self-dual.

**Lemma 2.1.** *Assume that  $\text{Im}(\bar{\rho}) \simeq S_5$ . Then  $\bar{\rho}$  is absolutely irreducible. Furthermore, there exist an index 2 subgroup  $H$  of  $G$ , a generator  $\iota$  of  $G/H$ , and an absolutely irreducible representation  $\bar{\tau}: H \rightarrow \text{GL}_2(\mathbb{F}_4)$  which is not equivalent to  ${}^t\bar{\tau}$  defined by  ${}^t\bar{\tau}(h) = \bar{\tau}(\iota h \iota^{-1})$  for each  $h \in H$  such that*

- (1)  $\text{Im}(\bar{\tau}) = \text{SL}_2(\mathbb{F}_4) \simeq A_5$ ;
- (2) if  $\text{Im}(\bar{\rho})$  is of type  $S_5(a)$ , then  $\bar{\rho} \simeq \text{Ind}_H^G \bar{\tau}$ ;
- (3) if  $\text{Im}(\bar{\rho})$  is of type  $S_5(b)$ , then  $\bar{\rho}$  is isomorphic to a twisted tensor product with respect to  $G/H$  (see [41, Section 3]).

*Proof.* Put  $H := \bar{\rho}^{-1}(A_5)$ . Clearly it is a subgroup of  $G$  of index 2. Since  $\text{Im}(\bar{\rho}) \simeq S_5$ , by Dickson’s result [43, p. 128, (2.1)],  $\bar{\rho}$  is absolutely irreducible. Then by Clifford’s theorem, it follows that  $\bar{\rho}|_H$  is either absolutely irreducible (by Dickson’s result again) or a sum of two 2-dimensional irreducible representations  $\bar{\tau}, \bar{\tau}': G \rightarrow \text{GL}_2(\mathbb{F}_2)$  after base extension to  $\mathbb{F}_2$ . In the latter case, by Schur’s Lemma and Frobenius reciprocity,

$$1 \leq \dim \text{Hom}_H(\bar{\rho}|_H, \bar{\tau}) = \dim \text{Hom}_G(\bar{\rho}, \text{Ind}_H^G \bar{\tau}) \leq 1,$$

therefore both have the same dimension and  $\bar{\rho}$  is irreducible. Further, irreducibility implies that  $\tau$  cannot be isomorphic to  ${}^t\bar{\tau}$ . Since  $A_5 \simeq \text{SL}_2(\mathbb{F}_4)$  (cf. [41, Section 3.3]), we may assume  $\bar{\tau}$  takes values in  $\mathbb{F}_4$  as desired. Further, by using (2.2) and (2.3), one can distinguish the types in terms of the trace.

The remaining (absolutely irreducible) case follows from [41, Proposition 3.5(1)]. □

Fix an isomorphism  $\text{GSp}_4(\mathbb{F}_2) \simeq S_6$  as in Section 2.2.

**Remark 2.2.** Keep the notation as above (recall that  $\text{Im}(\bar{\rho}) \simeq S_5$ ). The type of the image  $\text{Im}(\bar{\rho})$  can also be characterized in the following way:

- (1) (type  $S_5(a)$ ) it is a transitive subgroup of  $S_6$ ;
- (2) (type  $S_5(b)$ ) it is not transitive, hence up to conjugacy, it fixes 6 as a subgroup of  $S_6$ .

In this article, we focus on the case of type  $S_5(a)$ ; the other case is studied in [41].

**Proposition 2.3.** *Let  $F$  be a totally real field. Let  $\bar{\rho}: G_F \rightarrow \text{GSp}_4(\mathbb{F}_2)$  be an irreducible mod 2 Galois representation. Suppose that  $\text{Im}(\bar{\rho})$  is of type  $S_5(a)$ . Assume further that for each complex conjugation  $c$  of  $G_F$ ,  $\bar{\rho}(c)$  is of type  $(2, 2)$ . Then there exist a totally real quadratic extension  $L/F$  with  $\text{Gal}(L/F) = \langle \iota \rangle$  and an irreducible totally odd Galois representation  $\bar{\tau}: G_L \rightarrow \text{GL}_2(\mathbb{F}_4)$  which is not equivalent to  ${}^t\bar{\tau}$  satisfying*

- (1)  $\text{Im}(\bar{\tau}) \simeq \text{SL}_2(\mathbb{F}_4) \simeq A_5$ ;

(2)  $\bar{\rho} \simeq \text{Ind}_{G_L}^{G_F} \bar{\tau}$  as a representation to  $\text{GL}_4(\mathbb{F}_4)$ ;

(3) for each complex conjugation  $c$  of  $G_F$ ,  $\bar{\rho}(c)$  is conjugate to  $s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ .

Here the totally odd-ness for  $\bar{\tau}$  exactly means the third condition above.

*Proof.* Let  $L/F$  be the quadratic extension corresponding to the sign character  $\text{sgn}: \text{Im}(\bar{\rho}) \simeq S_5 \rightarrow \{\pm 1\}$ . By assumption  $L/F$  is a totally real quadratic extension and we have  $\bar{\rho}(G_L) \simeq A_5$  (see the explanation right after Theorem 1.1). The first two claims follow from Lemma 2.1. Further, by assumption, for each complex conjugation  $c$  of  $G_F$ ,  $\bar{\rho}(c)$  is conjugate to  $J$  (see the paragraph right after (2.3)). The third claim follows from this.  $\square$

### 3. Automorphy

Fix an embedding  $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$  and an isomorphism  $\bar{\mathbb{Q}}_p \simeq \mathbb{C}$  for each prime  $p$ . Let  $\iota = \iota_p: \bar{\mathbb{Q}} \rightarrow \bar{\mathbb{Q}}_p$  be an embedding that is compatible with the maps  $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$  and  $\bar{\mathbb{Q}}_p \simeq \mathbb{C}$  fixed above.

**3.1. Automorphic Galois representations.** Let  $F$  be a totally real field. For each place  $v$  of  $F$ , let  $F_v$  be the completion of  $F$  at  $v$ . In this section we recall basic properties of cuspidal automorphic representations of  $\text{GSp}_4(\mathbb{A}_F)$  such that each infinite component is a (limit of) discrete series representation. We basically follow the notation of Mok’s article [27] and add ingredients necessary for our purpose.

For any place  $v$  of  $F$ , we denote by  $W_{F_v}$  the Weil group of  $F_v$ . Let  $m_1, m_2, w$  be integers such that

$$m_1 > m_2 \geq 0 \quad \text{and} \quad m_1 + m_2 \equiv w + 1 \pmod{2}.$$

Let  $a = (m_1 + m_2)/2$ ,  $b = (m_1 - m_2)/2$ , and consider the  $L$ -parameter  $\phi_{(w;m_1,m_2)}: W_{\mathbb{R}} \rightarrow \text{GSp}_4(\mathbb{C})$  defined by

$$(3.1) \quad \phi_{(w;m_1,m_2)}(z) = |z|^{-w} \text{diag} \left( \left(\frac{z}{\bar{z}}\right)^a, \left(\frac{z}{\bar{z}}\right)^b, \left(\frac{z}{\bar{z}}\right)^{-b}, \left(\frac{z}{\bar{z}}\right)^{-a} \right)$$

and

$$\phi_{(w;m_1,m_2)}(j) = \begin{pmatrix} 0_2 & s \\ (-1)^{w+1} s & 0_2 \end{pmatrix}, \quad s = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}.$$

The archimedean  $L$ -packet  $\Pi(\phi_{(w;m_1,m_2)})$  corresponding to  $\phi_{(w;m_1,m_2)}$  under the Local Langlands Correspondence consists of two elements

$$\left\{ \pi_{(w;m_1,m_2)}^H, \pi_{(w;m_1,m_2)}^W \right\}$$

whose central characters both satisfy  $z \mapsto z^{-w}$  for  $z \in \mathbb{R}_{>0}^{\times}$ . These are essentially tempered unitary representations of  $\text{GSp}_4(\mathbb{R})$  and tempered exactly when  $w = 0$ . Let  $K$  be a maximal compact subgroup of  $\text{Sp}_4(\mathbb{R})$ . When  $m_2 \geq 1$  (resp.  $m_2 = 0$ ) the representation  $\pi_{(w;m_1,m_2)}^H$  is called a



(resp. limit of) holomorphic discrete series representation of minimal  $K$ -type  $\underline{k} = (k_1, k_2) := (m_1 + 1, m_2 + 2)$  which corresponds to an algebraic representation  $V_{\underline{k}} := \text{Sym}^{k_1 - k_2} \text{St}_2 \otimes \det^{k_2} \text{St}_2$  of  $K_{\mathbb{C}} = \text{GL}_2(\mathbb{C})$  where  $\text{St}_2$  stands for the 2-dimensional standard algebraic representation of  $K_{\mathbb{C}}$ . If  $m_2 \geq 1$  (resp.  $m_2 = 0$ ), the representation  $\pi_{(w; m_1, m_2)}^W$  is called a (resp. limit of) large (or generic) discrete series representation of minimal  $K$ -type  $V_{(m_1+1, -m_2)}$ . We say that a cuspidal automorphic representation  $\pi$  of  $\text{GSp}_4(\mathbb{A}_F)$  is regular if for each infinite place  $v$ ,  $\pi_v$  is a discrete series representation.

Fix an integer  $w$ . Let  $\pi = \otimes'_v \pi_v$  be an automorphic cuspidal representation of  $\text{GSp}_4(\mathbb{A}_F)$  such that for each infinite place  $v$ ,  $\pi_v$  has  $L$ -parameter  $\phi_{(w; m_{1,v}, m_{2,v})}$  with the parity condition  $m_{1,v} + m_{2,v} \equiv w + 1 \pmod{2}$ . Let  $\text{Ram}(\pi)$  be the set of all finite places at which  $\pi_v$  is ramified.

For the existence of Galois representations attached to regular algebraic self-dual cuspidal representations for general linear groups, see Theorem 1.1 of [1], which is the main reference for knowing the main contributors (Harris–Taylor, Shin, and others) as well as the latest results up to the time when loc. cit. appeared. In order to attach Galois representations for  $\text{GSp}_4$ , both Sorensen [38] and Mok [27] use Langlands functoriality from  $\text{GSp}_4$  to  $\text{GL}_4$  and reduce the problem to the known cases for general linear groups (specifically  $\text{GL}_4$ ). Sorensen focused on the case when the representation at any infinite place is generic (large discrete series) while Mok treated the limit of discrete series via a congruence method. Mok relied on results of Arthur that were at the time expected but not yet proved, and which are now guaranteed by [17] though remaining conditional on Arthur’s classification. We summarize here the known results taken from Theorem 3.1 (for the regular case) and Theorem 4.14 of [27] (see also Theorem 3.1 and Theorem 3.3 of [44] as a good summary):

**Theorem 3.1.** *Assume that  $\pi$  is neither CAP nor endoscopic. For each prime  $p$  and  $\iota_p: \overline{\mathbb{Q}}_p \xrightarrow{\sim} \mathbb{C}$  there exists a continuous, semisimple Galois representation  $\rho_{\pi, \iota_p}: G_F \rightarrow \text{GSp}_4(\overline{\mathbb{Q}}_p)$  such that*

- (1)  $\nu \circ \rho_{\pi, \iota_p}(c_{\infty}) = -1$  for any complex conjugation  $c_{\infty}$  in  $G_F$ .
- (2)  $\rho_{\pi, \iota_p}$  is unramified at all finite places that do not belong to the set  $\text{Ram}(\pi) \cup \{v|p\}$ ;
- (3) for each finite place  $v$  not lying over  $p$ , the local-global compatibility holds:

$$\text{rec}_v^{\text{GT}} \left( \pi_v \otimes |\nu|^{-\frac{3}{2}} \right) \simeq \begin{cases} \text{WD}(\rho_{\pi, \iota_p}|_{G_{F_v}})^{F\text{-ss}} & \text{if } \pi \text{ is regular,} \\ \text{WD}(\rho_{\pi, \iota_p}|_{G_{F_v}})^{\text{ss}} & \text{otherwise,} \end{cases}$$

with respect to  $\iota_p$ , where  $\text{rec}_v^{\text{GT}}$  stands for the local Langlands correspondence constructed by Gan–Takeda [16];

- (4) for each  $v|p$  and each embedding  $\sigma: F_v \hookrightarrow \overline{\mathbb{Q}}_p$ , let  $v_\sigma: F \hookrightarrow \mathbb{C}$  denote the embedding  $v_\sigma := \iota_p \circ \sigma|_F$ . Then the representation  $\rho_{\pi, \iota_p}|_{G_{F_v}}$  has Hodge–Tate weights

$$HT_\sigma(\rho_{\pi, \iota_p}|_{G_{F_v}}) = \{\delta_{v_\sigma}, \delta_{v_\sigma} + m_{2, v_\sigma}, \delta_{v_\sigma} + m_{1, v_\sigma}, \delta_{v_\sigma} + m_{2, v_\sigma} + m_{1, v_\sigma}\}$$

where  $\delta_{v_\sigma} = \frac{1}{2}(w + 3 - m_{1, v_\sigma} - m_{2, v_\sigma})$ ;

- (5) further,
- (a) if  $\pi_{v'}$  is discrete series for all infinite places  $v'$ , then for each finite place  $v$  of  $F$ ,  $\rho_{\pi, \iota_p}|_{G_{F_v}}$  is of de Rham and the local-global compatibility also holds up to Frobenius semi-simplification;
  - (b) for each finite place  $v$  such that  $\pi_v$  is unramified and the Satake parameters of  $\pi$  are distinct from each other,  $\rho_{\pi, \iota_p}|_{G_{F_v}}$  is crystalline and the local-global compatibility also holds up to semi-simplification.

**Remark 3.2.**

- (1) Regarding the fourth statement of the above theorem, when  $\pi$  is not regular, in general, we do not even know if  $\rho_{\pi, \iota_p}|_{G_{F_v}}$  is Hodge–Tate for each  $v|p$  such that  $\pi_{v_\sigma}$  is not discrete series. We remark that the case (b) of the fifth claim follows from [44, Theorem 3.3(vi)]. (see Remark 3.4 of [44]).
- (2) A priori, by construction,  $\rho_{\pi, \iota_p}$  takes values in  $GL_4(\overline{\mathbb{Q}}_p)$ . However, by [3, Corollary 1.3], it factors through  $GSp_4(\overline{\mathbb{Q}}_p)$  as stated.
- (3) Notice  $3 - k_1 - k_2 = -(m_1 + m_2)$ . Regarding Theorem 3.1(3), if we put  $w = 0$  and consider the twist  $\pi_v \otimes |\nu|^{-\frac{3}{2}} \otimes |\nu|^{\delta_v} = \pi_v \otimes |\nu|^{\frac{3 - k_1 - k_2}{2}}$  which yields the setting in [44, Theorem 3.1(vii)]. Accordingly, our Hodge–Tate weights are also shifted by  $-\delta_{v_\sigma}$  and they give the Hodge–Tate weights in [44, Theorem 3.1(v)].

**Definition 3.3.**

- (1) Let  $\rho: G_F \rightarrow GSp_4(\overline{\mathbb{Q}}_p)$  be a  $p$ -adic Galois representation. We say  $\rho$  is automorphic if there exists a cuspidal automorphic representation  $\pi$  of  $GSp_4(\mathbb{A}_F)$  with  $\pi_v$  a (limit of) discrete series representation for any  $v|\infty$ , and such that  $\rho \simeq \rho_{\pi, \iota_p}$  as a representation to  $GL_4(\overline{\mathbb{Q}}_p)$ .
- (2) Let  $\bar{\rho}: G_F \rightarrow GSp_4(\overline{\mathbb{F}}_p)$  be an irreducible mod  $p$  Galois representation. We say  $\bar{\rho}$  is automorphic if there exists a cuspidal automorphic representation  $\pi$  of  $GSp_4(\mathbb{A}_F)$  with  $\pi_v$  a (limit of) discrete series representation for any  $v|\infty$ , and such that  $\bar{\rho} \simeq \bar{\rho}_{\pi, \iota_p}$  as a representation to  $GL_4(\overline{\mathbb{F}}_p)$ .

**Remark 3.4.** Let  $h$  be a holomorphic Hilbert–Siegel Hecke eigen cusp form on  $GSp_4(\mathbb{A}_F)$  of parallel weight 2. Let  $\pi_h$  be the corresponding cuspidal automorphic representation of  $GSp_4(\mathbb{A}_F)$ . Then for each infinite place

$v$ , the local Langlands parameter at  $v$  is given by  $\phi_{(w;1,0)}$  and  $\pi_{h,\infty}$  is a limit of holomorphic discrete series. Conversely, if a cuspidal automorphic representation  $\pi$  of  $\mathrm{GSp}_4(\mathbb{A}_F)$  is neither CAP nor endoscopic and its local Langlands parameter at  $v|\infty$  is given by  $\phi_{(w;1,0)}$  for some integer  $w$ , one can associate such a form  $h$  by using [17]. Note that the results in [17] are conditional on the trace formula (see the second paragraph on p. 472 of [17]). However, in the course of the proof of Theorem 1.1, we apply the unconditional result in [30] to construct a corresponding automorphic cuspidal representation. Hence Theorem 1.1 is true unconditionally.

**3.2. Hilbert modular forms and the Jacquet–Langlands correspondence.** We refer to [40, Section 1] and [23, Section 3] for the theory of ( $p$ -adic) algebraic modular forms corresponding to (parititious) Hilbert modular forms via the Jacquet–Langlands correspondence.

In this section,  $p$  is any rational prime but we remind the reader that we will later consider  $p = 2$ . Let  $M$  be a totally real field of even degree  $m$ . For each finite place  $v$  of  $M$ , let  $M_v$  be the completion of  $M$  at  $v$ ,  $\mathcal{O}_v$  its ring of integers,  $\varpi_v$  a uniformizer of  $M_v$ , and  $\mathbb{F}_v$  the residue field of  $M_v$ . Let  $D$  be the quaternion algebra with center  $M$  which is ramified exactly at all the infinite places of  $M$  and  $\mathcal{O}_D$  be the ring of integral quaternions of  $D$ . For each finite place  $v$  of  $M$ , we fix an isomorphism

$$\iota_v : D_v := D \otimes_M M_v \simeq \mathrm{M}_2(M_v).$$

We view  $D^\times$  as an algebraic group over  $M$  so that for any  $M$ -algebra  $A$ ,  $D^\times(A)$  outputs  $(D \otimes_M A)^\times$  and similarly as an algebraic group scheme over  $\mathcal{O}_M$  such that  $D^\times(R) = (\mathcal{O}_D \otimes_{\mathcal{O}_M} R)^\times$  for any  $\mathcal{O}_M$ -algebra  $R$ .

Let  $K$  be a finite extension of  $\mathbb{Q}_p$  contained in  $\overline{\mathbb{Q}_p}$  with residue field  $k$  and ring of integers  $\mathcal{O}_K$ , and assume that  $K$  contains the images of all embeddings  $M \hookrightarrow \overline{\mathbb{Q}_p}$ .

For each finite place  $v$  of  $M$  lying over  $p$ , let  $\tau_v$  be a smooth representation of  $\mathrm{GL}_2(\mathcal{O}_v)$  acting on a finite free  $\mathcal{O}_K$ -module  $W_{\tau_v}$ . We also view it as a representation of  $D_v^\times$  via  $\iota_v$ . Put  $\tau := \otimes_{v|p} \tau_v$  which is a representation of  $\mathrm{GL}_2(\mathcal{O}_p) := \prod_{v|p} \mathrm{GL}_2(\mathcal{O}_v)$  acting on  $W_\tau := \otimes_{v|p} W_{\tau_v}$ . Suppose  $\psi : M^\times \backslash (\mathbb{A}_M^\infty)^\times \rightarrow \mathcal{O}_K^\times$  is a continuous character so that for each  $v|p$ ,  $Z_{D^\times}(\mathcal{O}_v) \simeq \mathcal{O}_v^\times$  acts on  $W_{\tau_v}$  by  $\psi^{-1}|_{\mathcal{O}_{M_v}^\times}$  where  $Z_{D^\times} \simeq \mathrm{GL}_1$  is the center of  $D^\times$  as a group scheme over  $\mathcal{O}_M$ . Note that we put the discrete topology on  $\mathcal{O}_K^\times$  and therefore, such a character is necessarily of finite order. Let  $U = \prod_v U_v$  be a compact open subgroup of  $D^\times(\mathbb{A}_M^\infty) \simeq \mathrm{GL}_2(\mathbb{A}_M^\infty)$  such that  $U_v \subset D^\times(\mathcal{O}_{M_v})$  for all finite places  $v$  of  $M$ . Put  $U_p := \prod_{v|p} U_v$  and  $U^{(p)} = \prod_{v \nmid p} U_v$ . For any local  $\mathcal{O}_K$ -algebra  $A$  put  $W_{\tau,A} := W_\tau \otimes_{\mathcal{O}_K} A$ . Let  $\Sigma$  be a finite set of finite places of  $M$ . For each  $v \in \Sigma$ , let  $\chi_v : U_v \rightarrow A^\times$

be a quasi-character. Define  $\chi_\Sigma: U \rightarrow A^\times$  whose local component is  $\chi_v$  if  $v \in \Sigma$ , the trivial representation otherwise.

**Definition 3.5** (*p*-adic algebraic quaternionic forms). Let  $S_{\tau,\psi}(U, A)$  denote the space of functions

$$f: D^\times \backslash D^\times(\mathbb{A}_M^\infty) \longrightarrow W_{\tau,A}$$

such that

- $f(gu) = \tau(u_p)^{-1}f(g)$  for  $u = (u^{(p)}, u_p) \in U = U^{(p)} \times U_p$  and any  $g \in D^\times(\mathbb{A}_M^\infty)$ ;
- $f(zg) = \psi(z)f(g)$  for  $z \in Z_{D^\times}(\mathbb{A}_M^\infty)$  and  $g \in D^\times(\mathbb{A}_M^\infty)$ .

Similarly, let  $S_{\tau,\psi,\chi_\Sigma}(U, A)$  denote the space of functions

$$f: D^\times \backslash D^\times(\mathbb{A}_M^\infty) \longrightarrow W_{\tau,A}$$

such that

- $f(gu) = \chi_\Sigma^{-1}(u)\tau(u_p)^{-1}f(g)$  for  $u = (u^{(p)}, u_p) \in U = U^{(p)} \times U_p$  and  $g \in D^\times(\mathbb{A}_M^\infty)$ ;
- $f(zg) = \psi(z)f(g)$  for  $z \in Z_{D^\times}(\mathbb{A}_M^\infty)$  and  $g \in D^\times(\mathbb{A}_M^\infty)$ .

We call a function belonging to these spaces a *p*-adic algebraic quaternionic form.

Let  $S$  be a finite set of finite places of  $M$  containing all places  $v \nmid p$  such that  $U_v \neq D^\times(\mathcal{O}_v)$ . We define the (formal) Hecke algebra

$$(3.2) \quad \mathbb{T}_A^S := A[T_v, S_v]_{v \notin S \cup \{v|p\}}$$

where

$$\begin{aligned} T_v &= [D^\times(\mathcal{O}_v)\iota_v^{-1}(\text{diag}(\pi_v, 1))D^\times(\mathcal{O}_v)], \\ S_v &= [D^\times(\mathcal{O}_v)\iota_v^{-1}(\text{diag}(\pi_v, \pi_v))D^\times(\mathcal{O}_v)] \end{aligned}$$

are the usual Hecke operators. It is easy to see that both of  $S_{\tau,\psi}(U, A)$  and  $S_{\tau,\psi,\chi_\Sigma}(U, A)$  have a natural action of  $\mathbb{T}_A^S$  (cf. [13, Definition 2.2]).

Let  $U = U^{(p)} \times U_p$  be as above. As explained in [40, Section 1], if we write  $\text{GL}_2(\mathbb{A}_M^\infty) = \coprod_i D^\times t_i U Z_{D^\times}(\mathbb{A}_M^\infty)$ , then

$$S_{\tau,\psi}(U, A) \simeq \bigoplus_i W_\tau^{(UZ_{D^\times}(\mathbb{A}_M^\infty) \cap t_i^{-1} D^\times t_i) / M^\times}.$$

The group  $(UZ_{D^\times}(\mathbb{A}_M^\infty) \cap t_i^{-1} D^\times t_i) / M^\times$  is trivial for all  $t$  when  $U$  is sufficiently small (see [23, p. 623]). Henceforth, we keep this condition until the end of the section. It follows from this that the functor  $W_\tau \mapsto S_{\tau,\psi}(U, A)$  is exact (cf. [24, Lemma 3.1.4]).

Fix an isomorphism  $\iota: \mathbb{Q}_p \simeq \mathbb{C}$ . Let

$$S_{\tau,\psi}(U_p, A) := \varinjlim_{U^{(p)}} S_{\tau,\psi}(U^{(p)} \times U_p, A)$$

where  $U^{(p)}$  tends to be small.

We consider  $(\underline{k}, \underline{w}) = ((k_\sigma)_\sigma, (w_\sigma)_\sigma) \in \mathbb{Z}_{>1}^{\text{Hom}(M, \overline{\mathbb{Q}}_p)} \times \mathbb{Z}^{\text{Hom}(M, \overline{\mathbb{Q}}_p)}$  with the property that  $k_\sigma + 2w_\sigma$  is independent of  $\sigma$ . Set  $\delta := k_\sigma + 2w_\sigma - 1$  for some (any)  $\sigma$ . A special case we will encounter later is  $(\underline{k}, \underline{w}) = (k \cdot \mathbf{1}, w \cdot \mathbf{1})$  with  $k \in \mathbb{Z}_{>1}$ ,  $w \in \mathbb{Z}$ , and  $\mathbf{1} = (1, \dots, 1) \in \mathbb{Z}^{\text{Hom}(M, \overline{\mathbb{Q}}_p)}$ , where  $\delta = k + 2w - 1$ . Let  $\psi_{\mathbb{C}}: M^\times \backslash \mathbb{A}_M^\times \rightarrow \mathbb{C}^\times$  be the character defined by

$$(3.3) \quad \psi_{\mathbb{C}}(z) = \iota \left( N(z_p)^{\delta-1} \psi(z^\infty) \right) N(z_\infty)^{1-\delta}$$

for  $z = (z^{(p)}, z_p, z_\infty) \in \mathbb{A}_M^\times$  where the symbol  $N$  stands for the norm. For each  $\sigma \in \text{Hom}(M, \overline{\mathbb{Q}}_p)$ , there exists a unique pair of  $v|p$  and an embedding  $\sigma_v: M_v \rightarrow \overline{\mathbb{Q}}_p$  such that  $\sigma_v|_M = \sigma$ . Therefore, we can rewrite  $(\sigma)_{\sigma \in \text{Hom}(M, \overline{\mathbb{Q}}_p)} = (\sigma_v)_{v|p, \sigma_v \in \text{Hom}(M_v, \overline{\mathbb{Q}}_p)}$ .

Since  $w_\sigma \in \mathbb{Z}$  for each  $\sigma$ , we can define the algebraic representation  $\tau_{(\underline{k}, \underline{w}), A}$  of  $\text{GL}_2(\mathcal{O}_p) = \prod_{v|p} \text{GL}_2(\mathcal{O}_v)$  by

$$(3.4) \quad \tau_{(\underline{k}, \underline{w}), A} = \bigotimes_{v|p} \bigotimes_{\sigma_v \in \text{Hom}(M, \overline{\mathbb{Q}}_p)} \text{Sym}^{k_{\sigma_v}-2} \text{St}_2(A) \otimes \det^{w_{\sigma_v}} A$$

where  $\text{St}_2$  is the standard representation of dimension two. We often drop the subscript  $A$  from  $\tau_{(\underline{k}, \underline{w}), A}$  which should not cause any confusion. Notice that  $\tau_{(\underline{k}, \underline{w}), \mathcal{O}_K} \otimes_{\mathcal{O}_K, \iota} \mathbb{C}$  is the algebraic representation of  $\text{GL}_2(\mathbb{C})$  of highest weight  $(\underline{k}, \underline{w})$  so that the center acts by  $z \mapsto z^{\delta-1}$ ,  $\delta = k_\sigma + 2w_\sigma - 1$  for  $z \in \mathbb{C}^\times$ . We write

$$(3.5) \quad S_{\underline{k}, \underline{w}, \psi}(U_p, A) := S_{\tau_{(\underline{k}, \underline{w}), \psi}}(U_p, A)$$

for simplicity.

By [40, Corollary 1.2, Lemma 1.3-2], we have an isomorphism

$$(3.6) \quad \left( S_{\underline{k}, \underline{w}, \psi}(U_p, \mathcal{O}_K) / S_{\underline{k}, \underline{w}, \psi}^{\text{triv}}(U_p, \mathcal{O}_K) \right) \otimes_{\mathcal{O}_K, \iota} \mathbb{C} \simeq \bigoplus_{\pi} \pi^{\infty, p} \otimes \pi_p^{U_p}$$

of  $D^\times(\mathbb{A}^{p, \infty})$ -modules, where  $\pi$  runs over the regular algebraic cuspidal automorphic representations of  $\text{GL}_2(\mathbb{A}_M)$  such that  $\pi$  has central character  $\psi_{\mathbb{C}}$  and  $S_{\underline{k}, \underline{w}, \psi}^{\text{triv}}(U_p, \mathcal{O}_K)$  is defined to be zero unless  $(\underline{k}, \underline{w}) = (2 \cdot \mathbf{1}, w \cdot \mathbf{1})$ , in which case we define it to be the subspace of  $S_{\tau_{(\underline{k}, \underline{w}), \psi}}(U_p, \mathcal{O}_K)$  consisting of functions that factor through the reduced norm of  $D^\times(\mathbb{A}_F)$ .

For  $\tau_{(\underline{k}, \underline{w}), \mathbb{C}}$  as above we can also consider the space of Hilbert cusp forms on  $\text{GL}_2(\mathbb{A}_M)$  of level  $U$  and of weight  $(\underline{k}, \underline{w})$  and their geometric counterparts (see [14, Section 1.5]). Thanks to many contributors (see [20] and the references there), to each (adelic) Hilbert Hecke eigen cusp form  $f$  of weight  $(\underline{k}, \underline{w})$  and level  $U$ , one can attach an irreducible  $p$ -adic Galois representation  $\rho_{f, \iota_p}: G_M \rightarrow \text{GL}_2(\overline{\mathbb{Q}}_p)$  for any rational prime  $p$  and fixed isomorphism  $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$ . The construction also works for  $\underline{k} \geq \mathbf{1}$  (in

the lexicographic order). In particular, in the case when  $\underline{k} = \mathbb{1}$  (parallel weight one), its image is finite and it gives rise to an Artin representation  $\rho_f: G_M \rightarrow \mathrm{GL}_2(\mathbb{C})$  (see [31]). Taking a suitable integral lattice, we consider the reduction  $\bar{\rho}_{f,p}: G_M \rightarrow \mathrm{GL}_2(\bar{\mathbb{F}}_p)$  of  $\rho_{f,p}$  or  $\rho_f$  modulo the maximal ideal of  $\bar{\mathbb{Z}}_p$ .

Let  $F$  be a totally real subfield of  $M$  such that  $[M:F] = 2$ . This is possible since  $M/\mathbb{Q}$  is a Galois extension of even degree. Let  $s$  be the generator of  $\mathrm{Gal}(M/F)$ . Put  $S_M := \mathrm{Hom}_{\mathbb{Q}}(M, \bar{\mathbb{Q}})$  and let  $S_M^{(1)}$  be a subset such that  $S_M = S_M^{(1)} \amalg S_M^{(2)}$  where  $S_M^{(2)} := S_M^{(1)} \circ s$ . Further, we identify  $S_M^{(1)}$  with  $S_F = \mathrm{Hom}_{\mathbb{Q}}(F, \bar{\mathbb{Q}})$  via  $\sigma \mapsto \sigma|_F$ .

Let  ${}^s f$  be the twist of  $f$  by  $s$  which is defined by the composition of  $f$  and the automorphism of  $D^\times \backslash D^\times (\mathbb{A}_M^\infty)$  induced from  $s$ . We denote by  $\omega_{sf}$  the central character, which satisfies  $\omega_{sf} = {}^s \omega_f$ . Let  $\pi_f$  (resp.  $\pi_{sf}$ ) be the corresponding cuspidal representation attached to  $f$  (resp.  ${}^s f$ ).

Changing the subset  $S_M^{(1)}$  if necessary, we may write  $\underline{k} = (k_\tau)_{\tau \in S_M}$  as  $\underline{k} = (k_{1,\sigma}, k_{2,\sigma})_{\sigma \in S(1)_M}$  with  $k_{1,\sigma} \geq k_{2,\sigma}$  for each  $\sigma \in S_M^{(1)}$ , where  $k_\tau = k_{1,\tau}$  if  $\tau \in S_M^1$  and  $k_\tau = k_{2,\sigma}$  if  $\tau = \sigma \circ s \in S_M^{(2)}$ .

Applying [4, 30, 37], we have the following unconditional theorem:

**Theorem 3.6.** *Keep the notation as above. Suppose  $\underline{k} = (k_1 \cdot \mathbb{1}, k_2 \cdot \mathbb{1})$  is in  $\mathbb{Z}^{S_M^{(1)}} \times \mathbb{Z}^{S_M^{(2)}}$  for some integers  $k_1 \geq k_2 \geq 2$  with  $k_1 \equiv k_2 \pmod{2}$ . For each  $\sigma \in S_M^{(1)}$ , put  $w_\sigma = 0$  and  $w_{\sigma \circ s} = \frac{k_1 - k_2}{2}$ . Further, suppose  $\pi_{sf}$  is not isomorphic to  $\pi_f$  (equivalently,  $f$  does not come from any Hilbert cusp form on  $\mathrm{GL}_2(\mathbb{A}_F)$  via base change) and suppose the central character  $\omega_f$  satisfies  $\omega_{sf} = \omega_f$ . Then, there exists a Hilbert–Siegel Hecke eigen cusp form  $h$  on  $\mathrm{GSp}_4(\mathbb{A}_F)$  such that the corresponding cuspidal automorphic representation  $\Pi = \Pi_h$  satisfies the following:*

- (1) *for each infinite place  $v \in S_F$  and  $\sigma \in S_M^{(1)}$  such that  $\sigma|_F = v$ , the  $L$ -parameter of  $\Pi_v$  is given by  $\phi_{(-k_{1,\sigma}; m_{1,\sigma}, m_{2,\sigma})} \otimes |\cdot|$  with*

$$m_{1,\sigma} = \frac{k_{1,\sigma} + k_{2,\sigma} - 2}{2}, \quad m_{2,\sigma} = \frac{k_{1,\sigma} - k_{2,\sigma}}{2};$$

- (2) *for each  $p$  and  $\iota_p$ , there exists an irreducible  $p$ -adic Galois representation  $\rho_{h,\iota_p}: G_F \rightarrow \mathrm{GSp}_4(\bar{\mathbb{Q}}_p)$  enjoying the following properties:*
  - (a)  $\rho_{h,\iota_p} = \mathrm{Ind}_{G_M}^{G_F} \rho_{f,\iota_p}$ ;
  - (b)  $\rho_{h,\iota_p}$  satisfies (1), (2), (3) of Theorem 3.1;
  - (c) *for each finite place  $v$  of  $F$  dividing  $p$ ,  $\rho_{h,\iota_p}|_{G_{F_v}}$  is de Rham and it satisfies the local-global compatibility up to Frobenius semi-simplification. Further, it has the Hodge–Tate weights as in (4) of Theorem 3.1.*

*Proof.* The condition on the central character is equivalent to  $\omega_f$  factoring through the norm map  $N_{M/F}$  via a (Hecke) character of  $\mathbb{A}_F^\times$  (cf. [18, Lemma 5.2]). Applying [30, p. 251, Theorem 8.6(1)], the theta lifting from  $f \otimes |\det|_{\mathbb{A}_M}^{-1}$  gives an automorphic representation  $\Pi'$  of  $\mathrm{GSp}_4(\mathbb{A}_F)$  such that for each  $v \in S_M$ ,  $\Pi'_v$  is a (limit) of holomorphic discrete series and  $\Pi = \Pi' \otimes |\det|$  is the desired one (the assumption on  $\pi_f$  guarantees  $\Pi'$  (or  $\Pi$ ) is, in fact, cuspidal). For each  $\sigma \in S_M^{(1)}$ , by the parameter in [4, p. 71, Definition], the local Langlands parameters of  $\pi_{f,\sigma} \otimes |\det|^{-1}$ ,  $\pi_{f,\sigma \circ s} \otimes |\det|^{-1}$  are given, respectively, by

$$|z|^{-k_1} \mathrm{diag} \left( (z/\bar{z})^{\frac{k_{1,\sigma}-1}{2}}, (z/\bar{z})^{-\frac{k_{1,\sigma}-1}{2}} \right),$$

$$|z|^{-k_1} \mathrm{diag} \left( (z/\bar{z})^{\frac{k_{2,\sigma}-1}{2}}, (z/\bar{z})^{-\frac{k_{2,\sigma}-1}{2}} \right),$$

where  $z \in \mathbb{C} \subset W_{M_\sigma}$ . By (3.1), we see the local  $L$ -parameter of  $\Pi'_\sigma$  (resp.  $\Pi_\sigma$ ) is given by  $\phi_{(-k_{1,\sigma}; m_{1,\sigma}, m_{2,\sigma})}$  (resp.  $\phi_{(-k_{1,\sigma}; m_{1,\sigma}, m_{2,\sigma})} \otimes |\det|$ ). Therefore, we have the first claim.

For the rest, we have only to check the claim (2)(a),(c) since the other one follows from Theorem 3.1. The claim (2)(a) follows from the matching of the Satake parameters at unramified places and Chebotarev density. By [37, Theorem 1 with the footnote 7 in p. 252],  $\rho_{f,\iota_p}|_{G_{F_v}}$  is de Rham and so is  $\rho_{h,\iota_p}|_{G_{F_v}}$ . Hence we have the claim (2)(c).  $\square$

**Remark 3.7.** The claim (c) of Theorem 3.6 above is much stronger than (5) of Theorem 3.1 when  $k_1 = k_2$  because as explained in the proof, the local-global compatibility holds for any Hilbert modular forms and any finite places by [37, Theorem 1].

The following proposition is a minor modification of [10, Corollary 2.12]. The proof itself is well-known to experts but we give the details for completeness; we also look carefully at what happens to the central characters in the process of the congruence method.

**Proposition 3.8.** *Let  $p = 2$ . Let  $M$  be a totally real field of even degree  $m$  over  $\mathbb{Q}$ . Let  $f$  be a Hilbert Hecke eigen cusp form on  $\mathrm{GL}_2(\mathbb{A}_M)$  of parallel weight one such that  $\bar{\rho}_{f,\iota_2}$  is irreducible. There exists a Hilbert Hecke eigen cusp form  $g$  on  $\mathrm{GL}_2(\mathbb{A}_M)$  such that*

- (1)  $\bar{\rho}_{f,\iota_2} \simeq \bar{\rho}_{g,\iota_2} \otimes \psi$  for some continuous character  $\psi: G_M \rightarrow \bar{\mathbb{F}}_2^\times$ ;
- (2) the character corresponding to the central character of  $g$  under (3.3) is trivial;
- (3)  $g$  is of weight  $(\underline{2}, \underline{0})$  with  $\underline{2} := 2 \cdot \mathbf{1}$  (parallel weight 2). Here we write  $\underline{0} = (0, \dots, 0) \in \mathbb{Z}^m$ .

Further, if  $\det(\bar{\rho}_{f,\iota_2})$  is trivial, then  $\psi$  can be taken to be trivial.

*Proof.* Let  $U$  be a sufficiently small open compact subgroup of  $\mathrm{GL}_2(\mathbb{A}_M)$  that fixes  $f$ . Since  $f$  is of parallel weight one, we have  $(\underline{k}, \underline{w}) = (\underline{1}, w \cdot \underline{1})$  for some  $w \in \mathbb{Z}$ . By twisting if necessary, we may assume  $w = 0$ . Let  $K$  be a finite extension of  $\mathbb{Q}_2$  in  $\overline{\mathbb{Q}}_2$  with ring of integers  $\mathcal{O}_K$  such that  $K$  contains all Hecke eigenvalues of  $f$  for  $T_{\mathcal{O}_K}^S$ . Let  $\mathbb{F}$  be the residue field of  $K$ . As in [14, Section 1.5], we can view  $f$  as a geometric Hilbert modular form over  $\mathcal{O}_K$  via a classical Hilbert modular form associated to  $f$  and consider its base change  $\bar{f}$  to  $\mathbb{F}$ . After multiplying by a high enough power of the Hasse invariant, we have another form  $\bar{g}_1$  of weight  $(\underline{k}, \underline{0})$  with  $\underline{k} = k \cdot \underline{1}$ ,  $k \gg 0$  such that

- (1)  $\bar{h} = \bar{g}_1$ ;
- (2)  $\bar{g}_1$  is liftable to a geometric Hilbert Hecke eigenform  $g_1$  over  $\mathcal{O}_K$  by enlarging  $K$  if necessary;
- (3)  $\bar{\rho}_{g_1, \iota_2} \simeq \bar{\rho}_{f, \iota_2}$ .

We view  $g_1$  as a classical Hilbert Hecke eigen cusp form and by the Jacquet–Langlands correspondence, we have a 2-adic algebraic quaternionic form  $h_1$  in  $S_{\tau_{(\underline{k}, \underline{0})}, \psi}(U, \mathcal{O}_K)$  corresponding to  $g_1$ ; here  $\psi: M^\times \backslash \mathbb{A}_M^\times \rightarrow \mathcal{O}_K^\times$  is the finite character corresponding to the central character of  $g_1$  under (3.3). For each finite place  $v$  of  $M$  lying over 2, let  $U_{1,v}$  be the subgroup of  $U_v$  consisting of all elements congruent to  $\begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$ . Put  $U_{1,2} := \prod_{v|2} U_{1,v}$ . By definition,  $\bar{h}_1 \in S_{\tau_{(\underline{k}, \underline{0})}, \psi}(U^{(2)} \times U_{1,2}, \mathbb{F})$ . Since  $U_{1,2}$  acts on  $\tau_{(\underline{k}, \underline{0}), \mathbb{F}}$  unipotently, it can be written as a successive extension of the trivial representation of  $U_{1,2}$ . This successive extension commutes with the Hecke action and one can find a Hecke eigenform  $\bar{h}_2 \in S_{\tau_{(\underline{2}, \underline{0})}, \psi}(U^{(2)} \times U_{1,2}, \mathbb{F})$ . Further, notice that  $(\mathbb{F}^\times)^2 = \mathbb{F}^\times$  and by twisting, we may assume that the reduction  $\bar{\psi}$  of  $\psi$  is trivial. Since  $U$  is taken to be sufficiently small, there exists a lift  $h_2 \in S_{\tau_{(\underline{2}, \underline{0})}, \psi^{\mathrm{triv}}}(U^{(2)} \times U_{1,2}, \mathcal{O}_K)$  of  $\bar{h}_2$  where  $\psi^{\mathrm{triv}}$  stands for the trivial character. In fact, the Hecke eigen system of  $\bar{h}_2$  is liftable to  $\mathcal{O}_K$  by the Deligne–Serre Lemma [12, Lemma 6.11] and by multiplicity one, we can recover a Hecke eigenform  $h_2$  from the Hecke eigensystem. Further  $h_2$  is non-trivial since  $\bar{\tau}$  is absolutely irreducible. Therefore, by [40, Lemma 1.3-2] the form  $g$  is taken to be the image of  $h_2$  under the Jacquet–Langlands correspondence.

The remaining claim on the central character is obvious by construction. □

**3.3. Mod 2 automorphy.** In this section we prove Theorem 1.1.

*Proof.* By assumption and Lemma 2.1,  $\mathrm{Im}(\bar{\rho}_{C,2})$  is of type  $S_5(a)$ . Applying Proposition 2.3 there exist a totally real quadratic extension  $L/F$  and an absolutely irreducible totally odd two-dimensional Galois representation  $\bar{\tau}: G_L \rightarrow \mathrm{GL}_2(\mathbb{F}_4)$  such that  $\bar{\rho} \simeq \mathrm{Ind}_{G_L}^{G_F} \bar{\tau}$ . Notice that  $\bar{\tau}$  is not equivalent to  ${}^t \bar{\tau}$  for any lift  $\iota$  of the generator of  $\mathrm{Gal}(L/F)$  and  $\mathrm{Im}(\bar{\tau}) = \mathrm{SL}_2(\mathbb{F}_4)$ .



Since  $SL_2(\mathbb{F}_4) \simeq A_5$  we have an embedding  $SL_2(\mathbb{F}_4) \hookrightarrow PGL_2(\mathbb{C})$ . Let  $W = W(\mathbb{F}_4)$  be the ring of Witt vectors of  $\mathbb{F}_4$  and take a sufficiently large finite extension  $K/\mathbb{Q}_2$  containing  $W$ . Then by using an explicit realization of the complex representation of  $A_5$ , we have an embedding  $SL_2(\mathbb{F}_4) \hookrightarrow PGL_2(\mathcal{O}_K)$ . Applying Tate’s theorem [35, Section 6], we have a representation  $\tau': G_L \rightarrow GL_2(\mathcal{O}_K)$  whose reduction modulo the maximal ideal  $m_K$  of  $\mathcal{O}_K$  is a twist of  $\bar{\tau} \otimes_{\mathbb{F}_4} \mathcal{O}_K/m_K$  by a finite character of  $G_L$ . It follows from this that  $\tau'$  is totally odd and the projective image is isomorphic to  $A_5$ . By [34, Theorem 2] or [28, Theorem 0.3],  $\bar{\tau}'$  is modular, hence there exists a Hilbert cusp form  $f_1$  of parallel weight 1 such that  $\bar{\rho}_{f_1, \iota_2} \simeq \bar{\tau}$ . Since  $\bar{\tau}$  has trivial determinant,  $\det(\bar{\rho}_{f_1, \iota_2})$  is trivial. Further, applying Proposition 3.8, there exists a Hilbert cusp form  $f$  of  $GL_2(\mathbb{A}_L)$  of  $(2, \underline{0})$  with trivial central character such that  $\bar{\rho}_{f, 2} \simeq \bar{\tau}$ . Let  $\pi$  be the cuspidal automorphic representation of  $GL_2(\mathbb{A}_L)$  corresponding to  $f$ . For each infinite place  $v$  of  $L$ , the local Langlands parameter of  $\pi_{f, v}$  is given by

$$\phi_{\pi_{f, v}}(z) = \text{diag}\left(\left(\frac{z}{\bar{z}}\right)^{\frac{1}{2}}, \left(\frac{z}{\bar{z}}\right)^{-\frac{1}{2}}\right).$$

Applying Theorem 3.6, we have a cuspidal automorphic representation  $\Pi$  of  $GSp_4(\mathbb{A}_F)$  corresponding to  $\text{Ind}_{G_L}^{G_F} \rho_{f, \iota_2}$ . It follows that the local Langlands parameter of  $\Pi_v$  is  $\phi_{(1;1,0)} \otimes |\cdot|^{-1}$ . Therefore,  $\Pi_v$  is a limit of holomorphic discrete series and there exists a Hilbert–Siegel cusp Hecke eigenform  $h$  of parallel weight 2 generating  $\Pi$  as desired. □

**Remark 3.9.** In the course of the proof, we apply Sasaki’s (or Pilloni–Stroh’s) modularity lifting theorem which requires raising the level. Therefore, we cannot specify the levels of the Hilbert modular forms appearing there. This implies that we are also unable to specify the levels of our Hilbert–Siegel modular forms. However, there is some hope and a substantial expectation for further development of the level-lowering method. Indeed, [10, Conjectures 4.7 and 4.9] indicate that we should be able to take the Hilbert cusp forms in question to have the correct level corresponding to the Artin conductor of  $\bar{\rho}$ .

### 4. Examples

We are looking for monic irreducible polynomials  $f \in \mathbb{Q}[x]$  of degree 6 such that

- (1) there is an isomorphism  $\sigma$  from the Galois group of  $f$  to the symmetric group  $S_5$ ;
- (2) for any complex conjugation  $c$  in the Galois group of  $f$ , the element  $\sigma(c) \in S_5$  has type  $(2, 2)$ .

We shall give two families of such polynomials. A general approach to produce them is to compute the sextic resolvent polynomial  $f$  of an irreducible quintic polynomial over  $F$  with Galois group  $S_5$ . This can be done using symbolic computation, in a straightforward but very tedious way; also, writing down an explicit form would take considerable space. To get around this, we apply classical results of Hermite and Klein.

**4.1. Using generic polynomials.** Let  $F = \mathbb{Q}$ . Hermite proved that the polynomial  $P \in \mathbb{Q}(s, t)[x]$  given by

$$P(x) = x^5 + sx^3 + tx + t$$

is generic for  $S_5$ , which means that every  $S_5$ -extension  $K/\mathbb{Q}$  is the splitting field of some specialization of  $P$ , and that the splitting field of  $P$  has Galois group  $S_5$  over  $\mathbb{Q}(s, t)$ . A proof appears in [21, Proposition 2.3.8]. The discussion in Section 2.4 of the same book contains the following observation: If  $h \in \mathbb{Q}[x]$  is a quintic polynomial with Galois group  $S_5$ , then the Weber sextic resolvent of  $h$  is an irreducible sextic with the same splitting field, corresponding to the transitive embedding of  $S_5$  into  $S_6$ . We can apply this to a specialization  $h$  of  $P$  with  $s, t \in \mathbb{Q}$ , and get the Weber sextic resolvent

$$f(x) = (x^3 + b_4x^2 + b_2x + b_0)^2 - 2^{10} \text{disc}(h)x,$$

where  $\text{disc}(h)$  is the discriminant of  $h$  and the coefficients are given by

$$\begin{aligned} b_0 &= -176s^2t^2 + 28s^4t + 4000st^2 - s^6 + 320t^3 \\ b_2 &= 3s^4 - 8s^2t + 240t^2 \\ b_4 &= -3s^2 - 20t. \end{aligned}$$

Taking different rational values of  $s$  and  $t$ , we can obtain lots of examples of  $f$  with property (1) above.

Property (2) is easy to verify once  $s$  and  $t$  are given, as it is equivalent to  $h$  having a unique real root. We determine the relation between the values of  $s$  and  $t$  and the number of real roots of  $h$  using Sturm's Theorem [2, Theorem 2.62], which requires computing the Sturm sequence

$$\begin{aligned} h_0(x) &= h(x) = x^5 + sx^3 + tx + t \\ h_1(x) &= h'(x) = 5x^4 + 3sx^2 + t \\ h_2(x) &= -(h_0(x) \bmod h_1(x)) = -\frac{2}{5}sx^3 - \frac{4}{5}tx - t \\ h_3(x) &= -(h_1(x) \bmod h_2(x)) = \frac{g_3}{s}x^2 + \frac{25t}{2s}x - t \end{aligned}$$

$$h_4(x) = -(h_2(x) \bmod h_3(x)) = \frac{tg_4}{2g_3^2}x + \frac{t(5t - s^2)(20t - 9s^2)}{g_3^2}$$

$$h_5(x) = -(h_3(x) \bmod h_4(x)) = \frac{g_3^2g_5}{g_4^2},$$

where  $a(x) \bmod b(x)$  denotes the remainder of the polynomial division of  $a(x)$  by  $b(x)$ , and for future use we define

$$g_3(s, t) = 10t - 3s^2$$

$$g_4(s, t) = 12s^4 - 88s^2t + 125st + 160t^2$$

$$g_5(s, t) = 108s^5 + 16s^4t - 900s^3t - 128s^2t^2 + 2000st^2 + 256t^3 + 3125t^2.$$

Given a polynomial  $p$  of degree  $n$  in  $x$  with leading coefficient  $a_n$ , we define the sign of  $p$  at  $+\infty$  to be the sign of  $a_n$ , and the sign of  $p$  at  $-\infty$  to be  $(-1)^n$  times the sign of  $a_n$ . For the Sturm sequence  $h_0, h_1, \dots, h_5$ , we write  $V(-\infty)$  for the number of sign changes in the sequence of signs at  $-\infty$ , and  $V(+\infty)$  for the number of sign changes in the sequence of signs at  $+\infty$ . Sturm's Theorem then says that the number  $r$  of real roots of  $h$  is given by

$$r = V(-\infty) - V(+\infty).$$

We gather some observations that will simplify our analysis:

- (1) If  $t < 0$  then  $g_3(s, t) < 0$ : clear as it is a sum of negative terms.
- (2) If  $s < 0$  and  $t < 0$  then  $g_4(s, t) > 0$ : clear as it is a sum of positive terms.
- (3) If  $s > 0$  and  $t > 0$  then  $g_5(s, t) > 0$ . This follows from completing a couple of squares to rewrite:

$$g_5(s, t) = 3s(6s^2 - 25t)^2 + 16t(s^2 - 4t)^2 + 125st^2 + 3125t^2.$$

- (4) If  $s > 0$ ,  $t > 0$ , and  $g_3(s, t) > 0$  then  $g_4(s, t) > 0$ . To see this, note that

$$g_4(s, t) = \frac{4}{3}g_3^2(s, t) + \frac{8}{3}tg_3(s, t) + 125st.$$

- (5) If  $s > 0$ ,  $t < 0$ , and  $g_4(s, t) < 0$ , then  $g_5(s, t) > 0$ . This follows from

$$g_5(s, t) = \frac{8}{5}g_4(s, t)t + 108s^5 - t \left( \frac{16}{5}s^4 + 900s^3 \right) + t^2 \left( \frac{64}{5}s^2 + 1800s + 3125 \right).$$

- (6) If  $s < 0$ ,  $t > 0$ ,  $g_3(s, t) > 0$  and  $g_4(s, t) > 0$ , then  $g_5(s, t) > 0$ . This follows implicitly from Sturm's Theorem: if  $g_5(s, t) < 0$  then the sign sequence at  $-\infty$  is  $- + - - -$  and the sign sequence at  $+\infty$  is  $+ + + - + -$ , hence the quantity  $V(-\infty) - V(+\infty) = -1$ .

Table 4.1 gives the number  $r$  of real zeros of  $h(x)$  in relation to the signs of the various relevant quantities. We have used the observations made above to reduce the number of possibilities from  $2^5 = 32$  to 15:

TABLE 4.1. Details of the inputs to Sturm’s Theorem, depending on the possible signs of  $s, t, g_i(s, t)$ . The output of Sturm’s Theorem, the number  $r$  of real roots of the polynomial  $h$ , appears in the rightmost column.

$s$	$t$	$g_3$	$g_4$	$g_5$	signs at $-\infty$	$V(-\infty)$	signs at $+\infty$	$V(+\infty)$	$r$
+	+	+	+	+	- + + + - +	3	+ + - + + +	2	1
+	+	-	+	+	- + + - - +	3	+ + - - + +	2	1
+	+	-	-	+	- + + - + +	3	+ + - - - +	2	1
-	+	+	+	+	- + - - - +	3	+ + + - + +	2	1
-	+	+	-	+	- + - - + +	3	+ + + - - +	2	1
-	+	+	-	-	- + - - + -	4	+ + + - - -	1	3
-	+	-	+	+	- + - + - +	5	+ + + + + +	0	5
-	+	-	+	-	- + - + - -	4	+ + + + + -	1	3
-	+	-	-	+	- + - + + +	3	+ + + + - +	2	1
-	+	-	-	-	- + - + + -	4	+ + + + - -	1	3
-	-	-	+	+	- + - + + +	3	+ + + + - +	2	1
-	-	-	+	-	- + - + + -	4	+ + + + - -	1	3
+	-	-	+	+	- + + - + +	3	+ + - - - +	2	1
+	-	-	+	-	- + + - + -	4	+ + - - - -	1	3
+	-	-	-	+	- + + - - +	3	+ + - - + +	2	1

We can summarize the findings in Table 4.1 as follows:

**Proposition 4.1.** *The polynomial  $h(x) = x^5 + sx^3 + tx + t$  has exactly 3 real roots if and only if  $g_5(s, t) < 0$ . If  $g_5(s, t) > 0$ , then  $h$  has exactly 5 real roots if and only if  $s < 0, t > 0, g_3(s, t) < 0$ , and  $g_4(s, t) > 0$ .*

The complement of the conditions listed in the Proposition gives the region in the  $(s, t)$ -plane of interest to us, namely that where  $h$  has exactly one real root. We note that this occurs everywhere in the first quadrant, and almost nowhere in the third quadrant. The behaviour in the second quadrant is by far the most interesting, as can be seen in Figure 4.1.

**4.2. Using 5-torsion on elliptic curves.** Next we consider the quintic polynomials arising from 5-division points of elliptic curves. This has the advantage that an explicit form of the resolvent is well-known: it goes back to work of Klein. Almost everything that follows is described in [19].

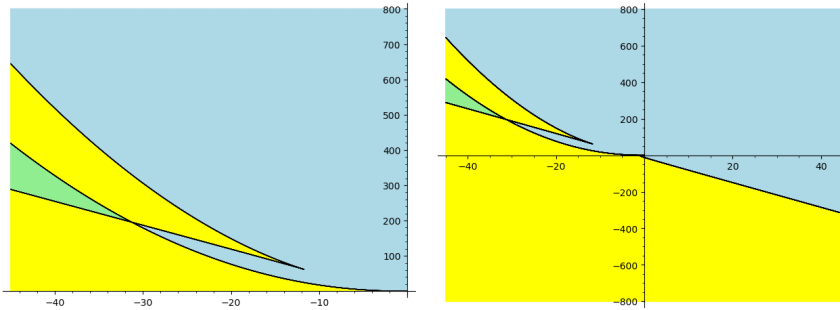


FIGURE 4.1. Second quadrant (left) and entire  $(s, t)$ -plane (right): blue (resp. yellow, green) points represent polynomials  $h$  having precisely 1 real root (resp. 3, 5 real roots). The boundaries of these regions are given by the black curve  $g_5(s, t) = 0$ .

Let  $F$  be a totally real field not containing  $\sqrt{5}$ . Let

$$E: \quad y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

be an elliptic curve over  $F$  with the property that the mod 5 representation  $\bar{\rho}_{E,5}: G_F \rightarrow \text{GL}_2(\mathbb{F}_5)$  is full,<sup>1</sup> hence surjective. The projective image of  $\bar{\rho}_{E,5}$  is  $\text{PGL}_2(\mathbb{F}_5)$ , which is isomorphic to  $S_5$ . In fact, the faithful action of  $\text{PGL}_2(\mathbb{F}_5)$  on the projective line  $\mathbb{P}^1(\mathbb{F}_5)$  by fractional linear transformations yields  $\text{PGL}_2(\mathbb{F}_5) \hookrightarrow \text{Aut}(\mathbb{P}^1(\mathbb{F}_5)) \simeq S_6$ . Since  $|\text{PGL}_2(\mathbb{F}_5)| = 120$ , by the classification of the subgroups of  $S_6$  (cf. GAP),  $\text{PGL}_2(\mathbb{F}_5)$  is isomorphic to  $S_5$ . Further, there are no fixed points in this action, hence the image of  $\text{PGL}_2(\mathbb{F}_5)$  is a transitive subgroup of  $S_6$ . Under this identification, for each complex conjugation  $c$ ,  $\bar{\rho}_{E,p}(c) \sim \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$  corresponds to an element of  $S_6$  of type  $(2, 2)$ .

The corresponding  $S_5$ -extension of  $F$  is described by a quintic polynomial

$$\theta_{E,5}(x) = x^5 - 40\Delta x^2 - 5c_4\Delta x - c_4^2\Delta,$$

(see [19, Equation (1.24)]) where the invariants  $\Delta, c_4$  are defined in [36, Section III.1, p. 42]. The resolvent of  $\theta_{E,5}$  is computed as in [19, Equation (2.37)] in conjunction with [25, Proposition 3.2.1] and it is explicitly given by

$$f_{E,6}(x) := x^6 + b_2x^5 + 10b_4x^4 + 40b_6x^3 + 80b_8x^2 + 16(b_2b_8 - b_4b_6)x + (-b_2b_4b_6 + b_2^2b_8 - 5b_6^2),$$

where  $b_2, b_4, b_6, b_8$  are also defined in [36, Section III.1, p. 42]. The Galois group of the splitting field  $F_{f_{E,6}}$  of  $f_{E,6}(x)$  over  $F$  in  $\bar{\mathbb{Q}}$  is a priori embedded

<sup>1</sup>We say that  $\bar{\rho}_{E,p}$  is full if  $\text{End}_{\bar{F}}(E) = \mathbb{Z}$  and the image of  $\bar{\rho}_{E,p}$  contains  $\text{SL}_2(\mathbb{F}_p)$ .

in  $S_6$  by permuting the roots but it is isomorphic to  $S_5$  since  $F_{f_{E,6}} = F_{\theta_{E,5}}$  by construction. Let us consider the hyperelliptic curve  $C = C_E$  defined by  $y^2 = f_{E,6}(x)$ . The above argument gives a natural embedding of  $\text{Im}(\bar{\rho}_{C,2})$  into  $S_6$ . It is well-known that  $\bar{\rho}_{E,5}$  is totally odd and it shows that  $\bar{\rho}_{C,2}(c)$  is of type  $(2, 2)$  for each complex conjugation of  $G_F$ . Further, if  $f_{E,6}(x)$  is irreducible, then  $\text{Im}(\bar{\rho}_{C,2})$  is transitive in  $S_6$  and hence is of type  $S_5(a)$ . Summing up, we have

**Theorem 4.2.** *Assume that  $\bar{\rho}_{E,5}$  is full and  $f_{E,6}$  is irreducible. Then  $\bar{\rho}_{C_E,2}$  is automorphic in the sense of Theorem 1.1.*

We illustrate the method with some explicit examples.

- Let us consider the elliptic curve  $E: y^2 + y = x^3 + x^2$  over  $\mathbb{Q}$ , of conductor 43. By [26, Elliptic curve with label 43.a1], the representation  $\bar{\rho}_{E,5}: G_{\mathbb{Q}} \rightarrow \text{GL}_2(\mathbb{F}_5)$  is full. On the other hand, we have  $\theta_{E,5} = x^5 + 1720x^2 + 3440x + 11008$  and it is easy to check (e.g. using SageMath [32] or Magma [6]) that

$$(4.1) \quad f_{E,6}(x) = x^6 + 4x^5 + 40x^3 + 80x^2 + 64x + 11$$

is irreducible over  $\mathbb{Q}$  with Galois group isomorphic to  $S_5$ . By Theorem 4.2,  $\bar{\rho}_{C_E,2}$  is automorphic.

- For an example where the ground field is not  $\mathbb{Q}$ , consider

$$E: y^2 = x^3 - x^2 + x \quad \text{over } F = \mathbb{Q}(\sqrt{2}),$$

see [26, Elliptic curve 72.1-a3 over number field  $\mathbb{Q}(\sqrt{2})$ ]. Once more,  $\bar{\rho}_{E,5}$  is full and the resolvent

$$f_{E,6}(x) = x^6 + 4x^5 + 20x^4 - 80x^2 - 64x - 16$$

is irreducible over  $F$ , so we conclude that  $\bar{\rho}_{C_E,2}$  is automorphic.

**4.3. Databases of genus 2 curves.** The methods used in Sections 4.1 and 4.2 produce infinite families of examples satisfying the conditions of Theorem 1.1, but they tend to give hyperelliptic curves with large conductors. For instance, the conductor of the curve (4.1) is<sup>2</sup>

$$4\,786\,321\,400\,000 = 2^6 \cdot 5^5 \cdot 7 \cdot 43^4$$

and the curve corresponding to the choice of parameters  $s = 0, t = -1$  in Section 4.1 has equation

$$y^2 = x^6 + 40x^5 + 880x^4 + 8960x^3 + 44800x^2 - 3091456x + 102400$$

and conductor

$$82\,311\,610\,000 = 2^4 \cdot 5^4 \cdot 19^2 \cdot 151^2$$

---

<sup>2</sup>We used the Magma package Genus2Conductor [15] by Tim Dokchitser and Christopher Doris for the computation of the conductors listed in this section.

There are however databases of genus 2 curves with conductor that is either small or has restricted prime factors. Currently the most comprehensive are based on [5], which produced:

- 66 158 curves with conductor less than 1 000 000, to be found at [26, Genus 2 curves over  $\mathbb{Q}$ ]; from this list, we verified that the curves labelled
 

50000.b.800000.1	378125.a.378125.1	681472.a.681472.1
64800.c.648000.1	382347.a.382347.1	703125.b.703125.1
180625.a.903125.1	506763.a.506763.1	

satisfy the conditions of Theorem 1.1;

- 487 493 curves with 5-smooth discriminant, to be found at [39]; we verified that 4 885 of these curves satisfy the conditions of Theorem 1.1.

Both databases provide the curves as global minimal models described by equations of the form  $y^2 + h(x)y = f(x)$ .

**Acknowledgments.** The authors thank the anonymous referee for their insightful comments.

## References

- [1] T. BARNET-LAMB, D. GERAGHTY, M. HARRIS & R. TAYLOR, “A family of Calabi-Yau varieties and potential automorphy II”, *Publ. Res. Inst. Math. Sci.* **47** (2011), no. 1, p. 29-98.
- [2] S. BASU, R. POLLACK & M.-F. ROY, *Algorithms in real algebraic geometry*, second ed., Algorithms and Computation in Mathematics, vol. 10, Springer, 2006, x+662 pages.
- [3] J. BELLAÏCHE & G. CHENEVIER, “The sign of Galois representations attached to automorphic forms for unitary groups”, *Compos. Math.* **147** (2011), no. 5, p. 1337-1352.
- [4] D. BLASIUS & J. D. ROGAWSKI, “Motives for Hilbert modular forms”, *Invent. Math.* **114** (1993), no. 1, p. 55-87.
- [5] A. R. BOOKER, J. SLSLING, A. V. SUTHERLAND, J. VOIGHT & D. YASAKI, “A database of genus-2 curves over the rational numbers”, *LMS J. Comput. Math.* **19** (2016), p. 235-254.
- [6] W. BOSMA, J. CANNON & C. PLAYOUST, “The Magma algebra system. I. The user language”, *J. Symb. Comput.* **24** (1997), no. 3-4, p. 235-265, Computational algebra and number theory (London, 1993).
- [7] G. BOXER, F. CALEGARI, T. GEE & V. PILLONI, “Abelian surfaces over totally real fields are potentially modular”, *Publ. Math., Inst. Hautes Étud. Sci.* **134** (2021), p. 153-501.
- [8] A. BRUMER & K. KRAMER, “Paramodular abelian varieties of odd conductor”, *Trans. Am. Math. Soc.* **366** (2014), no. 5, p. 2463-2516.
- [9] A. BRUMER, A. PACETTI, C. POOR, G. TORNARÍA, J. VOIGHT & D. S. YUEN, “On the paramodularity of typical abelian surfaces”, *Algebra Number Theory* **13** (2019), no. 5, p. 1145-1195.
- [10] K. BUZZARD, F. DIAMOND & F. JARVIS, “On Serre’s conjecture for mod  $\ell$  Galois representations over totally real fields”, *Duke Math. J.* **155** (2010), no. 1, p. 105-161.
- [11] F. CALEGARI, “The Artin conjecture for some  $S_5$ -extensions”, *Math. Ann.* **356** (2013), no. 1, p. 191-207.
- [12] P. DELIGNE & J.-P. SERRE, “Formes modulaires de poids 1”, *Ann. Sci. Éc. Norm. Supér.* **7** (1974), p. 507-530.
- [13] L. DEMBÉLÉ, “Explicit computations of Hilbert modular forms on  $\mathbb{Q}(\sqrt{5})$ ”, *Exp. Math.* **14** (2005), no. 4, p. 457-466.

- [14] M. DIMITROV, “Galois representations modulo  $p$  and cohomology of Hilbert modular varieties”, *Ann. Sci. Éc. Norm. Supér.* **38** (2005), no. 4, p. 505-551.
- [15] T. DOKCHITSER & C. DORIS, “3-torsion and conductor of genus 2 curves”, *Math. Comput.* **88** (2019), no. 318, p. 1913-1927.
- [16] W. T. GAN & S. TAKEDA, “The local Langlands conjecture for  $\mathrm{GSp}(4)$ ”, *Ann. Math.* **173** (2011), no. 3, p. 1841-1882.
- [17] T. GEE & O. TAÏBI, “Arthur’s multiplicity formula for  $\mathbf{GSp}_4$  and restriction to  $\mathbf{Sp}_4$ ”, *J. Éc. Polytech., Math.* **6** (2019), p. 469-535.
- [18] J. R. GETZ, “An approach to nonsolvable base change and descent”, *J. Ramanujan Math. Soc.* **27** (2012), no. 2, p. 143-211.
- [19] E. H. GOINS, *Elliptic curves and icosahedral Galois representations*, ProQuest LLC, 1999, Thesis (Ph.D.)—Stanford University, 110 pages.
- [20] F. JARVIS, “On Galois representations associated to Hilbert modular forms”, *J. Reine Angew. Math.* **491** (1997), p. 199-216.
- [21] C. U. JENSEN, A. LEDET & N. YUI, *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, vol. 45, Cambridge University Press, 2002, ix+258 pages.
- [22] J. JOHNSON-LEUNG & B. ROBERTS, “Siegel modular forms of degree two attached to Hilbert modular forms”, *J. Number Theory* **132** (2012), no. 4, p. 543-564.
- [23] M. KISIN, “Modularity of 2-adic Barsotti-Tate representations”, *Invent. Math.* **178** (2009), no. 3, p. 587-634.
- [24] ———, “Moduli of finite flat group schemes, and modularity”, *Ann. Math.* **170** (2009), no. 3, p. 1085-1180.
- [25] A. KLUTE, “Icosahedral Galois extensions and elliptic curves”, *Manuscr. Math.* **93** (1997), no. 3, p. 301-324.
- [26] THE LMFDB COLLABORATION, “The L-functions and modular forms database”, <https://www.lmfdb.org>, 2023, accessed 1 October 2020.
- [27] C. P. MOK, “Galois representations attached to automorphic forms on  $\mathrm{GL}_2$  over CM fields”, *Compos. Math.* **150** (2014), no. 4, p. 523-567.
- [28] V. PILLONI & B. STROH, “Surconvergence, ramification et modularité”, in *Arithmétique  $p$ -adique des formes de Hilbert*, Astérisque, vol. 382, Société Mathématique de France, 2016, p. 195-266.
- [29] D. RAMAKRISHNAN, “Modularity of solvable Artin representations of  $\mathrm{GO}(4)$ -type”, *Int. Math. Res. Not.* **2002** (2002), no. 1, p. 1-54.
- [30] B. ROBERTS, “Global  $L$ -packets for  $\mathrm{GSp}(2)$  and theta lifts”, *Doc. Math.* **6** (2001), p. 247-314.
- [31] J. D. ROGAWSKI & J. B. TUNNELL, “On Artin  $L$ -functions associated to Hilbert modular forms of weight one”, *Invent. Math.* **74** (1983), no. 1, p. 1-42.
- [32] THE SAGE DEVELOPERS, *SageMath, the Sage Mathematics Software System (Version 10.0)*, 2023, <https://www.sagemath.org>.
- [33] F. SAIRALJI, “On congruences between the coefficients of two  $L$ -series which are related to a hyperelliptic curve over  $\mathbf{Q}$ ”, *Osaka J. Math.* **37** (2000), no. 4, p. 789-799.
- [34] S. SASAKI, “Integral models of Hilbert modular varieties in the ramified case, deformations of modular Galois representations, and weight one forms”, *Invent. Math.* **215** (2019), no. 1, p. 171-264.
- [35] J.-P. SERRE, “Modular forms of weight one and Galois representations”, in *Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975)*, Academic Press Inc., 1977, p. 193-268.
- [36] J. H. SILVERMAN, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, 2009, xx+513 pages.
- [37] C. SKINNER, “A note on the  $p$ -adic Galois representations attached to Hilbert modular forms”, *Doc. Math.* **14** (2009), p. 241-258.
- [38] C. M. SORENSEN, “Galois representations attached to Hilbert-Siegel modular forms”, *Doc. Math.* **15** (2010), p. 623-670.
- [39] A. V. SUTHERLAND, “Genus 2 curves over  $\mathbf{Q}$ ”, 2016, <https://math.mit.edu/~drew/genus2curves.html>, accessed 1 October 2020.



- [40] R. TAYLOR, “On the meromorphic continuation of degree two  $L$ -functions”, *Doc. Math.* **2006** (2006), p. 729-779.
- [41] N. TSUZUKI & T. YAMAUCHI, “Automorphy of mod 2 Galois representations associated to the quintic Dwork family and reciprocity of some quintic trinomials”, 2022, <https://arxiv.org/abs/2008.09852>.
- [42] J. B. TUNNELL, “Artin’s conjecture for representations of octahedral type”, *Bull. Am. Math. Soc.* **5** (1981), no. 2, p. 173-175.
- [43] A. WAGNER, “The faithful linear representation of least degree of  $S_n$  and  $A_n$  over a field of characteristic 2.”, *Math. Z.* **151** (1976), no. 2, p. 127-137.
- [44] A. WEISS, “On the images of Galois representations attached to low weight Siegel modular forms”, *J. Lond. Math. Soc.* **106** (2022), no. 1, p. 358-387.
- [45] P.-J. WONG, “Applications of group theory to conjectures of Artin and Langlands”, *Int. J. Number Theory* **14** (2018), no. 3, p. 881-898.

Alexandru GHITZA  
School of Mathematics and Statistics  
University of Melbourne  
Parkville, VIC 3010, Australia  
*E-mail:* [aghitza@alum.mit.edu](mailto:aghitza@alum.mit.edu)  
*URL:* <https://aghitza.org>

Takuya YAMAUCHI  
Mathematical Inst. Tohoku Univ.  
6-3, Aoba, Aramaki, Aoba-Ku  
Sendai 980-8578, Japan  
*E-mail:* [takuya.yamauchi.c3@tohoku.ac.jp](mailto:takuya.yamauchi.c3@tohoku.ac.jp)  
*URL:* <https://sites.google.com/site/takuyayamauchigsp4>