JOURNAL
de Théorie des Nombres
de BORDEAUX

anciennement Séminaire de Théorie des Nombres de Bordeaux

Nobuo TSUZUKI et Takuya YAMAUCHI

Automorphy of mod 2 Galois representations associated to the quintic Dwork family and reciprocity of some quintic trinomials

Tome 38, nº 1 (2026), p. 253-293.

https://doi.org/10.5802/jtnb.1361

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

Journal de Théorie des Nombres
de Bordeaux **38** (2026), 253–293

Automorphy of mod 2 Galois representations associated to the quintic Dwork family and reciprocity of some quintic trinomials

par Nobuo TSUZUKI et Takuya YAMAUCHI

Résumé. Dans cet article, nous déterminons les représentations galoisiennes modulaires $\bar{\rho}_{\psi,2} : G_K := \mathrm{Gal}(\overline{K}/K) \to \mathrm{GSp}_4(\mathbb{F}_2)$ associées aux motifs miroir de rang 4 et de poids pur 3 provenant de la famille quintique de Dwork

$$X_0^5 + X_1^5 + X_2^5 + X_3^5 + X_4^5 - 5\psi X_0 X_1 X_2 X_3 X_4 = 0,\ \psi \in K$$

définie sur un corps de nombres K, sous la condition d'irréductibilité du trinôme quintique f_ψ ci-dessous.

En appliquant ce résultat à un corps totalement réel $K = F$, nous prouvons que pour une extension totalement réelle M/F de degré au plus 2, $\bar{\rho}_{\psi,2}|_{G_M}$ est associée à une forme de Hilbert–Siegel parabolique sur $\mathrm{GSp}_4(\mathbb{A}_M)$ de poids parallèle 3, propre pour les opérateurs de Hecke.

Chemin faisant, nous observons que l'image d'une telle représentation de caractéristique 2 est gouvernée par les lois de réciprocité associées au trinôme quintique

$$f_\psi(x) = 4x^5 - 5\psi x^4 + 1,\ \psi \in K$$

dont le corps de décomposition est génériquement de groupe de Galois S_5. Cela nous permet d'utiliser les résultats de modularité des représentations d'Artin de dimension 2 totalement impaires de $\mathrm{Gal}(\overline{F}/F)$ dus à Shu Sasaki ou Pilloni–Shu ainsi que des divers relèvements fonctoriels de Langlands pour les formes modulaires de Hilbert. Il en résulte l'existence d'une forme de Hilbert–Siegel parabolique, de poids parallèle 3, correspondant au type de Hodge du système compatible en question. Une version tordue est également discutée ; elle est liée aux trinômes quintiques généraux.

Abstract. In this paper, we determine mod 2 Galois representations $\bar{\rho}_{\psi,2} : G_K := \mathrm{Gal}(\overline{K}/K) \to \mathrm{GSp}_4(\mathbb{F}_2)$ associated to the mirror motives of rank 4 with pure weight 3 coming from the Dwork quintic family

$$X_0^5 + X_1^5 + X_2^5 + X_3^5 + X_4^5 - 5\psi X_0 X_1 X_2 X_3 X_4 = 0,\ \psi \in K$$

defined over a number field K under the irreducibility condition of the quintic trinomial f_ψ below. Applying this result, when $K = F$ is a totally real field, for

---

Manuscrit reçu le 15 décembre 2024, révisé le 4 mai 2025, accepté le 19 septembre 2025.
2020 *Mathematics Subject Classification.* 11F, 11F33, 11F80.
Mots-clefs. the quintic Dwork family, mod 2 Galois representations.
N.T. is partially supported by JSPS KAKENHI Grant Number (A) No. 18H03667.

some at most quadratic totally real extension M/F, we prove that $\bar{\rho}_{\psi,2}|_{G_M}$ is associated to a Hilbert–Siegel modular Hecke eigen cusp form for $\mathrm{GSp}_4(\mathbb{A}_M)$ of parallel weight three.

In the course of the proof, we observe that the image of such a mod 2 representation is governed by reciprocity of the quintic trinomial

$$f_\psi(x) = 4x^5 - 5\psi x^4 + 1,\ \psi \in K$$

whose decomposition field is generically of type 5-th symmetric group S_5. This enable us to use results on the modularity of 2-dimensional, totally odd Artin representations of $\mathrm{Gal}(\overline{F}/F)$ due to Shu Sasaki or Pilloni–Shu and several Langlands functorial lifts for Hilbert cusp forms. Then, it guarantees the existence of a desired Hilbert–Siegel modular cusp form of parallel weight three matching with the Hodge type of the compatible system in question. A twisted version is also discussed and it is related to general quintic trinomials.

1. Introduction

Let K be a number field in an algebraic closure $\overline{\mathbb{Q}}$ of $\mathbb{Q}$ and p be a prime number. Fix an isomorphism $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$ and embeddings $\overline{\mathbb{Q}} \to \mathbb{C}$ and $\iota = \iota_p : \overline{\mathbb{Q}} \to \overline{\mathbb{Q}}_p$ compatible with it.

We let $G_K := \mathrm{Gal}(\overline{\mathbb{Q}}/K)$ and $\bar{\rho} : G_K \to \mathrm{GL}_n(\overline{\mathbb{F}}_p)$ be an irreducible continuous representation. We say $\bar{\rho}$ is a mod p Galois representation. Number theorists expect that $\bar{\rho}$ is automorphic. That is, there should exist an algebraic automorphic representation π of $\mathrm{GL}_n(\mathbb{A}_K)$ such that its conjectural p-adic Galois representation $\rho_{\pi,\iota} : G_K \to \mathrm{GL}_n(\overline{\mathbb{Q}}_p)$ satisfies $\bar{\rho} \simeq \bar{\rho}_{\pi,\iota}$ (see [11] for algebraic automorphic representations).

The automorphy of $\bar{\rho}$ is understood as the Serre conjecture for (G_K, GL_n) and it has been broadly studied over the past few decades (see [23] and the references therein) in more general setting. To prove automorphy of a given geometric p-adic Galois representation with current techniques, it is first necessary to show that its mod p reduction is automorphic. In general, no concrete way has been known to find such a π for $\bar{\rho}$ except for some cases. Known cases of residual automorphy require p and the image of $\bar{\rho}$ to be small, and are dealt with using automorphy of Artin representations. Therefore, it would be important to find geometric objects whose residual Galois representations have small images in which case we can apply the known cases of automorphic Artin representations.

In this paper, we study mod 2 Galois representations given by the mirror family associated to the Dwork quintic family and its automorphy in connection with cuspidal automorphic representations of GSp_4.

Let us fix the notation to explain our results. For each $\psi \in K$ with $\psi^5 \neq 1$, let us consider the Calabi-Yau threefold defined by

$$X_\psi : X_0^5 + X_1^5 + X_2^5 + X_3^5 + X_4^5 - 5\psi X_0X_1X_2X_3X_4 = 0 \tag{1.1}$$

as a smooth projective hypersurface in $\mathbb{P}^4$ with the coordinates $[X_0 : X_1 : X_2 : X_3 : X_4]$. It is called the Dwork quintic family when we view it as a family with one parameter ψ. Let Y_ψ be the singular mirror symmetry of X_ψ, which is defined by the closure of the smooth affine variety

$$U_\psi : x_1 + x_2 + x_3 + x_4 + \frac{1}{x_1x_2x_3x_4} - 5\psi = 0, \tag{1.2}$$

in the projective toric variety $\mathbb{P}_\Delta$, this will be introduced in Section 5.1. Let us take a smooth mirror symmetry W_ψ of X_ψ introduced in [13] such that W_ψ is a crepant resolution of Y_ψ (see [4]). Then W_ψ has good reduction at each finite place v of K such that $v \nmid 5$ and $\psi^5 - 1$ is a v-adic unit (see Section 5.1). Such a mirror symmetry is not unique, but it is unique as a pure motif. The Hodge-diamond of W_ψ is given by

$$\begin{array}{lccccccc}
H^0 & & & & 1 & & & \\
H^1 & & & 0 & & 0 & & \\
H^2 & & 0 & & 101 & & 0 & \\
H^3 & 1 & & 1 & & 1 & & 1 \\
H^4 & & 0 & & 101 & & 0 & \\
H^5 & & & 0 & & 0 & & \\
H^6 & & & & 1 & & &
\end{array}$$

where H^* stands for the (complex) de Rham cohomology. Put

$$V_{\psi,2} := H^3_{\text{ét}}(W_{\psi,\overline{\mathbb{Q}}}, \mathbb{Q}_2)$$

where $H^*_{\text{ét}}$ stands for etale cohomology, and let $\langle\,\cdot\,,\cdot\,\rangle : V_{\psi,2} \times V_{\psi,2} \to \mathbb{Q}_2(-3)$ be the G_K-equivariant, perfect, alternating pairing defined by the Poincaré duality. It yields a 2-adic Galois representation

$$\rho_{\psi,2} = \rho_{\psi,\iota_2} : G_K \longrightarrow \mathrm{GSp}(V_{\psi,2}, \langle\,\cdot\,,\cdot\,\rangle) \simeq \mathrm{GSp}_4(\mathbb{Q}_2)$$

where the algebraic group $\mathrm{GSp}_4 = \mathrm{GSp}_J$ is the symplectic similitude group in GL_4 associated to $J = \begin{pmatrix} 0_2 & s \\ -s & 0_2 \end{pmatrix}$, $s = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Let us choose a G_K-stable lattice $T_{\psi,2}$ over $\mathbb{Z}_2$ of $V_{\psi,2}$ so that the above alternating pairing preserves the integral structure with respect to $T_{\psi,2}$. Put $\overline{T}_{\psi,2} = T_{\psi,2} \otimes_{\mathbb{Z}_2} \mathbb{F}_2$. Thus, it yields a mod 2 Galois representation

$$\bar{\rho}_{\psi,2} : G_K \longrightarrow \mathrm{GSp}(\overline{T}_{\psi,2}, \langle\,\cdot\,,\cdot\,\rangle_{\mathbb{F}_2}) \simeq \mathrm{GSp}_4(\mathbb{F}_2) \tag{1.3}$$

depending on the choice of $T_{\psi,2}$. We view it as a representation to $\mathrm{GL}_4(\mathbb{F}_2)$ via the natural inclusion $\mathrm{GSp}_4(\mathbb{F}_2) \subset \mathrm{GL}_4(\mathbb{F}_2)$. Therefore, one can consider the semisimplification $\bar{\rho}^{\mathrm{ss}}_{\psi,2}$ of $\bar{\rho}_{\psi,2}$. A priori, its image lands in $\mathrm{GL}_4(\mathbb{F}_2)$. We choose a symplectic basis so that it takes the values in $\mathrm{GSp}_4(\mathbb{F}_2)$. Hence we have a semisimple mod 2 Galois representation

$$\bar{\rho}^{\mathrm{ss}}_{\psi,2} : G_K \longrightarrow \mathrm{GSp}_4(\mathbb{F}_2)$$

associated to W_ψ. As is explained in Remark 5.2, $H^3_{\text{ét}}(W_{\psi,\overline{\mathbb{Q}}},\mathbb{Z}_2)$ is torsion free and one can choose it as $T_{\psi,2}$. As explained in Section 3, we fix an isomorphism $\mathrm{GSp}_4(\mathbb{F}_2)\simeq S_6$.

Let us introduce the following quintic trinomial

$$f_\psi(x) := 4x^5 - 5\psi x^4 + 1 \in K[x] \tag{1.4}$$

and denote by K_{f_ψ} its decomposition field over K in $\overline{\mathbb{Q}}$. Notice that the discriminant of f_ψ is given by $2^8 5^5(1-\psi^5)$. First we prove the following result:

Theorem 1.1 (Theorem 6.8, Proposition 3.4, and Theorem 7.1)**.** *Assume that f_ψ is irreducible over K. Then it holds that*

(1) $\mathrm{Im}(\bar{\rho}_{\psi,2})\simeq \mathrm{Gal}(K_{f_\psi}/K)$ *and* $\mathrm{Im}(\bar{\rho}_{\psi,2})$ *contains no element of type* $(3,3)$ *under the fixed isomorphism* $\mathrm{GSp}_4(\mathbb{F}_2)\simeq S_6$*. In particular, the image is regarded as a subgroup of the 5-th symmetric group* S_5 *whose order is divisible by five;*

(2) $\bar{\rho}_{\psi,2}$ *is irreducible over* $\mathbb{F}_2$ *and hence* $\bar{\rho}_{\psi,2}\simeq\bar{\rho}^{\mathrm{ss}}_{\psi,2}$*. Further, it is absolutely irreducible if and only if the image is isomorphic to* $F_{20}=C_4\ltimes C_5$*,* A_5 *or* S_5*, and otherwise the image is isomorphic to* C_5 *or* $D_{10}=C_2\ltimes C_5$ *(see Section 3.2 for the subgroups);*

(3) *Suppose* $K=\mathbb{Q}$*. If* $\psi=0$*, then* $\mathrm{Im}(\bar{\rho}_{0,2})\simeq F_{20}$*. For all other* $\psi\neq 0$*,* $\mathrm{Im}(\bar{\rho}_{\psi,2})\simeq S_5$*.*

This theorem explains reciprocity of the quintic trinomial f_ψ is governed by the reduction of the Frobenius polynomial $P_{\psi,v}$ defined below, as a polynomial in $\mathbb{F}_2[t]$. For each good finite place v of K with the residue field $\mathbb{F}_v$ of q_v elements, put

$$P_{\psi,v}(t) := \det(1_4 - t\rho_{\psi,2}(\mathrm{Frob}_v)) = 1 - a_{\psi,v}t + b_{\psi,v}t^2 - q_v^3 a_{\psi,v}t^3 + q_v^6 t^4 \in \mathbb{Z}_2[t]$$

which is a Weil polynomial over $\mathbb{Z}$. If $n(f_\psi,q_v)$ denotes the cardinal of solutions of the equation $f_\psi(x)=0$ in $\mathbb{F}_v$, then the reciprocity in f_ψ is the congruence

$$a_{\psi,v} \equiv n(f_\psi,q_v)+1 \pmod 2 \tag{1.5}$$

for all good finite places v not lying over 2 (see Proposition 5.1). There are only four cases for $P_{\psi,v}(t) \pmod 2$ and explicitly they are given as follows:

$$1+t^4,\ 1+t+t^3+t^4,\ 1+t+t^2+t^3+t^4,\ 1+t^2+t^4.$$

Under the fixed isomorphism $\mathrm{GSp}_4(\mathbb{F}_2)\simeq S_6$, the reciprocity in (1.5) and Chebotarev's density theorem reveal that K_{f_ψ} and $L_\psi := \overline{\mathbb{Q}}^{\mathrm{Ker}(\bar{\rho}_{\psi,2})}$ are equal. It follows that $\bar{\rho}_{\psi,2}$ takes values in a subgroup isomorphic into S_5. A key to analyze the image is to observe the absence of $(123)(456)\in S_6$ in the image of $\bar{\rho}_{\psi,2}$, whose characteristic polynomial corresponds to $1+t^2+t^4 \equiv (1+t+t^2)^2 \pmod 2$. One novel aspect of our result comprises the computation of residual images of Galois representations coming from higher dimensional varieties (see [20] for some previous work).

Applying the above theorem, one can describe $\bar{\rho}_{\psi,2}$ in terms of 2-dimensional mod 2 Galois representations. Artin representations with S_5-image have been studied in [12] and this result is suggestive to study our representations in a similar way, although more careful analysis is needed. In fact, $\mathrm{GSp}_4(\mathbb{F}_2)=\mathrm{Sp}_4(\mathbb{F}_2)\simeq \mathrm{SO}(4)(\mathbb{F}_2)$ implies there are two instances of mod 2 automorphy, coming orthogonal automorphic representations and symplectic automorphic representations. Notice that before taking the reduction modulo 2, the 2-adic Galois representation $\rho_{\psi,2}$ is symplectic. Therefore, we need to find symplectic automorphic representations for $\bar{\rho}_{\psi,2}$. However, when $\mathrm{Im}(\bar{\rho}_{\psi,2})\simeq S_5$ (generic case), $\bar{\rho}_{\psi,2}$ is realized as a twisted tensor product and it is naturally connected to orthogonal automorphic representations. Thus, it seems to be hard to find any symplectic automorphic lift from this. To overcome this issue we restrict $\bar{\rho}_{\psi,2}$ to G_M where M/K is the quadratic extension corresponding to the kernel of $G_K \to \mathrm{Im}(\bar{\rho}_{\psi,2})\simeq S_5 \xrightarrow{\mathrm{sgn}} \{\pm 1\}$. Then it turns out that $\bar{\rho}_{\psi,2}|_{G_M}$ has the symmetric cubic structure which can be easily lifted to a symplectic representation.

We can combine the above main theorem with many ingredients obtained in [37] or [43], the results of algebraic quaternionic forms, and known Langlands functorial lifts to prove the automorphy of our mod 2 Galois representations when $K=F$ is a totally real field. Let $\mathcal{H}_2$ be the Siegel-upper half space of degree 2.

Theorem 1.2 (Theorem 4.7 and Theorem 4.8). *Suppose that $K=F$ is a totally real field and f_ψ is irreducible over F. Assume that $\mathrm{Gal}(F_{f_\psi}/F)\simeq F_{20}$, A_5 or S_5 and each complex conjugation in $\mathrm{Gal}(F_{f_\psi}/F)$ corresponds to an element of type $(2,2)$ under this isomorphism, equivalently, $\sigma(\psi)<1$ for any embedding $\sigma: F\hookrightarrow \mathbb{R}$. Further assume $[F:\mathbb{Q}]$ is even if $\mathrm{Gal}(F_{f_\psi}/F)\simeq A_5$. Let M/F be the totally real quadratic extension associated to the kernel of $G_F\to \mathrm{Im}(\bar{\rho}_{\psi,2})\to S_5 \xrightarrow{\mathrm{sgn}} \{\pm 1\}$ if $\mathrm{Gal}(F_{f_\psi}/F)\simeq S_5$ and $M=F$ otherwise. Put $d=[M:\mathbb{Q}]$. Then there exists a holomorphic Hilbert–Siegel Hecke eigen cusp form h on $\mathcal{H}_2^d$ of parallel weight three such that*

$$\bar{\rho}_{\psi,2}|_{G_M}\simeq \bar{\rho}_{h,2}$$

where $\bar{\rho}_{h,2}$ is the reduction of 2-adic representation $\rho_{h,2}$ associated to h (see [34] for the construction of $\rho_{h,2}$).

To consider the restriction of $\bar{\rho}_{\psi,2}$ to G_M is harmless in proving the automorphy of $\rho_{\psi,2}$ since the automorphy of $\rho_{\psi,2}|_{G_M}$ implies the one of $\rho_{\psi,2}$ by a well-known descend argument.

The assumption on $[F:\mathbb{Q}]$ when $\mathrm{Gal}(F_{f_\psi}/F)\simeq A_5$ is necessary to fully apply the Jacquet–Langlands correspondence. If we succeed to make use of a level raising argument, we would be able to remove this assumption.

As observed, $\bar{\rho}_{\psi,2}$ can be viewed as an orthogonal representation via $\mathrm{GSp}_4(\mathbb{F}_2)=\mathrm{Sp}_4(\mathbb{F}_2)=\mathrm{SO}(4)(\mathbb{F}_2)$ where the orthogonal group $\mathrm{SO}(4)$ is defined by using $\begin{pmatrix} 0_2 & s \\ s & 0_2 \end{pmatrix}$, $s=\left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Although it is no longer related to the Dwork family, it is also interesting to discuss orthogonal automorphy. This may be related to the arithmetic variety associated to GL_4 (cf. [1]).

Theorem 1.3 (Theorem 4.9). *Let* $\bar{\rho}:G_F\to\mathrm{SO}(4)(\mathbb{F}_2)$ *be an irreducible mod 2 Galois representation. Assume that* $\mathrm{Im}(\bar{\rho})\simeq S_5$ *and each complex conjugation in* G_F *corresponds to an element of type* $(2,2)$ *under this isomorphism. Then there exists a cuspidal automorphic representation* π *of* $\mathrm{GO}(2,2)(\mathbb{A}_F)$ *which can be transferred to a regular algebraic essentially self-dual cuspidal automorphic representation* Π *of* $\mathrm{GL}_4(\mathbb{A}_F)$ *of weight zero such that*

$$\bar{\rho}\simeq\bar{\rho}_{\Pi,2}$$

where $\bar{\rho}_{\Pi,2}$ *is the reduction of* 2*-adic Galois representation* $\rho_{\Pi,2}$ *associated to* Π *(see* [3, Section 1] *for the construction of* $\rho_{\Pi,2}$*).*

In the course of the proof of the above theorem, we will use some arithmetic properties of non-paritious Hilbert modular forms to construct cuspidal automorphic representations of $\mathrm{GL}_4(\mathbb{A}_F)$ of weight zero. This is a new application of interesting results in [16] and [35].

Remark 1.4. *To the best of our knowledge, the levels of the Hilbert–Siegel forms in the main theorems cannot be specified, due to a lack of level-lowering results (see Remark 4.10).*

Remark 1.5. *The compatible system associated to our Dwork family* X_ψ *over a CM field is known to be potentially automorphic (*[2, 36]*). Hence we can study possible levels of the lifts potentially at a suitable* ℓ*-adic component and then we may convert some arithmetic information in the levels to those of the* 2*-adic component and its reduction modulo 2.*

Remark 1.6. *In the proof of Theorem 1.2, to obtain holomorphic forms we will apply the results in* [24]*. Note that the results in* [24] *are conditional on the trace formula (see* [24, second paragraph in p. 472]*). However, if we do not require holomorphic forms for automorphy, the proof of 1.2 shows unconditionally that there exists a global generic regular algebraic cuspidal automorphic representation* Π *of* $\mathrm{GSp}_4(\mathbb{A}_M)$ *such that* $\bar{\rho}_{\Pi,2}\simeq\bar{\rho}_{\psi,2}|_{G_M}$*.*

This paper is organized as follows. In Section 2, we study basic facts for mod 2 Galois representations to $\mathrm{GSp}_4(\mathbb{F}_2)$. We devote Section 3 and Section 4 to study automorphic forms in question and various congruences between several automorphic forms. We devote Section 5 and Section 6 to determine the image of $\bar{\rho}_{\psi,2}$, a necessary step to apply our automorphy results. In the last section, we give some observations in the possibility of the image of $\bar{\rho}_{\psi,2}$ being related to some rational points on Diophantine equations. Here we use a technique reminiscent of Coleman–Chabauty method, although our method is more elementary and is of independent interest. Finally, we discuss a variant of our main theorems by introducing a twist of the Dwork quintic family.

Let us give a guide for readers. The determination of the mod 2 Galois representations are more friendlier than other contents to readers and they may read Section 3 and Section 6 assuming the results in Section 5. Section 4 and Section 7 are readable independently apart from the other sections. The main results in Section 1 are slightly generalized to a twisted version in Section 8.

In [48], the second author studies the residual monodromy in characteristic 2 of the higher-dimensional Dwork family, with the aim of investigating the automorphy of 2-adic symplectic Galois representations of general degree involving the rank four case with the residual image A_5, using the ideas of [45] and [30].

Acknowledgment. This work started when the second author discussed with the first author about the quintic Dwork family. We thank Tohoku university for making this opportunity and incredible hospitality. Finally, we would like to give special thanks to the referee, whose suggestions have greatly improved the presentation and readability of this paper.

2. $\mathbf{GSp_4}$

Let us fix some notation for the smooth group scheme $\mathrm{GSp}_4 = \mathrm{GSp}_J$ over $\mathbb{Z}$ which is defined as the symplectic similitude group in GL_4 associated to $J = \begin{pmatrix} 0_2 & s \\ -s & 0_2 \end{pmatrix}$, $s = \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$. Explicitly,

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

Put $\mathrm{Sp}_4 = \mathrm{Ker}(\nu : \mathrm{GSp}_4 \to \mathrm{GL}_1, X \mapsto \nu(X))$. Let B be the upper Borel subgroup in GSp_4 with the Levi decomposition $B = TN$. Let P be the Siegel parabolic subgroup containing B and denote by $P = M_P N_P$ its Levi decomposition. Let Q be the Klingen parabolic subgroup containing B with the Levi decomposition $Q = M_Q N_Q$. All non-trivial (rational) parabolic subgroups containing B are either of B, P, or Q. An explicit form in each case can be found in [40, p. 28-29]. Finally, we define the endoscopic subgroup H of GSp_4 consisting of all elements

$$\begin{pmatrix} x & 0 & 0 & y \\ 0 & a & b & 0 \\ 0 & c & d & 0 \\ z & 0 & 0 & w \end{pmatrix}$$

with $xw - yz = ad - bc$.

Lemma 2.1. *Let $\mathbb{F}_q$ be a finite field of characteristic 2. Then it holds that*

(1) $B(\mathbb{F}_q) \simeq (\mathbb{F}_q^\times)^3 \ltimes (\mathbb{F}_q \ltimes \mathbb{F}_q^3)$;
(2) $P(\mathbb{F}_q) \simeq (\mathbb{F}_q^\times \times \mathrm{GL}_2(\mathbb{F}_q)) \ltimes \mathbb{F}_q^3$;
(3) $Q(\mathbb{F}_q) \simeq (\mathbb{F}_q^\times \times \mathrm{GL}_2(\mathbb{F}_q)) \ltimes \mathbb{F}_q^3$.

Proof. Since the characteristic of $\mathbb{F}_q$ is 2, it is easy to see that $N_Q(\mathbb{F}_q)$ is abelian. The third claim easily follows from the structure of Q. For B, $N(\mathbb{F}_q)$ consists of all elements of form

$$n(x, \lambda, \mu, \kappa) := \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & x & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & \lambda & \mu & \kappa \\ 0 & 1 & 0 & \mu \\ 0 & 0 & 1 & -\lambda \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Let $N_1 = \{n(0, \lambda, \mu, \kappa) \in N(\mathbb{F}_q)\}$. It is easy to check that it is a normal abelian subgroup of $N(\mathbb{F}_q)$ and it follows from this that $N_1 \simeq \mathbb{F}_q^3$. Clearly, $N(\mathbb{F}_q)/N_1 \simeq \{n(x, 0, 0, 0,) \in N(\mathbb{F}_q)\} \simeq \mathbb{F}_q$. Hence we have the claim for B. The remaining case P is similar to the case of Q. □

Notice that the statement of Lemma 2.1 is false for B and Q when the characteristic of the base field is different from 2.

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

In this section, we study some elementary properties of mod 2 Galois representations to $\mathrm{GSp}_4(\mathbb{F}_2)$. We denote by S_n n-th symmetric group.

3.1. An identification between $\mathrm{GSp}_4(\mathbb{F}_2)$ and S_6. Let $s : \mathbb{F}_2^6 \to \mathbb{F}_2$ be the linear functional defined by $s(x_1, \ldots, x_6) = x_1 + \cdots + x_6$ and 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

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

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

$$\varphi : S_6 \longrightarrow \mathrm{GSp}(W, \langle \cdot, \cdot \rangle_W).$$

It is easy to see that the action of S_6 on W is faithful and φ turns out to be isomorphism by counting all elements of both sides. There is no canonical choice of basis of W but we have a canonical choice with respect to the endoscopic subgroup H. Let us consider the action of the symmetric group S_3 on $Y = \{(x_1, x_2, x_3) \in \mathbb{F}_2^3 \mid x_1 + x_2 + x_3 = 0\}$. Similarly, we have an isomorphism

$$\psi : S_3 \longrightarrow \mathrm{GL}(Y) = \mathrm{GL}(Y, \langle\,\cdot\,,\cdot\,\rangle_Y).$$

The isomorphism

$$\begin{aligned} \eta : \qquad\qquad\qquad & Y \oplus Y \longrightarrow W, \\ ((x_1, x_2, x_3), (y_1, y_2, y_3)) & \longmapsto (x_1, x_2, x_3, y_1, y_2, y_3) \mod U \end{aligned}$$

as a $\mathbb{F}_2$-vector space satisfies the relation

$$\langle u_1, v_1\rangle_Y + \langle u_2, v_2\rangle_Y = \langle \eta(u_1, v_1), \eta(u_2, v_2)\rangle_W$$

and further we have the following commutative diagram:

$$\begin{tikzcd} S_3 \times S_3 \arrow[r, "(\psi,\psi)"] \arrow[d, "\iota"'] & \mathrm{GL}(Y) \times \mathrm{GL}(Y) \arrow[d, "\eta"'] \\ S_6 \arrow[r, "\varphi"] & \mathrm{GSp}(W, \langle\,\cdot\,,\cdot\,\rangle_W) \end{tikzcd}$$

where the left vertical arrow ι is defined by the identification

$$S_3 \times S_3 = \mathrm{Aut}(\{1,2,3\}) \times \mathrm{Aut}(\{4,5,6\}) \subset \mathrm{Aut}(\{1,2,3,4,5,6\}) = S_6.$$

For instance, choose $f_1 = (1,1,0), f_2 = (1,0,1)$ as a basis of Y. Then we see that

$$e_1 = \eta(f_1, 0),\ e_2 = \eta(0, f_1),\ e_3 = \eta(0, f_2),\ e_4 = \eta(f_2, 0) \tag{3.1}$$

make up a basis of W. Using these basis, we have the following commutative diagram:

$$\begin{tikzcd} S_3 \times S_3 \arrow[r] \arrow[d, "\iota"'] & \mathrm{GL}_2(\mathbb{F}_2) \times \mathrm{GL}_2(\mathbb{F}_2) \arrow[d] \\ S_6 \arrow[r] & \mathrm{GSp}_4(\mathbb{F}_2) \end{tikzcd}$$

such that the image of the right vertical arrow coincides with $H(\mathbb{F}_2)$. For instance, the element $(123)(345)$ of order 3 is represented by

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

To end this subsection, we list up all representation matrices with respect to the basis (3.1) for each conjugacy class of S_5. Here S_5 is regarded as $\{\sigma \in S_6 \mid \sigma(6) = 6\}$. They are

$$\tau_1 = e, \quad \tau_2 = (12), \quad \tau_{22} = (12)(34), \quad \tau_3 = (123),$$
$$\tau_{32} = (123)(45), \quad \tau_4 = (1234), \quad \tau_5 = (12345)$$

where e stands for the identity element in S_5. In this order, we have seven matrices respectively,

$$A_{\tau_1} = I_4,$$
$$A_{\tau_2} = \begin{pmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_{\tau_{22}} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad A_{\tau_3} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix},$$
$$A_{\tau_{32}} = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad A_{\tau_4} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \quad A_{\tau_5} = \begin{pmatrix} 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \end{pmatrix}.$$

The eigenpolynomials are

$$f_{\tau_1}(t) = f_{\tau_2}(t) = f_{\tau_{22}}(t) = f_{\tau_4}(t) = (1+t)^4,$$
$$f_{\tau_3}(t) = f_{\tau_{32}}(t) = (1+t)^2(1+t+t^2),$$
$$f_{\tau_5}(t) = 1 + t + t^2 + t^3 + t^4.$$

3.2. Certain subgroups of S_6. In our setting, we are concerned with any subgroup of S_6 whose order is divisible by 5. Applying GAP [22], up to conjugacy, we find the groups

$$C_5, D_{10} := C_2 \ltimes C_5, \; F_{20} := C_4 \ltimes C_5, \; A_5, \; S_5, \; A_6, \; S_6.$$

Clearly, $C_5 \subset D_{10} \subset F_{20}$ and $D_{10} \subset A_5$ but $F_{20} \not\subset A_5$. Here C_n stands for the cyclic group of order n and A_n is the alternating group of degree n. For instance, in terms of the basis (3.1), the generators $\sigma = (23)(56)$, $\tau = (25463)$ of D_{10} in S_6 have the following matrix representations

$$J = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \end{pmatrix} \in \mathrm{GSp}_4(\mathbb{F}_2)$$

respectively.

On the other hand, F_{20} can be realized as

$$F_{20} = \langle \sigma = (12345), \; \tau = (1243) \rangle \subset S_5.$$

Notice that $\tau^2 = (14)(23)$ is of type $(2,2)$.

3.3. An identification between A_5 and $\mathrm{SL}_2(\mathbb{F}_4)$. It is well-known that $A_5 \simeq \mathrm{SL}_2(\mathbb{F}_4)$ as an abstract group. Notice that $\mathrm{PGL}_2(\mathbb{F}_4) \simeq \mathrm{PSL}_2(\mathbb{F}_4) = \mathrm{SL}_2(\mathbb{F}_4)$ since $(\mathbb{F}_4^\times)^2 = \mathbb{F}_4^\times$. Then we have an embedding

$$\mathrm{SL}_2(\mathbb{F}_4) \simeq \mathrm{PGL}_2(\mathbb{F}_4) \xrightarrow{\sim} (\mathrm{Aut}_{\mathrm{alg}}(\mathbb{P}^1_{\mathbb{F}_4}))(\mathbb{F}_4) \hookrightarrow \mathrm{Aut}_{\mathrm{set}}(\mathbb{P}^1(\mathbb{F}_4))$$

where $\mathrm{Aut}_{\mathrm{alg}}(\mathbb{P}^1_{\mathbb{F}_4})$ stands for a group scheme of the algebraic automorphisms of $\mathbb{P}^1_{\mathbb{F}_4}$ while $\mathrm{Aut}_{\mathrm{set}}(\mathbb{P}^1(\mathbb{F}_4))$ stands for the set theoretic automorphisms. It follows $\mathrm{Aut}_{\mathrm{set}}(\mathbb{P}^1(\mathbb{F}_4)) \simeq S_5$ since $|\mathbb{P}^1(\mathbb{F}_4)| = 5$. By counting elements, we can check the image of the above embedding is, indeed, A_5. Fix a generator a of $\mathbb{F}_4^\times$. Let us give all conjugacy classes of $\mathrm{SL}_2(\mathbb{F}_4)$ as below:

- the identity matrix I_2;
- $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$ the class of order 2;
- $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ the class of order 3;
- $\left(\begin{smallmatrix} 1 & 0 \\ 1 & a \end{smallmatrix}\right)$ the class of order 5;
- $\begin{pmatrix} 1 & 0 \\ 1 & a^2 \end{pmatrix}$ the class of order 5.

3.4. Representations of A_5 to $\mathrm{GSp}_4(\overline{\mathbb{F}}_2)$. As in the previous subsection, we fix an isomorphism $A_5 \simeq \mathrm{SL}_2(\mathbb{F}_4)$ and let us denote its tautological faithful representation by $\bar{\tau} : A_5 \to \mathrm{GL}_2(\mathbb{F}_4)$ whose image coincides with $\mathrm{SL}_2(\mathbb{F}_4)$. Since the determinant character of $\bar{\tau}$ is trivial, $\bar{\tau}_1 := \mathrm{Sym}^3 \bar{\tau} : A_5 \to \mathrm{GL}_4(\mathbb{F}_4)$ factors through $\mathrm{GSp}_4(\mathbb{F}_4)$. By direct computation, one can check $\mathrm{End}_{\bar{\tau}_1}(\mathbb{F}_4^{\oplus 4}) = \mathbb{F}_4$. Hence $\bar{\tau}_1$ is absolutely irreducible. By Example 5.1.9 of [9], the restriction of $S_5(b)$ (see the table in Lemma 5.1.7 of loc. cit.) to A_5 gives a representation of A_5 to $\mathrm{GSp}_4(\mathbb{F}_2)$ which is equivalent to $\bar{\tau}_1$ by Brauer–Nesbitt's theorem. Notice that $\mathrm{Im}(\bar{\tau}_1)$ contains no element of type $(3,3)$ under a fixed isomorphism $\mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$.

On the other hand, we regard $\mathbb{F}_4$ as a two dimensional vector space over $\mathbb{F}_2$. Put $V = \mathbb{F}_4^{\oplus 2} \simeq \mathbb{F}_2^{\oplus 4}$. Then a map $\langle\,\cdot\,,\cdot\,\rangle : V \times V \to \mathbb{F}_2$, $((x_1,y_1),(x_2,y_2)) \mapsto \mathrm{tr}_{\mathbb{F}_4/\mathbb{F}_2}(x_1x_2 + y_1y_2)$ yields a non-degenerate alternating form on V. Hence we have another representation $\bar{\tau}_2 : A_5 \to \mathrm{SL}_2(\mathbb{F}_4) \to \mathrm{GSp}_4(V, \langle\,\cdot\,,\cdot\,\rangle) \simeq \mathrm{GSp}_4(\mathbb{F}_2)$. It is easy to see that it is irreducible over $\mathbb{F}_2$ but not absolutely irreducible. In fact, over $\mathbb{F}_4$, it is included in the endoscopic subgroup $H(\mathbb{F}_4)$ up to conjugacy. Notice that $\mathrm{Im}(\bar{\tau}_2)$ contains an element of type $(3,3)$. Combining the above observation with Lemma 5.1.7 of [9], we have the following:

Proposition 3.1. *Let G be a group and $\bar{\rho} : G \to \mathrm{GSp}_4(\mathbb{F}_2)$ be a representation. Fix an isomorphism $\mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$. Suppose that $\mathrm{Im}(\bar{\rho}) \simeq A_5$ and $\mathrm{Im}(\bar{\rho})$ contains no element of type $(3,3)$. Then $\bar{\rho}$ is absolutely irreducible and it is equivalent to $\bar{\tau}_1$ via the isomorphism $\mathrm{Im}(\bar{\rho}) \simeq A_5$.*

3.5. Semi-simplicity. Let $\mathbb{F}_q$ be a finite field of characteristic 2. Let G be a group and $\bar{\rho} : G \to \mathrm{GSp}_4(\mathbb{F}_q)$ be a representation. As in the previous section, by taking the base change to $\mathbb{F}_q$ we have the identification $\mathrm{GSp}_4(\mathbb{F}_q) = \mathrm{GSp}(W_{\mathbb{F}_q}, \langle\,\cdot\,,\cdot\,\rangle_{W_{\mathbb{F}_q}})$. The dual $\bar{\rho}^\vee$ of $\bar{\rho}$ is naturally identified with $\bar{\rho}$ by using $\langle\,\cdot\,,\cdot\,\rangle_{W_{\mathbb{F}_q}}$.

Proposition 3.2. *Keep the notation as above. There exists a symplectic basis of W such that if $\bar{\rho}$ is reducible, then either of the followings holds:*

(1) $\mathrm{Im}(\bar{\rho}) \subset B(\mathbb{F}_q)$*;*
(2) $\mathrm{Im}(\bar{\rho}) \subset P(\mathbb{F}_q)$ *but* $\bar{\rho} \not\subset B(\mathbb{F}_q)$*;*
(3) $\mathrm{Im}(\bar{\rho}) \subset Q(\mathbb{F}_q)$ *but* $\bar{\rho} \not\subset B(\mathbb{F}_q)$*;*
(4) $\mathrm{Im}(\bar{\rho}) \subset H(\mathbb{F}_q)$ *but neither of parabolic subgroups contains* $\mathrm{Im}(\bar{\rho})$*;*

Proof. It follows by using the alternating pairing. ☐

Corollary 3.3. *Keep the notation in Proposition 3.2. Assume that* $\mathbb{F}_q = \mathbb{F}_2$*. If* $\mathrm{Im}(\bar{\rho})$ *contains an element of order five, then* $\bar{\rho}$ *is irreducible.*

Proof. It follows from Lemma 2.1 and Proposition 3.2. ☐

Recall the subgroups of S_6 whose order divisible by five are given as follows:

$$C_5, D_{10} := C_2 \ltimes C_5,\ F_{20} := C_4 \ltimes C_5,\ A_5,\ S_5,\ A_6,\ S_6.$$

Let us fix an isomorphism $\mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$.

Proposition 3.4. *Let G be a group and $\bar{\rho} : G \to \mathrm{GSp}_4(\mathbb{F}_2)$ be a representation such that the order of* $\mathrm{Im}(\bar{\rho})$ *is divisible by five and* $\mathrm{Im}(\bar{\rho})$ *contains no element of type* $(3,3)$*. Then the following are equivalent*

(1) $\mathrm{Im}(\bar{\rho})$ *is isomorphic to neither C_5 nor D_{10};*
(2) $\bar{\rho}$ *is absolutely irreducible.*

Proof. Suppose that $\mathrm{Im}(\bar{\rho})$ is isomorphic to either C_5 or D_{10}. In either case, $\mathrm{Im}(\bar{\rho})$ contains C_5 and let us put $H = \bar{\rho}^{-1}(C_5)$. Then $\bar{\rho}|_H$ is reducible over $\mathbb{F}_{2^4}$. Let $\omega_4 : H \to \mathbb{F}_{2^4}^\times$ be a component of $\bar{\rho}|_H$ which is of order five. Then it is easy to see that $\bar{\rho}|_H \simeq \omega_4 \oplus \omega_4^2 \oplus \omega_4^4 \oplus \omega_4^8$. Therefore, the case when $\mathrm{Im}(\bar{\rho}) \simeq C_5$ is done. In the case when $\mathrm{Im}(\bar{\rho}) \simeq D_{10}$, we have $\bar{\rho} \simeq \mathrm{Ind}_H^G\,\omega_4 \oplus \mathrm{Ind}_H^G\,\omega_4^2$.

Assume to the contrary. If $\bar{\rho}$ is not absolutely irreducible, we see that it is contained in $P'(\mathbb{F}_q)$ or $H(\mathbb{F}_q)$ for a finite extension $\mathbb{F}_q/\mathbb{F}_2$ where P' is one of three parabolic subgroups in Section 2. Assume $\mathrm{Im}(\bar{\rho}) \subset P'(\mathbb{F}_q)$. Then an element of order five in $\mathrm{Im}(\bar{\rho})$ has to belong to the Levi factor of P' which normalizes the unipotent radical of P'. However, this can not occur by the structure of P'. When $\mathrm{Im}(\bar{\rho}) \subset H(\mathbb{F}_q)$ but $\mathrm{Im}(\bar{\rho}) \not\subset P'(\mathbb{F}_q)$ for any parabolic subgroup P', by Lemma 5.1.7 and Example 5.1.11 of [9], the only possibility is $\mathrm{Im}(\bar{\rho}) \simeq A_5$ and $\bar{\rho}$ is obtained from the natural action of

$A_5 \simeq \mathrm{SL}_2(\mathbb{F}_4)$ acting on $\mathbb{F}_4^{\oplus 2} \simeq \mathbb{F}_2^{\oplus 4}$. Then the image contains an element of type (3,3) but it contradicts the assumption. ☐

Let G be a group with a subgroup H of index 2. For a representation $\rho : H \to \mathrm{GL}(V)$ of H and a lift $\widetilde{h}$ of the generator h of G/H to G, we define the representation $\rho \otimes {}^h\rho$ of G by

$$(\rho \otimes {}^h\rho)(g)(x \otimes y) = \begin{cases} \rho(g)x \otimes \rho(\widetilde{h}^{-1}g\widetilde{h})y & (g \in H) \\ y \otimes \rho(\widetilde{h}^2)x & (g = \widetilde{h}), \end{cases} \quad x, y \in V$$

whose isomorphism class is independent of the choice of $\widetilde{h}$. For any quadratic extension M/K of fields with $\mathrm{Gal}(M/K) = \langle \iota \rangle$ and a Galois representation ρ of G_M, the representation $\rho \otimes {}^\iota\rho$ of G_K is said to be the twisted tensor product of ρ (cf. [7, Section 2.1]).

Let us fix an isomorphism $\mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$.

Proposition 3.5. *Let K be a totally real field. Let $\bar{\rho} : G_K \to \mathrm{GSp}_4(\mathbb{F}_2)$ be an irreducible mod 2 Galois representation. Suppose that $\mathrm{Im}(\bar{\rho})$ is isomorphic to S_5 and $\mathrm{Im}(\bar{\rho})$ contains no element of type $(3,3)$. Assume further that for each complex conjugation c of G_K, $\bar{\rho}(c)$ is of type $(2,2)$. Then there exist a totally real quadratic extension M/K with $\mathrm{Gal}(M/K) = \langle \iota \rangle$ and an irreducible totally odd Galois representation $\bar{\tau} : G_M \to \mathrm{GL}_2(\mathbb{F}_4)$ satisfying*

1. *$\bar{\rho} \simeq \bar{\tau} \otimes {}^\iota\bar{\tau}$ as a representation to $\mathrm{GL}_4(\mathbb{F}_4)$;*
2. *$\mathrm{Im}(\bar{\tau}) \simeq \mathrm{SL}_2(\mathbb{F}_4) \simeq A_5$;*
3. *for each complex conjugation c of G_K, $\bar{\tau}(c)$ is conjugate to $s := \left(\begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix}\right)$.*

Proof. Let us fix an isomorphism $\mathrm{Im}(\bar{\rho}) \simeq S_5$ and consider the composition $\mu := \mathrm{sgn} \circ \bar{\rho} : G_K \to \{\pm 1\}$ where $\mathrm{sgn} : S_5 \to \{\pm 1\}$ stands for the sign character. By assumption, for each complex conjugation c of G_K, $\mu(c) = 1$. Hence there exists a totally real quadratic extension M/K corresponding to the kernel of ν such that $\bar{\rho}(G_M) \simeq A_5$. Since $A_5 \simeq \mathrm{SL}_2(\mathbb{F}_4)$, there is a representation $\bar{\tau} : G_M \to \mathrm{SL}_2(\mathbb{F}_4)$ such that $\mathrm{Im}(\bar{\rho}|_{G_M}) \simeq \mathrm{Im}(\bar{\tau})$. Under this isomorphism, by comparing characteristic polynomials of all elements in S_5 by using results in Section 3.1 and Section 3.3, we can easily check that

$$\bar{\rho} \simeq \bar{\tau} \otimes {}^\iota\bar{\tau}$$

by the Brauer–Nesbitt theorem.

Further, by assumption, for each complex conjugation c of G_K, $\bar{\rho}(c)$ is conjugate to either J or $\begin{pmatrix} s & 0_2 \\ 0_2 & s \end{pmatrix}$. They are not conjugate in $\mathrm{GSp}_4(\mathbb{F}_2)$ but conjugate each other in $\mathrm{GL}_4(\mathbb{F}_2)$. The third claim follows from this. ☐

Remark 3.6.

1. *The group S_5 can be realized in $\mathrm{GSp}_4(\mathbb{F}_2)$ as a twisted tensor product of a mod 2 two-dimensional representation $\bar{\tau}$ of A_5 twisted by S_5/A_5*

as in Theorem 3.5. As in Proposition 3.4, it is absolutely irreducible even after the restriction to A_5. *On the other hand,* $\mathrm{Ind}_{A_5}^{S_5}\bar{\tau}$ *is a representation to* $\mathrm{GSp}_4(\mathbb{F}_4)$ *which can not be descend to* $\mathrm{GSp}_4(\mathbb{F}_2)$ *since it contains an element of order 3 with the characteristic polynomial* $(1+t+t^2)^2$. *Such representations appear in the context of* [44] *regarding abelian surfaces with real multiplication by* $\mathbb{Q}(\sqrt{5})$.

(2) *It is easy to see that* $\wedge^2 \mathrm{Ind}_{G_M}^{G_K}\bar{\tau} \simeq (\bar{\tau}\otimes {}^{\iota}\bar{\tau}) \oplus \mathbf{1} \oplus \mathbf{1}$.

Proposition 3.7. *Let* K *be a totally real field. Let* $\bar{\rho} : G_K \to \mathrm{GSp}_4(\mathbb{F}_2)$ *be an irreducible mod 2 Galois representation. Suppose that* $\mathrm{Im}(\bar{\rho})$ *is isomorphic to* A_5 *and* $\mathrm{Im}(\bar{\rho})$ *contains no element of type* $(3,3)$. *Assume further that for each complex conjugation* c *of* G_K, $\bar{\rho}(c)$ *is of type* $(2,2)$. *Then there exists an irreducible totally odd Galois representation* $\bar{\tau} : G_K \to \mathrm{GL}_2(\mathbb{F}_4)$ *satisfying*

(1) $\bar{\rho} \simeq \mathrm{Sym}^3(\bar{\tau})$ *as a representation to* $\mathrm{GL}_4(\mathbb{F}_4)$*;*
(2) $\mathrm{Im}(\bar{\tau}) \simeq \mathrm{SL}_2(\mathbb{F}_4) \simeq A_5$*;*
(3) *for each complex conjugation* c *of* G_K, $\bar{\tau}(c)$ *is conjugate to* $s := \left(\begin{smallmatrix}0&1\\1&0\end{smallmatrix}\right)$.

Proof. As in the proof of the previous proposition, we have only to compute the characteristic polynomials by using the results in Section 3.1, Section 3.3, and Proposition 3.1. ☐

4. Automorphy

4.1. Automorphic Galois representations. Let F be a totally real field. For each place v of F, let F_v be the completion of F along v. In this section we recall basic properties of cuspidal automorphic representations of $\mathrm{GSp}_4(\mathbb{A}_F)$ whose infinite components are discrete series representations. We basically follow the notation of Mok's article [34] and add more necessary ingredients 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 $m_1 > m_2 > 0$ and $m_1 + m_2 \equiv w+1 \bmod 2$. The L-parameter $\phi_{(w;m_1,m_2)} : W_{\mathbb{R}} \to \mathrm{GSp}_4(\mathbb{C})$ is defined by

$$\phi_{(w;m_1,m_2)}(z) = |z|^{-w}\,\mathrm{diag}\Big(\Big(\frac{z}{\bar{z}}\Big)^{\frac{m_1+m_2}{2}}, \Big(\frac{z}{\bar{z}}\Big)^{\frac{m_1-m_2}{2}}, \Big(\frac{z}{\bar{z}}\Big)^{-\frac{m_1-m_2}{2}}, \Big(\frac{z}{\bar{z}}\Big)^{-\frac{m_1+m_2}{2}}\Big)$$

and

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

By local Langlands correspondence the archimedean L-packet $\Pi(\phi_{(w;m_1,m_2)})$ corresponding to $\phi_{(w;m_1,m_2)}$ consists of two elements $\{\pi^H_{(w;m_1,m_2)}, \pi^W_{(w;m_1,m_2)}\}$

whose central characters both satisfy $z \mapsto z^{-w}$ for $z \in \mathbb{R}^{\times}_{>0}$. These are essentially tempered unitary representations of $\mathrm{GSp}_4(\mathbb{R})$ and tempered exactly when $w = 0$. Since $m_2 > 0$, the representation $\pi^{H}_{(w;m_1,m_2)}$ is called a 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

$$V_{\underline{k}} := \mathrm{Sym}^{k_1-k_2}\,\mathrm{St}_2 \otimes \det{}^{k_2}\,\mathrm{St}_2 = \mathrm{Sym}^{m_1-m_2-1}\,\mathrm{St}_2 \otimes \det{}^{m_2+2}\,\mathrm{St}_2$$

of $K_{\mathbb{C}} = \mathrm{GL}_2(\mathbb{C})$. Here K is the maximal compact subgroup of $\mathrm{Sp}_4(\mathbb{R})$. The representation $\pi^{H}_{(w;m_1,m_2)}$ is called a discrete series representation of minimal K-type

$$V_{(m_1+1,-m_2)} = \mathrm{Sym}^{m_1+m_2+1}\,\mathrm{St}_2 \otimes \det{}^{-m_2}\,\mathrm{St}_2\,.$$

Fix an integer w. Let $\pi = \otimes'_v \pi_v$ be a cuspidal automorphic representation of $\mathrm{GSp}_4(\mathbb{A}_F)$ such that for each infinite place v, π_v has L-parameter $\varphi_{(w;m_{1,v},m_{2,v})}$ with the parity condition $m_{1,v} + m_{2,v} \equiv w + 1 \bmod 2$ and $m_2 > 0$. Let $\mathrm{Ram}(\pi)$ be the set of all finite places of which π_v is ramified. Thanks to [34] with [24] we can attach to π certain Galois representations:

Theorem 4.1 ([34, Theorem 3.1 and Remark 3.3, Theorem 1.1])**.** *Assume that π 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 $\rho_{\pi,\iota_p} : G_F \to$* $\mathrm{GSp}_4(\overline{\mathbb{Q}}_p)$ *such that*

1. $\nu \circ \rho_{\pi,\iota_p}(c_\infty) = -1$ *for any complex conjugation c_∞ in G_F where ν is the similitude character of* GSp_4.
2. ρ_{π,ι_p} *is unramified for all finite places which do not belong to* $\mathrm{Ram}(\pi) \cup \{v|p\}$;
3. *for each finite place v of F not lying over p, the local-global compatibility holds:*

   $$\mathrm{WD}(\rho_{\pi,\iota_p}|_{G_{F_v}})^{F-\mathrm{ss}} \simeq \mathrm{rec}^{\mathrm{GT}}_v(\pi_v \otimes |\nu|^{-\frac{3}{2}})$$

   with respect to ι_p where $\mathrm{rec}^{\mathrm{GT}}_v$ stands for the local Langlands correspondence constructed by Gan–Takeda [21];
4. *for each finite place v of F lying over p, $\rho_{\pi,\iota_p}|_{G_{F_v}}$ is crystalline and the local-global compatibility also holds up to semi-simplification.*
5. *for each $v|p$ and an embedding $\sigma : F_v \hookrightarrow \overline{\mathbb{Q}}_p$, there is a unique embedding $v_\sigma : F \hookrightarrow \mathbb{C}$ such that $\iota_p \circ \sigma|_F = v_\sigma$. Then the representation $\rho_{\pi,\iota_p}|_{G_{F_v}}$ is Hodge–Tate of 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 $\delta_{v_\sigma} = \frac{1}{2}(w + 3 - m_{1,v_\sigma} - m_{2,v_\sigma})$.

Definition 4.2.

(1) *Let* $\rho : G_F \to \mathrm{GSp}_4(\overline{\mathbb{Q}}_p)$ *be an irreducible* p*-adic Galois representation. We say* ρ *is automorphic if there exists a cuspidal automorphic representation* π *of* $\mathrm{GSp}_4(\mathbb{A}_F)$ *with* π_v *a discrete series representation for any* $v|\infty$ *such that* $\rho \simeq \rho_{\pi,\iota_p}$ *as a representation to* $\mathrm{GL}_4(\overline{\mathbb{Q}}_p)$*. By definition, if* ρ *is automorphic, then it is totally odd.*

(2) *Let* $\bar{\rho} : G_F \to \mathrm{GSp}_4(\overline{\mathbb{F}}_p)$ *be an irreducible mod* p *Galois representation. We say* $\bar{\rho}$ *is automorphic if there exists a cuspidal automorphic representation* π *of* $\mathrm{GSp}_4(\mathbb{A}_F)$ *with* π_v *a discrete series representation for any* $v|\infty$ *such that* $\bar{\rho} \simeq \bar{\rho}_{\pi,\iota_p}$ *as a representation which takes the values in* $\mathrm{GL}_4(\overline{\mathbb{F}}_p)$*.*

Remark 4.3.

(1) *For each holomorphic Hilbert–Siegel Hecke eigen cusp form* h *over* F *on* $\mathcal{H}_2^d$*, one can associate a cuspidal automorphic form on* $\mathrm{GSp}_4(\mathbb{A}_F)$ *and vice versa. We often identify these two forms.*

(2) *Let* h *be a holomorphic Hilbert–Siegel Hecke eigen cusp form on* $\mathcal{H}_2^d$ *of parallel weight* 3 *where* $d = [F : \mathbb{Q}]$*. Let* π_h *be the corresponding cuspidal automorphic representation of* $\mathrm{GSp}_4(\mathbb{A}_F)$*. Then for each infinite place* v*, the local Langlands parameter at* v *is given by* $\phi_{(w;2,1)}$ *for some* $w \in \mathbb{Z}$*. Conversely, if a cuspidal automorphic representation* π *of* $\mathrm{GSp}_4(\mathbb{A}_F)$ *is neither CAP nor endoscopic, one can associate such a form* h *by using* [47] *for* $F = \mathbb{Q}$ *and* [24] *in general. Note that the results in* [24] *are conditional on the trace formula (see* [24, second paragraph in p. 472]*).*

4.2. Paritious Hilbert modular forms and Jacquet–Langlands correspondence. We refer to [44] and [32, Section 3]. In this section, p is any rational prime, but we remind the readers to keep in mind the application to $p = 2$. Let F be a totally real field of even degree g. For each finite place v of F, let F_v be the completion of F along v, $\mathcal{O}_v$ its integer ring, ϖ_v a uniformizer of F_v, and $\mathbb{F}_v$ the residue field of F_v. Let D be a quaternion algebra with center F which is ramified exactly at all the infinite places of F and $\mathcal{O}_D$ be a maximal order of D. For each finite place v of F, we fix an isomorphism $\iota_v : D_v := D \otimes_F F_v \simeq \mathrm{GL}_2(F_v)$. We view $D^\times$ as an algebraic group over F so that for any F-algebra A, $D^\times(A)$ outputs $(D \otimes_F A)^\times$ and similarly as an algebraic group scheme over $\mathcal{O}_F$ such that $D^\times(R) = (\mathcal{O}_D \otimes_{\mathcal{O}_F} R)^\times$ for any $\mathcal{O}_F$-algebra R.

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

For each finite place v lying over p of F, let τ_v be a smooth representation of $\mathrm{GL}_2(\mathcal{O}_v)$ on a finite free $\mathcal{O}$ module W_{τ_v}. We also view it as a representation of D_v via ι_v. Put $\tau := \otimes_{v|p} \otimes_{\sigma_v \in \mathrm{Hom}(F_v,\overline{\mathbb{Q}}_p)} {}^{\sigma_v}\tau_v$ which is a representation of $\mathrm{GL}_2(\mathcal{O}_p)$ acting on $W_\tau := \otimes_{v|p} \otimes_{\sigma_v \in \mathrm{Hom}(F_v,\overline{\mathbb{Q}}_p)} {}^{\sigma_v}W_{\tau_v}$. Suppose $\psi : F^\times \backslash (\mathbb{A}_F^\infty)^\times \to \mathcal{O}^\times$ is a continuous character so that for each $v|p$, $Z_{D^\times}(\mathcal{O}_v) \simeq \mathcal{O}_v^\times$ acts on W_{τ_v} by $\psi^{-1}|_{\mathcal{O}_{F_v}^\times}$ where $Z_{D^\times} \simeq GL_1$ be the center of $D^\times$ as a group scheme over $\mathcal{O}_F$. Note that we put the discrete topology on $\mathcal{O}^\times$ and therefore such a character is necessarily of finite order. Let $U = \prod_v U_v$ be a compact open subgroup of $D^\times(\mathbb{A}_F^\infty) \simeq \mathrm{GL}_2(\mathbb{A}_F^\infty)$ such that $U_v \subset D^\times(O_{F_v})$ for each finite place v of F. Put $U_p := \prod_{v|p} U_v$ and $U^{(p)} = \prod_{v\nmid p} U_v$. For any local $\mathcal{O}$-algebra A put $W_{\tau,A} := W_\tau \otimes_{\mathcal{O}} A$. Let Σ be a finite set of finite places of F. For each $v \in \Sigma$, let $\chi_v : U_v \to A^\times$ be a quasi character. Define $\chi_\Sigma : U \to A^\times$ whose local component is χ_v if $v \in \Sigma$, the trivial representation otherwise.

Definition 4.4 (p-adic algebraic quaternionic forms)**.** *Let $S_{\tau,\psi}(U,A)$ denote the space of the functions $f : D^\times \backslash D^\times(\mathbb{A}_F^\infty) \to W_{\tau,A}$ such that*

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

Similarly, let $S_{\tau,\psi,\chi_\Sigma}(U,A)$ denote the space of the functions $f : D^\times \backslash D^\times(\mathbb{A}_F^\infty) \to W_{\tau,A}$ 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 $g \in D^\times(\mathbb{A}_F^\infty)$;*
- *$f(zg) = \psi(z)f(g)$ for $z \in Z_{D^\times}(\mathbb{A}_F^\infty)$ and $g \in D^\times(\mathbb{A}_F^\infty)$.*

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

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

$$\mathbb{T}_A^S := A[T_v, S_v]_{v \notin S \cup \{v|p\}} \tag{4.1}$$

where

$$T_v = [D^\times(\mathcal{O}_v)\iota_v^{-1}(\mathrm{diag}(\varpi_v, 1))D^\times(\mathcal{O}_v)],$$
$$S_v = [D^\times(\mathcal{O}_v)\iota_v^{-1}(\mathrm{diag}(\varpi_v, \varpi_v))D^\times(\mathcal{O}_v)]$$

are 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. [15, Definition 2.2]).

Let $U = U^{(p)} \times U_p$ be as above. As explained in [44, Section 1], if we take the double coset decomposition $\mathrm{GL}_2(\mathbb{A}_F^\infty) = \coprod_i D^\times t_i U Z_{D^\times}(\mathbb{A}_F^\infty)$, then

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

The group $(UZ_{D^\times}(\mathbb{A}_F^\infty)\cap t_i^{-1}D^\times t_i)/F^\times$ is trivial for all t_i when U is sufficiently small (see [32, 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. [33, Lemma 3.1.4]).

Fix an isomorphism $\iota : \overline{\mathbb{Q}}_p \simeq \mathbb{C}$. 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. For each $(\underline{k},\underline{w}) = ((k_\sigma)_\sigma,(w_\sigma)_\sigma) \in \mathbb{Z}_{>1}^{\mathrm{Hom}(F,\overline{\mathbb{Q}}_p)} \times \mathbb{Z}^{\mathrm{Hom}(F,\overline{\mathbb{Q}}_p)}$ such that $k_\sigma + 2w_\sigma$ is independent of σ. This independence is called the parity condition and it is necessary to arithmetic structure on the space of Hilbert modular forms. Let $\psi_{\mathbb{C}} : F^\times\backslash\mathbb{A}_F^\times \to \mathbb{C}^\times$ be the character defined by

$$\psi_{\mathbb{C}}(z) = \iota(N(z_p)^{\delta-1}\psi(z^\infty))N(z_\infty)^{1-\delta} \tag{4.2}$$

for $z = (z_p, z^{(p)}, z_\infty) \in \mathbb{A}_F^\times$ where the symbol N stands for the norm. For each $\sigma \in \mathrm{Hom}(F,\overline{\mathbb{Q}}_p)$, there exist a unique pair of $v|p$ and an embedding $\sigma_v : F_v \to \overline{\mathbb{Q}}_p$ such that $\sigma_v|_F = \sigma$. There we can rewrite $(\sigma)_{\sigma\in\mathrm{Hom}(F,\overline{\mathbb{Q}}_p)} = (\sigma_v)_{v|p,\ \sigma_v\in\mathrm{Hom}(F_v,\overline{\mathbb{Q}}_p)}$. Let us define the representation $\tau_{(\underline{k},\underline{w}),A}$ of $\mathrm{GL}_2(\mathcal{O}_p) = \prod_{v|p}\mathrm{GL}_2(\mathcal{O}_v)$ by

$$\tau_{(\underline{k},\underline{w}),A} = \bigotimes_{v|p}\ \bigotimes_{\sigma_v\in\mathrm{Hom}(F,\overline{\mathbb{Q}}_p)} \mathrm{Sym}^{k_{\sigma_v}-2}\,\mathrm{St}_2(A)\otimes \det{}^{w_{\sigma_v}} A \tag{4.3}$$

where St_2 is the standard representation of dimension two. We often drop the subscript A from $\tau_{(\underline{k},\underline{w}),A}$ which never causes any confusion. Notice that $\tau_{(\underline{k},\underline{w}),\mathcal{O}} \otimes_{\mathcal{O},\iota} \mathbb{C}$ is the algebraic representation of $\mathrm{GL}_2(\mathbb{C})$ of the 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

$$S_{\underline{k},\underline{w},\psi}(U_p,A) := S_{\tau_{(\underline{k},\underline{w})},\psi}(U_p,\mathcal{O}) \tag{4.4}$$

for simplicity.

By Lemma 1.3-2 of [44], we have an isomorphism of $D^\times(\mathbb{A}^{p,\infty})$-modules

$$(S_{\underline{k},\underline{w},\psi}(U_p,\mathcal{O})/S^{\mathrm{triv}}_{\underline{k},\underline{w},\psi}(U_p,\mathcal{O}))\otimes_{\mathcal{O},\iota}\mathbb{C} \simeq \bigoplus_{\pi} \pi^{\infty,p}\otimes\pi_p^{U_p} \tag{4.5}$$

where π turns over regular algebraic cuspidal automorphic representations of $\mathrm{GL}_2(\mathbb{A}_F)$ such that π has the central character $\psi_{\mathbb{C}}$ and $S^{\mathrm{triv}}_{\underline{k},\underline{w},\psi}(U_p,\mathcal{O})$ is zero unless $(\underline{k},\underline{w}) = (2\cdot\mathbf{1}, w\cdot\mathbf{1})$ with $w \in \mathbb{Z}$ and $\mathbf{1} = (1,\ldots,1) \in \mathbb{Z}^{\mathrm{Hom}(F,\overline{\mathbb{Q}}_p)}$, in which case let it denote the subspace of $S_{\tau_{(\underline{k},\underline{w})},\psi}(U_p,\mathcal{O})$ consisting of functions which factor through the reduced norm of $D^\times(\mathbb{A}_F)$.

For each $\tau_{(\underline{k},\underline{w}),\mathbb{C}}$, one can also consider the space of Hilbert modular cusp forms on $\mathrm{GL}_2(\mathbb{A}_F)$ of level U and of weight $(\underline{k},\underline{w})$ and their geometric counterparts (see [17, Section 1.5]). Thanks to many contributors (see [27] and the reference therein), for each (adelic) Hilbert modular Hecke eigen cusp form f of weight $(\underline{k}, \underline{w})$ and of level U, one can attach an irreducible p-adic Galois representation $\rho_{f,\iota_p} : G_F \to \mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ for any rational prime p and a fixed isomorphism $\iota_p : \overline{\mathbb{Q}}_p \simeq \mathbb{C}$. The construction also works for $\underline{k} \geq \mathbf{1}$ (in the lexicographic order). In particular, in the case when $\underline{k} = \mathbf{1}$ (parallel weight one), its image is finite and it gives rise to an Artin representation $\rho_f : G_F \to \mathrm{GL}_2(\mathbb{C})$ (see [41]). Taking a suitable integral lattice, we consider the reduction $\bar{\rho}_{f,p} : G_F \to \mathrm{GL}_2(\overline{\mathbb{F}}_p)$ of $\rho_{f,p}$ or ρ_f modulo the maximal ideal of $\overline{\mathbb{Z}}_p$.

Recall that we have fixed $\overline{\mathbb{Q}}_p \simeq \mathbb{C}$ and under this isomorphism we identify $\mathrm{Hom}(K, \overline{\mathbb{Q}}_p)$ with $\mathrm{Hom}(K, \mathbb{C})$ for any number field K. Let M be a totally real quadratic extension of a totally real field F. Put $d = [F : \mathbb{Q}]$ and then $m = [M : \mathbb{Q}] = 2d$. For each embedding $\sigma_i \in \mathrm{Hom}(F, \overline{\mathbb{Q}}_p)$ $(1 \leq i \leq d)$, let $\sigma_i^{(1)}$, $\sigma_i^{(2)}$ be the extensions of σ_i to M with any ordering for $\sigma_i^{(1)}$, $\sigma_i^{(2)}$. Put

$$S_M^{(1)} = \left\{\sigma_i^{(1)} \,\middle|\, 1 \leq i \leq d\right\},\ S_M^{(2)} = \left\{\sigma_i^{(2)} \,\middle|\, 1 \leq i \leq d\right\}.$$

According to this notation, we rewrite $(\underline{k}, \underline{w}) = ((k_\sigma)_\sigma, (w_\sigma)_\sigma) \in \mathbb{Z}_{\geq 1}^{\mathrm{Hom}(M,\overline{\mathbb{Q}}_p)} \times \mathbb{Z}^{\mathrm{Hom}(M,\overline{\mathbb{Q}}_p)}$ as

$$(\underline{k}, \underline{w}) = ((\underline{k}^{(1)}, \underline{k}^{(2)}), (\underline{w}^{(1)}, \underline{w}^{(2)})) \in (\mathbb{Z}_{\geq 1}^d)^2 \times (\mathbb{Z}^d)^2.$$

Put $\mathbf{1}_m = (1, \ldots, 1) \in \mathbb{Z}^m$ and $\mathbf{1}_d = (1, \ldots, 1) \in \mathbb{Z}^d$.

The following result is a key step for residual automorphy results:

Proposition 4.5. *Put $p = 2$. Assume that M/F is a totally real quadratic extension of a totally real field F. Put $d = [F : \mathbb{Q}]$ and $m = [M : \mathbb{Q}] = 2d$. Let f be a Hilbert modular Hecke eigen cusp form on $\mathrm{GL}_2(\mathbb{A}_M)$ of parallel weight one such that $\bar{\rho}_{f,2}$ is irreducible. There exists a Hilbert modular Hecke eigen cusp form g on $\mathrm{GL}_2(\mathbb{A}_M)$ such that*

1. *$\bar{\rho}_{f,2} \simeq \bar{\rho}_{g,2} \otimes \psi$ for some continuous character $\psi : G_M \to \overline{\mathbb{F}}_2^\times$;*
2. *the character corresponding to the central character of g under (4.2) is trivial;*
3. *g is of weight $(\underline{k}, \underline{w})$ with $\underline{k} = 2 \cdot \mathbf{1}_m$ (parallel weight 2) for some $\underline{w} \in \mathbb{Z}^m$.*

Furthermore, g can be taken to be congruent modulo a prime lying over 2 to a Hilbert modular Hecke eigen cusp form of weight $(\underline{k}, \underline{w}')$ with

$$\underline{k} = (2 \cdot \mathbf{1}_d, 4 \cdot \mathbf{1}_d)$$

for some $\underline{w}' \in \mathbb{Z}^m$.

Proof. Let U be a sufficiently small open compact subgroup of $\mathrm{GL}_2(\mathbb{A}_M)$ which fixes f. Fix $\underline{w} = w \cdot \mathbf{1}_m$ for some $w \in \mathbb{Z}$ in the weight of f. Let K be a sufficiently large finite extension of $\mathbb{Q}_2$ in $\overline{\mathbb{Q}}_2$ with the integer ring $\mathcal{O}$ such that K contains all Hecke eigen values of f for $\mathbb{T}^S_{\mathcal{O}}$. Let $\mathbb{F}$ be the residue field of K. As in [17], we can view f as a geometric Hilbert modular form over $\mathcal{O}$ via a classical Hilbert modular form associated to f and consider its base change $\bar{f}$ to $\mathbb{F}$. By multiplying a high power of Hasse invariant, we have another form $\bar{g}_1$ of weight $(\underline{k}, \underline{w})$ with $\underline{k} = n \cdot \mathbf{1}_m,\ n \gg 0$ such that

(1) $\bar{g}_1$ is a liftable to a geometric Hilbert modular Hecke eigenform g_1 over $\mathcal{O}$ by enlarging $\mathcal{O}$ if necessary;

(2) $\bar{\rho}_{g_1,2} \simeq \bar{\rho}_{f,2}$.

Let us get g_1 back to the classical Hilbert modular Hecke eigen cusp form and by Jacquet–Langlands correspondence, we have a 2-adic algebraic quaternionic Hecke eigenform h_1 in $S_{\tau_{(\underline{k},\underline{w})},\psi}(U, \mathcal{O})$ corresponding to g_1 where $\psi : M^\times \backslash \mathbb{A}_M^\infty \to \mathcal{O}^\times$ is the finite character corresponding to the central character of g_1 under (4.2). For each finite place v of M lying of over 2, let $U_{1,v}$ be the subgroup U_v consisting of all elements congruent to $\left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right)$. Put $U_{1,2} := \prod_{v|2} U_{1,v}$. By definition, $\overline{h}_1 \in S_{\tau_{(\underline{k},\underline{w})},\psi}(U^{(2)} \times U_{1,2}, \mathbb{F})$. Since $U_{1,2}$ acts on $\tau_{(\underline{k},\underline{w}),\mathbb{F}}$ unipotently, it can be written as a successive extension of the trivial representation of $U_{1,2}$. This successive extension commutes with Hecke actions and one can find a Hecke eigenform $\overline{h}_2 \in S_{\tau_{(2\cdot\mathbf{1},\underline{w})},\psi}(U^{(2)} \times U_{1,2}, \mathbb{F})$. Further, notice that $(\mathbb{F}^\times)^2 = \mathbb{F}^\times$ and by twisting, we may assume that the reduction $\overline{\psi}$ of ψ is trivial. Since U is taken to be sufficiently small, there exists a lift $h_2 \in S_{\tau_{(2\cdot\mathbf{1},\underline{w})},\psi^{\mathrm{triv}}}(U^{(2)} \times U_{1,2}, \mathcal{O})$ of $\overline{h}_2$ where ψ^{triv} stands for the trivial character. By using Lemma 6.11 of [14], h_2 can be taken to be a Hecke eigenform by multiplicity one. Further by Theorem 1.3-4 of [44], h_2 is non-trivial since $\bar{\tau}$ is absolutely irreducible. The desired form g is obtained as the image of h_2 under the Jacquet–Langlands correspondence.

Let us keep the form $\overline{h}_2 \in S_{\tau_{(2\cdot\mathbf{1},\underline{w})},\overline{\psi}^{\mathrm{triv}}}(U^{(2)} \times U_{1,2}, \mathbb{F})$. For each finite place v of M lying over 2 and embedding $\sigma_v : M_v \to \overline{\mathbb{Q}}_2$ which induces an embedding $\mathbb{F}_v \hookrightarrow \mathbb{F}$, let us observe the following exact sequence of $\mathrm{GL}_2(\mathbb{F}_v)$-modules

$$0 \longrightarrow {}^{\sigma_v}(\mathrm{St}_2(\mathbb{F}))^{(2)} \longrightarrow {}^{\sigma_v}\mathrm{Sym}^2\,\mathrm{St}_2(\mathbb{F}) \longrightarrow {}^{\sigma_v}\det \mathbb{F} \longrightarrow 0. \tag{4.6}$$

Here the superscript "σ_v" means the twisted representation induced by the embedding $\mathbb{F}_v \hookrightarrow \mathbb{F}$. We apply this exact sequence to $S_M^{(2)}$. Since ${}^{\sigma_v}\det : Z_D(\mathcal{O}_v) \to \mathbb{F}^\times$ can be viewed as a square of a character, by twisting, we have a Hecke eigen lift to $\overline{h}_3 \in S_{\tau_{(2\cdot\mathbf{1}_d, 4\cdot\mathbf{1}_d, \underline{w}')},\det^{-1}}(U^{(2)} \times U_{1,2}, \mathbb{F})$. Twisting it back to $\overline{h}_4 \in S_{\tau_{(2\cdot\mathbf{1}_d, 4\cdot\mathbf{1}_d, \underline{w}')},\overline{\psi}^{\mathrm{triv}}}(U^{(2)} \times U_{1,2}, \mathbb{F})$. We have a lift g of $\overline{h}_4$ which has the desired properties. $\square$

4.3. Non-paritious Hilbert modular forms. We refer [16, 35] for non-paritious Hilbert modular forms. Keep the notation in the previous section.

We can also consider Hilbert modular forms on $\mathrm{GL}_2(\mathbb{A}_M)$ of non-paritious weight. However we will immediately encounter the lack of some arithmetic structures for such forms. In fact, the automorphic representation associated to a non-paritious Hilbert cusp form is non-algebraic and its Hecke field is not finite over $\mathbb{Q}$. This explains that we can not construct any p-adic Galois representations for such a form which takes the values in $\mathrm{GL}_2(\overline{\mathbb{Q}}_p)$ for any p. However, if we lift the cuspidal automorphic representation to a suitable group by some Langlands functoriality, it can be algebraic, hence we have a Galois representation. In [35] with his related works, Patrikis has studies there objects throughly. We will use some results in [16] which is related to [35] and it is rather suitable in our purpose.

Let us recall our setting. Let M/F be a real quadratic extension of a totally real field F with the Galois group $\mathrm{Gal}(M/F)=\langle\iota\rangle$. Put $d=[F:\mathbb{Q}]$ and $m=[M:\mathbb{Q}]=2d$. Put $H=\mathrm{Ker}(\mathrm{Nr})=\mathrm{Ker}(D^\times\xrightarrow{\mathrm{Nr}}GL_1)$ where Nr stands for the reduced norm. Clearly, $H(\mathbb{A}^\infty_M)\simeq\mathrm{SL}_2(\mathbb{A}_M)$. For each non-paritious weight $\underline{k}\in\mathbb{Z}^m_{>1}$ and an open compact subgroup U of $H(\mathbb{A}^\infty_M)$ such that $U_v\subset H(\mathcal{O}_v)$ for each finite place v of M, we can also consider the space of p-adic algebraic quaternionic forms on $H(\mathbb{A}_M)$ which we denote it by $S_{\underline{k},\psi}(U_p,\mathcal{O})$ where the weight corresponds to $\tau_{(\underline{k},\underline{0}),\mathcal{O}}|_{U_2\cap H(\mathbb{A}^\infty_M)}$ with $\underline{0}=(0,\dots,0)\in\mathbb{Z}^m$. We define the (formal) Hecke algebra for H by

$$\mathbb{T}^{S,H}_A:=A[T_{2,v}]_{v\notin S\cup\{v|p\}} \tag{4.7}$$

where $T_{2,v}=[H(\mathcal{O}_v)\iota_v^{-1}(\mathrm{diag}(\varpi_v,\varpi_v^{-1}))H(\mathcal{O}_v)]$ and S is as in (4.1). As in the case of paritious weight, if U is sufficiently small, then the reduction map $S_{\underline{k},\psi}(U_p,\mathcal{O})\to S_{\underline{k},\psi}(U_p,\mathbb{F})$ is surjective.

Let us consider the diagonal action of S_d on $\mathbb{Z}^m=\mathbb{Z}^d\times\mathbb{Z}^d$. Similarly, $(\sigma_1,\dots,\sigma_d)\in(S_2)^d$ acts on $\mathbb{Z}^d\times\mathbb{Z}^d$ by

$$\begin{aligned}&\Big(\big(x_1^{(1)},\dots,x_d^{(1)}\big),\big(x_1^{(2)},\dots,x_d^{(2)}\big)\Big)\\ &\qquad\longmapsto\Big(\big(x_1^{(\sigma_1(1))},\dots,x_d^{(\sigma_d(1))}\big),\big(x_1^{(\sigma_1(2))},\dots,x_d^{(\sigma_d(2))}\big)\Big).\end{aligned}$$

Then these two actions induce the action of $(S_2)^d\rtimes\Delta S_d$ on $\mathbb{Z}^d\times\mathbb{Z}^d$ where each $\tau\in S_d$ acts on $(S_2)^d$ by $(\sigma_1,\dots,\sigma_d)\mapsto(\sigma_{\tau(1)},\dots,\sigma_{\tau(d)})$. Then we now prove the following result:

Proposition 4.6. *Put $p=2$. Keep the notation as above. Let f be a Hilbert modular Hecke eigen cusp form on $\mathrm{GL}_2(\mathbb{A}_M)$ of parallel weight one such that $\bar\rho_{f,2}$ is irreducible. There exists a Hilbert modular Hecke eigen cusp form g on $\mathrm{GL}_2(\mathbb{A}_M)$ such that*

1. *the character corresponds to the central character of g under* (4.2)*;*
2. *g is of weight $(\underline{k},\underline{w})$ with $\underline{k}=(2\cdot\mathbf{1}_d,3\cdot\mathbf{1}_d)\in\mathbb{Z}^{S^{(1)}_M}\times\mathbb{Z}^{S^{(2)}_M}$ for some $\underline{w}\in\frac{1}{2}\mathbb{Z}^m$.*

(3) $\bar{\rho}_{f,2}\otimes {}^{\iota}\bar{\rho}_{f,2}\simeq \bar{\rho}_{\Pi,2}\otimes\psi$ *for some continuous character* $\psi : G_M\to \overline{\mathbb{F}}_2^{\times}$ *where* Π *is the automorphic induction of* π_g *to* $\mathrm{GL}_4(\mathbb{A}_F)$ *and* $\bar{\rho}_{\Pi,2}$ *is the reduction of* $\rho_{\Pi,\iota_2} : G_F\to \mathrm{GL}_4(\overline{\mathbb{Q}}_2)$ *constructed in Theorem 5.1 of* [16].

Proof. As in the proof of Proposition 4.5, there exists $\overline{h}\in S_{2\cdot\mathbf{1},\underline{w},\overline{\psi}^{\mathrm{triv}}}(U^{(2)}\times U_{1,2},\mathbb{F})$ for some $w\in\mathbb{Z}^m$ such that the Hecke eigen system of $\overline{h}$ coincides with one of the original f up to twist where $U^{(2)}\times U_{1,2}\subset D^{\times}(\mathbb{A}_M^{\infty})$ is in the proof there. Let us restrict $\overline{h}$ to $(U^{(2)}\times U_{1,2})\cap H(\mathbb{A}_M^{\infty})$ and denote it by $\overline{h}$ again. For each finite place $v\notin S\cup\{v|2\}$ of M, let $\bar{a}_{T_{2,v}}(\overline{h})$ be the eigenvalue of $T_{2,v}$ for $\overline{h}$ and $a_{T_v}(f)$ for f. Then it is easy to see that $\bar{a}_{T_{2,v}}(\overline{h})=a_{T_v}^2(f)$ (mod $m_{\mathcal{O}}$). For each $\sigma\in S_M^{(2)}$, there exist unique finite place v of M lying over 2 and am embedding $\sigma_v : M_v\to\overline{\mathbb{Q}}_2$ such that $\sigma_v|_M=\sigma$. As in (4.6) let us observe the following exact sequence of $\mathrm{GL}_2(\mathbb{F}_v)$-modules

$$0\longrightarrow {}^{\sigma_v}(\mathrm{St}_2(\mathbb{F}))^{(2)}\longrightarrow {}^{\sigma_v}\mathrm{Sym}^2\,\mathrm{St}_2(\mathbb{F})\longrightarrow {}^{\sigma_v}\det\mathbb{F}\longrightarrow 0. \tag{4.8}$$

Since this is non-split as a $U_{1,2}$-module, there exists a Hecke eigenform $\overline{h}_2\in S_{\tau,\overline{\psi}^{\mathrm{triv}}}((U^{(2)}\times U_{1,2})\cap H(\mathbb{A}_M^{\infty}),\mathbb{F})$ for $\tau=\bigotimes_{\sigma\in S_M^{(2)}}\mathrm{Sym}^1\,\mathrm{St}_2^{(2)}(\mathbb{F})$ whose Hecke system for $\mathbb{T}_{\mathbb{F}}^{S,H}$ is same as one of $\overline{h}$. Notice that the Frobenius twist induces a permutation on $\mathrm{Hom}(\mathbb{F}_v,\mathbb{F})$ and the central character is always trivial since the center of H is $Z_H=\mu_2$ the group scheme of order 2. Then it is easy to see that there exists a subset $X\subset S_M^{(1)}\coprod S_M^{(2)}=\mathrm{Hom}(M,\overline{\mathbb{Q}}_2)$ with $|X|=d$ such that $\tau\simeq\bigotimes_{\sigma\in X}\mathrm{Sym}^1\,\mathrm{St}_2(\mathbb{F})$. Let X^c be the complement of X in $\mathrm{Hom}(M,\overline{\mathbb{Q}}_2)$. Then there exists an element $\alpha\in(S_2)^d\rtimes S_d$ such that

$$\alpha\left((2\cdot\mathbf{1}_d,3\cdot\mathbf{1}_d)_{S_M^{(1)}\times S_M^{(2)}}\right)=(2\cdot\mathbf{1}_d,3\cdot\mathbf{1}_d)_{X^c\times X}.$$

Hence we may assume that $\overline{h}_2\in S_{(2\cdot\mathbf{1}_d,3\cdot\mathbf{1}_d),\overline{\psi}^{\mathrm{triv}}}((U^{(2)}\times U_{1,2})\cap H(\mathbb{A}_M^{\infty}),\mathbb{F})$. Then, by Lemma 6.11 of [14], there exist a Hecke eigenform

$$h_2\in S_{(2\cdot\mathbf{1}_d,3\cdot\mathbf{1}_d),\overline{\psi}^{\mathrm{triv}}}((U^{(2)}\times U_{1,2})\cap H(\mathbb{A}_M^{\infty}),\mathcal{O})$$

whose reduction of the Hecke eigen system coincides with one of $\overline{h}_2$. Though we can not conclude that $\overline{h}_2$ coincides with the reduction of h_2 due to the lack of the multiplicity one, it is enough to observe only Hecke eigensystems in our purpose. Let π_{h_2} be the cuspidal automorphic representation associated to h_2. Then there exists a lift π_g of π_{h_2} to $D^{\times}(\mathbb{A}_M)$ such that the character of $M^{\times}\backslash\mathbb{A}_M^{\times}$ corresponding to the central character of π_g via (4.2) and a Hecke eigenform g generating π_g of weight $((2\cdot\mathbf{1}_d,3\cdot\mathbf{1}_d),w')\in\mathbb{Z}^m\times\left(\frac{1}{2}\mathbb{Z}\right)^m$ for some $w'\in\left(\frac{1}{2}\mathbb{Z}\right)^m$. Notice that for each finite place $v\notin S\cup\{v|2\}$ (see (4.7) for the set S) the Hecke eigenvalue $a_{T_{2,v}}(g)$ of $T_{2,v}$ for $g|_{H(\mathbb{A}_M^{\infty})}$ belongs to $\mathcal{O}$, but $a_{T_v}(g) \notin \mathcal{O}$ in general and we have $a_{T_{2,v}}(g) \equiv a_{T_v}^2(f) \pmod{m_{\mathcal{O}}}$. However, it is easy to see that $a_{T_v}(g)a_{T\iota_v}(g) \in \mathcal{O}$ and its reduction modulo $m_{\mathcal{O}}$ can be recovered from the square root of

$$(a_{T_v}(g)a_{T\iota_v}(g))^2 \equiv a_{T_v}^2(f)a_{T\iota_v}^2(f) \pmod{m_{\mathcal{O}}}$$

which is uniquely determined since the characteristic of $\mathbb{F}$ is 2. Notice that the weight of g is not parallel weight 2. By Theorem 6.10 of [16], there exists a Hilbert modular Hecke eigen cusp form on $\mathrm{GL}_2(\mathbb{A}_M)$ of weight $((2 \cdot \mathbf{1}_d, 3 \cdot \mathbf{1}_d), w')$. Hence the claim follows from matching with Frobenius eigenvalues and the Brauer–Nesbitt's theorem. ☐

4.4. mod 2 automorphy.

4.4.1. ***Symplectic automorphy.*** Let F be a totally real field. Let $\bar{\rho} : G_F \to \mathrm{GSp}_4(\mathbb{F}_2)$ be an irreducible mod 2 Galois representation.

Theorem 4.7. *Suppose that* $\mathrm{Im}(\bar{\rho})$ *is isomorphic to* A_5 *and the degree of* $F/\mathbb{Q}$ *is even. Assume further that for each complex conjugation* c *of* G_K*,* $\bar{\rho}(c)$ *is of type* $(2,2)$*. Then there exists a Hilbert–Siegel Hecke eigen cusp form* h *on* $\mathrm{GSp}_4(\mathbb{A}_F)$ *of parallel weight 3 such that* $\bar{\rho} \simeq \bar{\rho}_{h,2}$.

Proof. By Proposition 3.7, there exists a totally odd irreducible representation $\bar{\tau} : G_F \to \mathrm{SL}_2(\mathbb{F}_4)$ such that $\bar{\rho} \simeq \mathrm{Sym}^3 \bar{\tau}$. By Theorem 2 of [43], $\bar{\tau}$ is modular. Further, applying Proposition 4.5, there exists a Hilbert modular cusp form f of $\mathrm{GL}_2(\mathbb{A}_F)$ of parallel weight 2 with the trivial central character such that $\bar{\rho}_{f,2} \simeq \bar{\tau}$. Let π be the cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_F)$ corresponding to f. Notice that π is not of dihedral since $\mathrm{Im}\,\bar{\rho}_{f,2} \simeq A_5$. By using Kim–Shahidi cubic lift [31], there exists a globally generic cuspidal automorphic representation $\mathrm{Sym}^3 \pi$ of $\mathrm{GL}_4(\mathbb{A}_F)$. Since π has the trivial central character, we can lift it back to a globally generic cuspidal automorphic representation Π' of $\mathrm{GSp}_4(\mathbb{A}_F)$. Finally, we apply [24] to switch infinite types of Π'. Then we have a cuspidal automorphic representation Π of $\mathrm{GSp}_4(\mathbb{A}_F)$ such that for each infinite place v of F, Π_v is holomorphic discrete series and its Langlands parameter is given by $\phi_{(w;2,1)}$ for some integer w which can be easily deduce from $\mathrm{Sym}^3(\phi(\pi_v))$ where $\phi(\pi_v)$ is the local Langlands parameter of π_v given by $\phi(\pi_v)(z) = |z|^{-w'} \mathrm{diag}((\frac{z}{\bar{z}})^{\frac{1}{2}}, (\frac{z}{\bar{z}})^{-\frac{1}{2}})$ for $z \in \mathbb{C}$ and for some integer w'. ☐

Theorem 4.8. *Suppose that* $\mathrm{Im}(\bar{\rho})$ *is isomorphic to* F_{20}*. Assume further that for each complex conjugation* c *of* G_F*,* $\bar{\rho}(c)$ *is of type* $(2,2)$*. Then there exists a Hilbert–Siegel cusp form* h *on* $\mathrm{GSp}_4(\mathbb{A}_F)$ *of parallel weight 3 such that* $\bar{\rho} \simeq \bar{\rho}_{h,2}$ *as a representation to* $\mathrm{GL}_4(\overline{\mathbb{F}}_2)$.

Proof. We may assume, there exists an extension $L \supset M \supset F$ such that M/F is a totally real quadratic extension, L/M is a totally imaginary quadratic extension, and L/F is a Galois extension with the Galois group C_4. Then we have

$$\bar{\rho} \simeq \mathrm{Ind}_{G_M}^{G_F} \bar{\tau},\ \ \bar{\tau} = \mathrm{Ind}_{G_L}^{G_M} \bar{\chi}$$

for some character $\bar{\chi} : G_L \to \overline{\mathbb{F}}_2^{\times}$ such that $\mathrm{Im}\,\bar{\tau} \simeq D_{10}$ and $\mathrm{Im}\,\bar{\chi} \simeq C_5$. By assumption, $\bar{\tau}$ is totally odd and it comes from a Hilbert modular Hecke eigen cusp form on $\mathrm{GL}_2(\mathbb{A}_M)$ of parallel weight 1. Further, applying Proposition 4.5, there exists a Hilbert modular cusp form f of $\mathrm{GL}_2(\mathbb{A}_M)$ of parallel weight $(\underline{k}, \underline{w}')$ with

$$\underline{k} = (2 \cdot \mathbf{1}_d, 4 \cdot \mathbf{1}_d) \in \mathbb{Z}^{S_M^{(1)}} \times \mathbb{Z}^{S_M^{(2)}}$$

such that f has the trivial central character and $\bar{\rho}_{f,2} \simeq \bar{\tau}$. Let π be the cuspidal automorphic representation of $\mathrm{GL}_2(\mathbb{A}_M)$ corresponding to f. Applying Theorem 8.6 of [39, p. 251], we have a cuspidal automorphic representation Π of $\mathrm{GSp}_4(\mathbb{A}_F)$ such that for each infinite place v, Π_v is holomorphic discrete series. It follows from Section 2.1 of [18] that for each infinite place v of M, the local Langlands parameter is given by

$$\phi_{\pi_v}(z) = |z|^{-w'_v} \begin{cases} \mathrm{diag}\Big((\frac{z}{\bar{z}})^{\frac{1}{2}}, (\frac{z}{\bar{z}})^{-\frac{1}{2}} \Big) & (v \in S_M^{(1)}) \\ \mathrm{diag}\Big((\frac{z}{\bar{z}})^{\frac{3}{2}}, (\frac{z}{\bar{z}})^{-\frac{3}{2}} \Big) & (v \in S_M^{(2)}). \end{cases}$$

It follows this that the local Langlands parameter of Π_v is $\phi_{(w;2,1)}$ for some $w \in \mathbb{Z}$. Hence we have the claim. $\square$

4.4.2. *Orthogonal automorphy.* Recall that $\mathrm{GSp}_4(\mathbb{F}_2) = \mathrm{Sp}_4(\mathbb{F}_2) = \mathrm{SO}_4(\mathbb{F}_2)$. We discuss mod 2 automorphy of $\bar{\rho}$ when we view it with a representation to $\mathrm{SO}_4(\mathbb{F}_2)$. For background on Galois representations associated to regular algebraic, essentially self-dual, cuspidal automorphic representations of $\mathrm{GL}_n(\mathbb{A}_F)$ for a totally real field F, we refer the reader to [3, Section 1].

Theorem 4.9. *Suppose that* $\mathrm{Im}(\bar{\rho})$ *is isomorphic to* S_5*. Assume further that for each complex conjugation* c *of* G_F*,* $\bar{\rho}(c)$ *is of type* $(2,2)$*. Then there exists a regular orthogonal cuspidal automorphic representation* Π *of* $\mathrm{GL}_4(\mathbb{A}_F)$ *of weight zero such that* $\bar{\rho} \simeq \bar{\rho}_{\Pi,2}$ *as a representation to* $\mathrm{GL}_4(\overline{\mathbb{F}}_2)$.

Proof. By Proposition 3.5, there exist a finite character $\bar{\psi} : G_F \to \mathbb{F}_4^{\times}$ of order dividing 3, a totally real quadratic extension M/F with the Galois group $\mathrm{Gal}(M/F) = \langle \iota \rangle$ and a totally odd irreducible representation $\bar{\tau} : G_M \to \mathrm{SL}_2(\mathbb{F}_4)$ such that $\bar{\rho} \simeq (\mathrm{Ind}_{G_M}^{G_F} \bar{\tau}) \otimes \psi$. By Theorem 2 of [43], $\bar{\tau}$ is modular. Further, applying Proposition 4.5, there exists a Hilbert modular cusp form f of $\mathrm{GL}_2(\mathbb{A}_F)$ of weight $(\underline{k}, \underline{w}')$ with

$$\underline{k} = (2 \cdot \mathbf{1}_d, 3 \cdot \mathbf{1}_d) \in \mathbb{Z}^{S_M^{(1)}} \times \mathbb{Z}^{S_M^{(2)}}$$

such that the central character of f is a power of $|\det|_{\mathbb{A}_M^\times}$ and $\bar{\rho}_{\pi,2} \simeq \bar{\tau} \otimes {}^{\iota}\bar{\tau}$ where $\pi = \pi_f \otimes {}^{\iota}\pi_f$ is the tensor product of π_f and its twists ${}^{\iota}\pi_f$. Notice that the central character of π_f is $\mathrm{Gal}(M/F)$-invariant. Hence, it can be viewed as a cuspidal automorphic representation of $\mathrm{GO}(2,2)(\mathbb{A}_F)$. Further, by Theorem M of [38, p. 54], it can be transfered to a cuspidal automorphic representation Π of $\mathrm{GL}_4(\mathbb{A}_F)$. For each infinite place v of M, the local Langlands parameter is given by

$$\phi_{\pi_v}(z) = |z|^{-w'_v} \begin{cases} \mathrm{diag}\Big(\big(\frac{z}{\bar{z}}\big)^{\frac{1}{2}}, \big(\frac{z}{\bar{z}}\big)^{-\frac{1}{2}}\Big) & (v \in S_M^{(1)}) \\ \mathrm{diag}\Big(\big(\frac{z}{\bar{z}}\big), \big(\frac{z}{\bar{z}}\big)^{-1}\Big) & (v \in S_M^{(2)}). \end{cases}$$

It follows from this that Π is of weight zero. Hence for such a v, the local Langlands parameter of Π_v is given by $\phi_{(w;2,1)} : W_{\mathbb{R}} \to \mathrm{GL}_4(\mathbb{C})$ via $\mathrm{GSp}_4(\mathbb{C}) \subset \mathrm{GL}_4(\mathbb{C})$. □

Remark 4.10. *In the course of the proofs of above theorems, we raised the level by congruence. Therefore, we lose the specification of the levels of Hilbert modular forms appearing there. In conclusion, we can not specify the levels of our Hilbert–Siegel modular forms as well. However, there is some hope and a substantial expectation for further development of the level lowering method. In fact, Conjecture 4.7 and Conjecture 4.9 of* [10] *show that we can take Hilbert modular forms in question to have the correct level regarding Artin conductor of* $\bar{\rho}$.

5. Local mod 2 computations

Let us regard X_ψ as a smooth projective scheme over $\mathrm{Spec}\, \mathcal{O}_K[\frac{1}{5}, \psi, \frac{1}{\psi^5-1}]$. The mirror variety W_ψ of the Dwork quintic X_ψ is defined over $\mathrm{Spec}\, \mathcal{O}_K[\frac{1}{5}, \psi, \frac{1}{\psi^5-1}]$ by the toric construction in Section 5.1 and Lemma 5.4 in Section 5.2. We devote this section to calculating the number of rational points on W_ψ modulo 2 over a finite field.

Let p be a prime number with $p \neq 2, 5$, q be a positive power of p, and $\psi \in \mathbb{F}_q$ such that $\psi^5 \neq 1$. The zeta function of W_ψ over $\mathbb{F}_q$ is given by

$$Z_{W_\psi/\mathbb{F}_q}(t) = \frac{P_{\psi,q}(t)}{(1-t)Q_{\psi,q}(t)Q_{\psi,q}(qt)(1-q^3t)}.$$

with the numerator

$$P_{\psi,q}(t) = 1 - a_{\psi,q}t + b_{\psi,q}t^2 - q^3 a_{\psi,q}t^3 + q^6 t^4 \in \mathbb{Z}[t]$$

and the polynomial $Q_{\psi,q}(t) = 1 + \cdots \pm q^{101}t^{101} \in \mathbb{Z}[t]$ of degree 101 such that the absolute values of all reciprocal roots of $Q_{\psi,q}(t) = 0$ are q by Poincaré duality and the strong Lefschetz formula. Consider the polynomial $f_\psi(x) = 4x^5 - 5\psi x^4 + 1$ with discriminant $2^8 5^5 (1-\psi^5)$.

Proposition 5.1. *Let $n(f_\psi, q)$ be the number of solutions of the equation $f_\psi(x) = 0$ in $\mathbb{F}_q$. Then the congruence below holds:*

$$a_{\psi,q} = 1 - (Q'_{\psi,q}(0) + qQ'_{\psi,q}(0)) + q^3 - \sharp W_\psi(\mathbb{F}_q) \equiv n(f_\psi, q) + 1 \pmod 2.$$

Proposition 5.1 follows from Lemmas 5.3, 5.5 and 5.6 below.

5.1. Toric Calabi-Yau 3-folds. Let us recall a toric construction of W_ψ by Batyrev in [4] but we follow the notation in Section 6 of [46]. Let U_ψ be a smooth affine variety defined by the equation below in $\mathbb{G}_{\mathrm{m}}^4$:

$$U_\psi : x_1 + x_2 + x_3 + x_4 + \frac{1}{x_1x_2x_3x_4} - 5\psi = 0.$$

It follows from $\psi^5 - 1 \neq 0$ that U_ψ is smooth. Let Δ be the convex 4-dimensional reflexive polyhedron with vertices

$$e_1,\ e_2,\ e_3,\ e_4,\ -e_1 - e_2 - e_3 - e_4$$

in $M_{\mathbb{R}} = \mathbb{R}^4$, where e_i is the standard basis of $M_{\mathbb{R}}$. We define an $\mathbb{R}$-linear isomorphism $\eta_j : M_{\mathbb{R}} \to M_{\mathbb{R}}$ $(j = 1, 2, 3, 4)$ by $\eta_j(e_j) = -e_1-e_2-e_3-e_4$ and $\eta_j(e_i) = e_i$ $(i \neq j)$. Then $\eta_j(\Delta) = \Delta$. We also define $\mathbb{P}_\Delta$ by the projective toric variety associated to the polyhedron Δ. The projective toric variety $\mathbb{P}_\Delta$ is a singular Fano variety such that

$$\mathbb{P}_\Delta = \bigcup_{0\le i\le 4} U_i \quad \text{where} \quad U_i \subset \mathbb{A}^5 \text{ is defined by } y_{i,1}y_{i,2}y_{i,3}y_{i,4} = y_{i,0}^5$$

$$\text{with } \begin{cases} y_{0,0} = x_1x_2x_3x_4, y_{0,j} = x_jx_1\cdots x_4 & \text{if } i = 0 \\ y_{i,0} = \frac{1}{x_i}, y_{i,i} = \frac{1}{x_ix_1\cdots x_4}, y_{i,j} = \frac{x_j}{x_i}\ (j \neq 0, i) & \text{if } i \neq 0. \end{cases}$$

Note that η_j's induce an automorphism $\widetilde{\eta}_j$ of $\mathbb{P}_\Delta$ such that $\widetilde{\eta}_j(U_k) = U_l$ for $(k, l) = (0, j), (j, 0)$ or for $k = l \neq 0, j$. $\mathbb{P}_\Delta$ has a stratification $\mathbb{P}_\Delta = \coprod_{\tau\in\Delta} \mathbb{T}_{\Delta,\tau}$ where τ runs through all faces of Δ such that $\mathbb{T}_{\Delta,\tau} \cong \mathbb{G}_{\mathrm{m}}^{\dim\tau}$ since $y_{i,0} = \frac{y_{0,0}}{y_{0,i}}, y_{i,i} = y_{0,i}, y_{i,j} = \frac{y_{0,j}}{y_{0,i}}$ $(j \neq 0, i)$ for $i \neq 0$.

We regard U_ψ as a closed subscheme in $\mathbb{T}_{\Delta,\Delta} = \mathbb{G}_{\mathrm{m}}^4$ with coordinates $x_1^{\pm1}, x_2^{\pm1}, x_3^{\pm1}, x_4^{\pm1}$ and define Y_ψ by the Zariski closure of U_ψ in $\mathbb{P}_\Delta$. The stratification of $\mathbb{P}_\Delta$ induces a stratification

$$Y_\psi = \coprod_{\tau\in\Delta} Y_{\psi,\tau},\ \ Y_{\psi,\tau} = Y_\psi \cap \mathbb{T}_{\Delta,\tau} : z_1 + \cdots + z_{\dim\tau} + 1 = 0 \text{ in } T_{\Delta,\tau} \cong \mathbb{G}_{\mathrm{m}}^{\dim\tau}$$

of Y_ψ by smooth subvarieties $Y_{\psi,\tau}$, i.e., Y_ψ is Δ-regular [4, Definition 3.1.1]. In this situation we obtain a projective smooth mirror symmetry W_ψ of X_ψ as an MPCP-desingularization (maximal projective crepant partial desingularization)

$$\pi_\psi : W_\psi \longrightarrow Y_\psi$$

by [4, Theorem 4.2.2 and Corollary 4.2.3] because of $\dim W_\psi = 3$. In fact, let us take the dual reflexive polyhedron Δ^* which is generated by $5e_i^* - e_1^* - e_2^* - e_3^* - e_4^*$ $(1 \le i \le 4)$

$$5e_i^* - e_1^* - e_2^* - e_3^* - e_4^* \ (1 \le i \le 4), \quad -e_1^* - e_2^* - e_3^* - e_4^*$$

in the dual space $N_{\mathbb{R}}$ of $M_{\mathbb{R}}$ [4, Definition 4.1.1], where $\{e_i^*\}$ is the dual basis of $\{e_i\}$. We choose a triangulation $\mathcal{T}^*$ of Δ^* such that any codimension 1 face of Δ^* have a triangulation into all basic simplices with vertices in $\Delta^* \cap N$. Here $N = \langle e_1^*, e_2^*, e_3^*, e_4^* \rangle \cong \mathbb{Z}^4$ is the standard lattice of $N_{\mathbb{R}}$. Then $\mathcal{T}^*$ is a maximal projective triangulation of Δ^* [4, Definitions 2.2.15, 2.2.18] and [28, Chapter III, Section 2B]. The subdivision $\Sigma(\mathcal{T}^*)$ of the fan $\Sigma(\Delta^*)$ associated to $\mathcal{T}^*$ and Δ^* [4, Proposition 2.1.1], respectively, gives an MPCP-desingularization $\pi : \mathbb{P}_{\Sigma(\mathcal{T}^*)} \to \mathbb{P}_{\Sigma(\Delta^*)}$ and W_ψ is the closure of U_ψ in $\mathbb{P}_{\Sigma(\mathcal{T}^*)}$. Moreover the number of rational points over a finite field does not depend on the choice of crepant resolutions for projective smooth Calabi-Yau varieties [5, Theorem 2.8].

Remark 5.2. *Batyrev and Kreuzer studied the topological fundamental groups and the Brauer groups for toric Calabi-Yau manifolds in* [6]*. Fix an embedding $\overline{\mathbb{Q}} \subset \mathbb{C}$. By their work of integral cohomologies the topological fundamental group $\pi_1^{\mathrm{top}}(W_\psi(\mathbb{C}))$ and the Brauer group $B(W_\psi(\mathbb{C}))$ of the associated complex manifold $W_\psi(\mathbb{C})$ vanish by* [6, Corollaries 1.9, 3.9]*. Hence the singular cohomology $H^i(W_\psi(\mathbb{C}), \mathbb{Z})$ is torsion-free for any i. Therefore, the ℓ-adic etale cohomology $H^i_{\acute{e}t}(W_{\psi,\overline{\mathbb{Q}}}, \mathbb{Z}_\ell)$ is torsion-free for any i and any prime number ℓ by the comparison theorem between singular and etale cohomologies with torsion coefficients.*

5.2. Proof of Proposition 5.1.

Lemma 5.3 ([46, Section 6, (11)])**.** *With the notation as above, we have*

$$\sharp\, Y_\psi(\mathbb{F}_q) = \sharp\, U_\psi(\mathbb{F}_q) - \frac{(q-1)^4 + (-1)^5}{q} + \frac{q^4 - 1}{q - 1}.$$

In particular, $\sharp\, Y_\psi(\mathbb{F}_q) \equiv \sharp\, U_\psi(\mathbb{F}_q) + 1 \pmod 2$*.*

Proof. The following formula is in the proof of [46, Section 6] for the case $n = 4$. It follows

$$\sharp\, Y_{\psi,\tau}(\mathbb{F}_q) = \sum_{i=1}^{\dim \tau} (-1)^{i-1} \binom{\dim \tau}{i-1} q^{\dim \tau - i} = \frac{1}{q}((q-1)^{\dim \tau} + (-1)^{\dim \tau + 1})$$

by the equation of $Y_{\psi,\tau}$ in Section 5.1 if $1 \le \dim\tau < 4$ and $Y_{\psi,\tau} = \emptyset$ if $\dim\tau = 0$. Thus, we have

$$\begin{aligned}
&\sharp\, Y_\psi(\mathbb{F}_q)\\
&= \sharp\, U_\psi(\mathbb{F}_q) - \frac{(q-1)^4 + (-1)^5}{q} + \sum_{\tau\in\Delta} \frac{1}{q}((q-1)^{\dim\tau} + (-1)^{\dim\tau+1})\\
&= \sharp\, U_\psi(\mathbb{F}_q) - \frac{(q-1)^4 + (-1)^5}{q} + \frac{q^4-1}{q-1}. \qquad \square
\end{aligned}$$

Lemma 5.4. *There exists a triangulation $\mathcal{T}^*$ of Δ^* such that all basic simplices consist of vertices in $\Delta^* \cap N$ and the cyclic group C_4 of order 4 acts on $\mathcal{T}^*$ by $\sigma(e_i^*) = e^*_{\sigma^{-1}(i)}$ for $i \in \mathbb{Z}/4\mathbb{Z}$ and $\sigma \in C_4$.*

Proof. Let Δ_0^* (resp. Δ_j^* $(j = 1,2,3,4)$) be a 3-dimensional face of Δ^* generated by $5e_i^* - e_1^* - e_2^* - e_3^* - e_4^*$ $(1 \le i \le 4)$ (resp. $-e_1^* - e_2^* - e_3^* - e_4^*, 5e_i^* - e_1^* - e_2^* - e_3^* - e_4^*$ $(i \in \{1,2,3,4\} \setminus \{j\})$. It is sufficient to construct a triangulation $\mathcal{T}_0^*$ of the face Δ_0^* of Δ^* such that $\mathcal{T}_0^*$ consists of basic simplices with vertexes in $\Delta_0^* \cap N$, the cyclic group C_4 of order 4 acts on $\mathcal{T}_0^*$ as in the statement, and 2-dimensional faces consists of basic simplices all of which are congruent triangles. Indeed, if $\eta_j^* : N_\mathbb{R} \to N_\mathbb{R}$ is a dual linear map of η_j, then $\mathcal{T}_j^* = \eta_j^*(\mathcal{T}_0^*)$ is a triangulation of the face Δ_j^* of Δ^* which consists of basic simplices with vertexes in $\Delta_j^* \cap N$. Moreover, since $\eta_j^*|_{\Delta_0^*\cap\Delta_j^*} = \mathrm{id}_{\Delta_0^*\cap\Delta_j^*}$, $(\eta_j^*)^2 = \mathrm{id}_{N_\mathbb{R}}$ and the triangulation of 2-dimensional faces are unique by our hypothesis, $\mathcal{T}^* = \cup_{0\le j\le 4}\mathcal{T}_j^*$ forms a triangulation $\mathcal{T}^*$ of Δ^* such that all basic simplices consist of vertices in $\Delta^* \cap N$. Moreover, the induced liner map $\sigma^* : N_\mathbb{R} \to N_\mathbb{R}$ from $\sigma \in (1,2,3,4) \in C_4$ is given by $\sigma^* = \eta_1^* \circ \eta_4^* \circ \eta_3^* \circ \eta_2^* \circ \eta_1^*$ so that the cyclic group C_4 acts on $\mathcal{T}^*$ by the restriction.

Let us explain how to construct a triangulation $\mathcal{T}_0^*$ of Δ_0^*. The volume of the 3-dimensional face Δ_0^* is 125. Note that the volume of the 3-dimensional simplex generated by $e_1^*, \cdots, e_4^*$ is $\frac{1}{3}$. Let $y_1, \cdots, y_4$ be a system of standard coordinates of $N_\mathbb{R}$. Consider the 16 partitions of $N_\mathbb{R}$ by 4 hyperplanes defined by $y_1 = 0, y_2 = 0, y_3 = 0$ and $y_4 = 0$ including boundaries, and denotes each of them by $(\pm,\pm,\pm,\pm)$.

(I) Case $(+,+,+,+)$. In this case there exists a unique 3-dimensional basic simplex generated by $(1,0,0,0), (0,1,0,0), (0,0,1,0), (0,0,0,1)$ on $\Delta_0^* \cap (+,+,+,+)$.

(II) Case $(-,+,+,+)$. The volume of $\Delta_0^* \cap (-,+,+,+)$ is 7. Consider the subdivision of the partition by $\alpha_j \le y_j \le \alpha_j + 1$ $(j = 2,3,4)$ for $\alpha_j = 0, 1$.

(II-i). If $\alpha_2 = \alpha_3 = \alpha_4 = 0$, then 6 points

$$(-1,1,1,0), (-1,1,0,1), (-1,0,1,1), (0,1,0,0), (0,0,1,0), (0,0,0,1)$$

belong $\Delta_0^* \cap N$. Let us connects 2 points of 6 points by an edge if either (a) $y_i = 1$ for some $2 \le i \le 4$, (b) $y_1 = 0$ or (c) two points are $(-1, 1, 0, 1)$ and $(0, 0, 1, 0)$. Here the edge between $(-1, 1, 0, 1)$ and $(0, 0, 1, 0)$ is drawn by our choice. Then there exists 4 pieces of 3-dimensional basic simplices.

(II-ii). If $\alpha_2 = 1$ and $\alpha_3 = \alpha_4 = 0$, then there exists a unique 3-dimensional basic simplex generated by $(-1, 2, 0, 0), (-1, 1, 1, 0), (-1, 1, 0, 1), (0, 1, 0, 0)$ on Δ_0^*.

(II-iii). Otherwise, the intersection with Δ_0^* is of dimension less than 3 and they are union of faces of 3-dimensional simplices obtained in (II-i), (II-ii) and (II-iii).

Hence we obtain $4 + 1 \times 3 = 7$ basic simplices. By the action of C_4 we have 28 basic simplices on Δ_0^* in $(-,+,+,+) \cup (+,-,+,+) \cup (+,+,-,+) \cup (+,+,+,-)$.

(III) Case $(-,-,+,+)$. The volume of $\Delta_0^* \cap (-,-,-,+)$ is 12 such that $\Delta_0^* \cap N \cap (-,-,+,+)$ consists of 12 points.

(III-i). If $0 \le y_3, y_4 \le 1$, then there exists a unique 3-dimensional basic simplex generated by $(-1, 0, 1, 1), (0, -1, 1, 1), (0, 0, 1, 0), (0, 0, 0, 1)$ on Δ_0^*.

(III-ii). If $0 \le y_3 \le 1$ and $1 \le y_4 \le 2$, then 6 points

$$(-1, -1, 1, 2), (-1, 0, 0, 2), (0, -1, 0, 2), (-1, 0, 1, 1), (0, -1, 1, 1), (0, 0, 0, 1)$$

belong $\Delta_0^* \cap N$. Connects two of points for either y_1, y_2, y_3 or y_4 coincides with each other by edges. We also connect points $(-1, -1, 1, 2)$ and $(0, 0, 0, 1)$ by an edge. Then the area is divided by 4 pieces of 3-dimensional basic simplices. Note that the edge between $(-1, -1, 1, 2)$ and $(0, 0, 0, 1)$ is our choice. We also have a similar division if $1 \le y_3 \le 2$ and $0 \le y_4 \le 1$ by permutation y_3 and y_4.

(III-iii). If $0 \le y_3 \le 1$ and $2 \le y_4 \le 3$, then there exists a unique 3-dimensional basic simplex generated by $(-1, -1, 0, 3)$, $(-1, -1, 1, 2)$, $(-1, 0, 0, 2)$, $(0, -1, 0, 2)$ on Δ_0^*.

(III-iv). If $1 \le y_3, y_4 \le 2$, then there exists a unique 3-dimensional basic simplex generated by $(-1, -1, 1, 2), (-1, -1, 2, 1), (-1, 0, 1, 1), (0, -1, 1, 1)$ on Δ_0^*.

(III-v). Otherwise, the intersection with Δ_0^* is of dimension less than 3 and they are union of faces of 3-dimensional simplices obtained in (III-i), (III-ii), (III-iii), and (III-iv).

Hence we obtain $1 + 1 \times 2 + 4 \times 2 + 1 \times 2 + 1 = 12$ basic simplices. By the action of S_4 we have 24 basic simplices on Δ_0^* in $(-,-,+,+) \cup (-,+,-,+) \cup (-,+,+,-) \cup (+,-,-,+) \cup (+,-,+,-) \cup (+,+,-,-)$.

(IV) Case $(-,-,-,+)$. The volume of $\Delta_0^* \cap (-,-,-,+)$ is 2 such that $\Delta_0^* \cap N \cap (-,-,-,+)$ consists of 8 points

$$(-1,-1,-1,4),(-1,-1,0,3),(-1,0,-1,3),(0,-1,-1,3),$$
$$(-1,0,0,2),(0,-1,0,2),(0,0,-1,2),(0,0,0,1).$$

(IV-i). If $1 \leq y_4 \leq 2$, then there exists a unique 3-dimensional basic simplex generated by $(-1,0,0,2),(0,-1,0,2),(0,0,-1,2),(0,0,0,1)$ on Δ_0^*.

(IV-ii). If $2 \leq y_4 \leq 3$, then the situation is similar to the case (II-i). Here we connect two points $(-1,0,-1,3),(0,-1,0,2)$ as our choice. Then there exists 4 pieces of 3-dimensional basic simplices.

(IV-iii). If $3 \leq y_4 \leq 4$, then there exists a unique 3-dimensional basic simplex generated by $(-1,-1,-1,4),(-1,-1,0,3),(-1,0,-1,3),(0,-1,-1,3)$ on Δ_0^*.

(IV-iv). Otherwise, the intersection with Δ_0^* is of dimension less than 3 and they are union of faces of 3-dimensional simplices obtained in (IV-i), (IV-ii) and (IV-iii).

Hence we obtain $1+4+1=6$ basic simplices. By the action of C_4 we have 24 basic simplices on Δ_0^* in $(-,-,-,+)\cup(-,-,+,-)\cup(-,+,-,-)\cup(+,-,-,-)$.

(V) Case $(-,-,-,-)$. This case never happens.

Now we have obtained

$$1+28+72+24=125$$

basic simplices on Δ_0^* such that all basic simplices in 2-dimensional faces of Δ_0^* are equilateral triangles which are not triangles in (II-i), (III-ii) and (IV-ii). By our construction the 3-dimensional basic simplices above and induced faces from them form a desired triangulation $\mathcal{T}_0^*$ of Δ_0^* on which the cyclic group C_4 naturally acts. This completes a proof. ☐

Lemma 5.5. *With the notation as above, the congruence* $\sharp W_\psi(\mathbb{F}_q) \equiv \sharp Y_\psi(\mathbb{F}_q) \pmod 2$ *holds.*

Proof. Let us now fix a triangulation $\mathcal{T}^*$ of Δ^* as in Lemma 5.4. Note that the number of $\mathbb{F}_q$-rational points of W_ψ is independent of the choices of triangulations (see the paragraph before Remark 5.2). If Y_ψ^{reg} (resp. Y_ψ^{sing}) denotes the regular (resp. singular) locus of Y_ψ, then π_ψ induces an isomorphism $\pi_\psi^{-1}(Y_\psi^{\mathrm{reg}}) \cong Y_\psi^{\mathrm{reg}}$ and $Y_\psi^{\mathrm{reg}} = \coprod_{\dim \tau \geq 3} Y_{\psi,\tau}$. Then the cyclic group C_4 of order 4 acts on the toric structure of Y_ψ by permutation of coordinates and it acts compatibly on the triangulation $\mathcal{T}^*$ of Δ^*. Let us observe the cardinal of the C_4-orbits of rational points of W_ψ. Each single orbit is lying over the inverse image $\pi_\psi^{-1}(Y_\psi^{\mathrm{reg}})$ of the smooth locus. Therefore, on $\pi_\psi^{-1}(Y_\psi^{\mathrm{sing}})$, the cardinal of each C_4-orbit is either 2 or 4 so that

$$\begin{aligned}\sharp\, W_\psi(\mathbb{F}_q) &\equiv \sharp\, Y_\psi^{\mathrm{reg}}(\mathbb{F}_q) + \sharp\, \pi_\psi^{-1}(Y_\psi^{\mathrm{sing}})(\mathbb{F}_q)\\ &\equiv \sharp\, Y_\psi^{\mathrm{reg}}(\mathbb{F}_q) \equiv \sharp\, Y_\psi(\mathbb{F}_q) - \sharp\, Y_\psi^{\mathrm{sing}}(\mathbb{F}_q) \pmod 2.\end{aligned}$$

The proof completes after the congruence

$$\sharp\, Y_\psi^{\mathrm{sing}}(\mathbb{F}_q) = \sum_{\dim \tau \le 2} \sharp\, Y_{\psi,\tau}(\mathbb{F}_q) = 10(q-1) + 10 = 10q \equiv 0 \pmod 2. \quad \square$$

Lemma 5.6. $\sharp\, U_\psi(\mathbb{F}_q) \equiv n(f_\psi, q) \pmod 2$.

Proof. We may use the natural C_4-action on U_ψ inducing by permutation of coordinates. □

Remark 5.7. *One can prove the congruence* $a_{\psi,q} \equiv n(f_\psi, q) + 1 \pmod 2$ *in Proposition 5.1 using the formula of zeta function of* X_ψ *for* $\psi^5 \neq 0, 1$, *which was conjectured in* [13] *and proved in* [25]*:*

$$Z_{X_\psi/\mathbb{F}_q}(t) = \frac{P_{\psi,q}(t) P_{A_\psi/\mathbb{F}_q}(qt)^{10} P_{B_\psi/\mathbb{F}_q}(qt)^{15}}{(1-t)(1-qt)(1-q^2t)(1-q^3t)}$$

where A_ψ *and* B_ψ *are projective smooth models of the affine curves defined by*

$$y^5 = x^2(1-x)^3(x-\psi^5)^2 \quad \text{and} \quad y^5 = x^2(1-x)^4(x-\psi^5),$$

respectively. Indeed, one has $\sharp\, X_\psi(\mathbb{F}_q) \equiv n(f_\psi, q) + 1 \pmod 2$ *by a direct computation, and* $P_{B_\psi/\mathbb{F}_q}(t)$ *is a square of polynomial of degree* 4 *if* $5 \mid q-1$ *since* B_ψ *is furnished with an involution defined by*

$$(x, y) \longmapsto \left(\frac{\psi^5}{x}, \frac{\psi^3(1-x)(x-\psi^5)}{xy}\right)$$

and $P_{B_\psi/\mathbb{F}_q}(t)$ *is a product of L-functions of character sums*

$$x \longmapsto \chi_r^i\left(x^2(1-x)^4(x-\psi^5)\right)$$

on $\mathbb{P}^1 \setminus \{0, 1, \infty, \psi^5\}$ *for* $1 \le i \le 4$ *where* $\chi : \mathbb{F}_q^\times \to \mathbb{C}^\times$ *is a primitive multiplicative character of order* 5 *and* $\chi_r^i = \chi^i \circ N_{\mathbb{F}_{q^r}/\mathbb{F}_q}$. *The similar result also holds for* $\psi = 0$.

6. Global monodromy

Let K be a number field, and $\psi \in K$ such that $\psi^5 \neq 1$. We denote by L_ψ the fixed field of the kernel $\mathrm{Ker}(\bar\rho_{\psi,2})$ of the mod 2 representation

$$\bar\rho_{\psi,2} : G_K \longrightarrow \mathrm{GSp}(\overline{T}_{\psi,2}, \langle\,\cdot\,,\cdot\,\rangle_{\mathbb{F}_2}),$$

where $T_{\psi,2}$ is a lattice of $V_{\psi,2} = H^3_{\text{ét}}(W_{\psi,\overline{\mathbb{Q}}}, \mathbb{Q}_2)$ and $\overline{T}_{\psi,2} = T_{\psi,2} \otimes_{\mathbb{Z}_2} \mathbb{F}_2$. Let us fix an isomorphism $\mathrm{GSp}(\overline{T}_{\psi,2}, \langle\,\cdot\,,\cdot\,\rangle_{\mathbb{F}_2}) \cong S_6$. In this section we prove Theorem 1.1 (1), that is, to determine the global monodromy group $\mathrm{Im}(\bar{\rho}_{\psi,2})$.

6.1. Euler factors and global monodromy modulo 2. At first we fix notation. Let v be a finite place with $v \nmid 10$ such that W_ψ has a good reduction at v, that is, $\psi^5 - 1$ is a v-adic unit. Let us define the local Euler factor

$$P_{\psi,v}(t) = 1 - a_{\psi,v}t + b_{\psi,v}t^2 - q_v^3 a_{\psi,v}t^3 + q_v^6 t^4 \in \mathbb{Z}[t]$$

of $V_{\psi,2}$ at v, where $\mathbb{F}_v$ is the residue field of K at v and q_v is the cardinal of $\mathbb{F}_v$. We denote the mod 2 Galois representation

$$\bar{\rho}_{\psi,v,2} : \mathrm{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v) \longrightarrow \mathrm{GSp}(\overline{T}_{\psi,2}, \langle\,\cdot\,,\cdot\,\rangle_{\mathbb{F}_2}).$$

for a finite place v with good reduction via $G_K \supset D_{K,v} \to \mathrm{Gal}(\overline{\mathbb{F}}_v/\mathbb{F}_v)$. Here $D_{K,v}$ is the decomposition group at the place v. We also denote the geometric Frobenius at v by Frob_v and then

$$P_{\psi,v}(t) = \det(1 - t\rho_{\psi,\ell}(\mathrm{Frob}_v); V_{\psi,\ell})$$

for a prime number ℓ with $v \nmid \ell$.

Our initial idea to determine the monodromy group $\mathrm{Im}(\bar{\rho}_{\psi,2})$ came from an observation of the numerical table in [13], and we expect the following property which will be proved in Theorem 6.10.

Property 6.1 (Theorem 6.10)**.** *If $a_{\psi,v}$ is even, then so is $b_{\psi,v}$. In particular, the possible characteristic polynomial $P_{\psi,v}(t)$ modulo 2 is one of the following:*

$$1 + t^4,\ 1 + t + t^3 + t^4,\ 1 + t + t^2 + t^3 + t^4.$$

An immediate observation shows the following:

Proposition 6.2. *Assume that Property 6.1 holds for ψ. Any conjugate of* $(123)(456)$ *in* $S_6 \cong \mathrm{GSp}(\overline{T}_{\psi,2}, \langle\,\cdot\,,\cdot\,\rangle_{\mathbb{F}_2})$ *does not appear in the image of $\bar{\rho}_{2,v}$. In particular, the image* $\mathrm{Im}(\bar{\rho}_{\psi,2})$ *is isomorphic to a subgroup of S_5 or $S_4 \times S_2$.*

Proof. Let L_ψ be the fixed field of the kernel $\mathrm{Ker}(\bar{\rho}_{\psi,2})$ in $\overline{\mathbb{Q}}$. Let us regard $\mathrm{Im}(\bar{\rho}_{\psi,2})$ as a subgroup of S_6. Then the characteristic polynomial of the conjugate of $\sigma = (123)(456) \in S_6$ is $1 + t^2 + t^4$. Suppose that $\mathrm{Im}(\bar{\rho}_{\psi,2})$ contains an element conjugated to $\sigma = (123)(456)$. Then there exist infinitely many finite places v of K which are unramified such that, for such a v the characteristic polynomial $P_{\psi,v}(t)$ of the geometric Frobenius Frob_v at v is $1 + t^2 + t^4$ modulo 2 by Chebotarev's density theorem. It contradicts the assertion of Property 6.2. Hence, any conjugate of $\sigma = (123)(456)$ is not contained in $\mathrm{Im}(\bar{\rho}_{\psi,2})$. Moreover, it means the order of $\mathrm{Im}(\bar{\rho}_{\psi,2})$ divides 240. Then the assertion follows from the classification of subgroups of S_6. ☐

Henceforth, we will try to relate reciprocity of the quintic trinomial f_ψ with the global monodromy $\mathrm{Im}(\bar{\rho}_{\psi,2})$. As a byproduct, we will confirm Property 6.1 in Theorem 6.10.

6.2. Local to global. Let $f_\psi(x) = 4x^5 - 5\psi x^4 + 1$ be a polynomial over K, and K_{f_ψ} be the decomposition field of f_ψ over K.

Proposition 6.3. *The degree of the extension $K_{f_\psi} L_\psi$ over L_ψ is a power of* 2.

Proof. Let M be a subextension of $K_{f_\psi} L_\psi / L_\psi$, and v a finite place of M such that $\psi^5 - 1$ is a unit at v. Then the characteristic polynomial $P_{\psi,v}(t)$ of the geometric Frobenius Frob_v is $1 + t^4$ modulo 2 since $L_\psi \subset M$ and thus $\bar{\rho}_{\psi,v,2}(\mathrm{Frob}_v)$ is trivial. Hence the equation $f_\psi = 0$ admits an odd number of solutions at each finite place of M as above by Proposition 5.1. Hence the equation $f_\psi = 0$ has an odd number of solutions in M by Chebotarev's density theorem. Since $K_{f_\psi} L_\psi = (L_\psi)_{f_\psi}$, $\deg(K_{f_\psi} L_\psi / L_\psi)$ is a power of 2. ☐

Proposition 6.4. *The degree of the extension $K_{f_\psi} L_\psi$ over K_{f_ψ} is a number of the form $2^i 3^j$ for some non-negative integers i, j.*

Proof. For any place v of K_{f_ψ} such that $\psi^5 - 1$ is a unit at v, the characteristic polynomial $P_{\psi,v}(t)$ of the geometric Frobenius Frob_v is either $1 + t^2 + t^4$ or $1 + t^4$ modulo 2 by Proposition 5.1 since $n(f_\psi, q_v) = 5$. Hence its order is $2^i \times 3^j$ for some $i, j \geq 0$. Since the order of extension of the residue fields at almost all places in the extension $K_{f_\psi} L_\psi / K_{f_\psi}$ is $2^i \times 3^j$ for some integers $i, j \geq 0$, the degree of the extension $K_{f_\psi} L_\psi / K_{f_\psi}$ is a multiple of a power of 2 and a power of 3 by Chebotarev's density theorem. ☐

For any finite extension L/M of fields, let us write its degree for $\deg(L/M) = [L : M]$.

Corollary 6.5. *It holds that*

(1) $\deg(L_\psi/K)$ *is divided by* 5 *if and only if so is* $\deg(K_{f_\psi}/K)$*;*
(2) *If* $\deg(K_{f_\psi}/K)$ *is divided by* 3*, then so is* $\deg(L_\psi/K)$*.*

Proof. The assertion follows from Propositions 6.3 and 6.4 and the equality

$$\begin{aligned}\deg(K_{f_\psi} L_\psi / K_{f_\psi}) \deg(K_{f_\psi}/K) &= \deg(K_{f_\psi} L_\psi / K) \\ &= \deg(K_{f_\psi} L_\psi / L_\psi) \deg(L_\psi / K).\end{aligned}$$ ☐

6.3. Non-fullness.

Theorem 6.6. *Under the natural inclusion, we have* $\mathrm{Im}(\bar{\rho}_{\psi,2}) \neq S_6, A_6$.

Proof. Suppose $\mathrm{Im}(\bar{\rho}_{\psi,2})$ is isomorphic to either S_6 or A_6. Consider the natural morphism

$$\nu : \mathrm{Gal}(K_{f_\psi} L_\psi / K_{f_\psi}) \longrightarrow \mathrm{Gal}(L_\psi / K)$$

by restriction. Then ν is injective and $\mathrm{Im}(\nu)$ is a normal subgroup of $\mathrm{Gal}(L_\psi/K)$ by Galois theory. Since the order of $\mathrm{Im}(\nu)$ is a multiple of a power of 2 and a power of 3 by Proposition 6.4, $\mathrm{Im}(\nu)$ is trivial by Lemma 6.7 below. Hence $L_\psi \subset K_{f_\psi}$. Since $\mathrm{Gal}(K_{f_\psi}/K)$ is a subgroup of S_5, one has $\mathrm{Im}(\bar{\rho}_{\psi,2}) \not\cong S_6, A_6$. $\square$

Lemma 6.7. *Let H be a subgroup of S_6 such that the order of H is divided by* 5*. Then any normal subgroup of H whose order is not divided by* 5 *is trivial.*

Proof. It follows from Section 3.2 that H is isomorphic to one of $C_5, D_{10} = C_4 \ltimes C_5, F_{20} = C_4 \ltimes C_5, A_5, S_5, A_6$ and S_6. Then the conclusion is a well-known fact. $\square$

6.4. Irreducible case. We determine the mod 2 monodromy group when f_ψ is irreducible.

Theorem 6.8. *If f_ψ is irreducible over K, then $L_\psi = K_{f_\psi}$, that is,*

$$\mathrm{Im}(\bar{\rho}_{\psi,2}) \cong \mathrm{Gal}(K_{f_\psi}/K).$$

Lemma 6.9. *Suppose that f_ψ is irreducible over K. Then K_{f_ψ} is a subfield of L_ψ.*

Proof. Since f_ψ is irreducible, $\mathrm{Gal}(K_{f_\psi}/K)$ is a subgroup of S_5 whose order is divided by 5. Consider the surjection

$$\theta : \mathrm{Gal}(K_{f_\psi} L_\psi / K) \longrightarrow \mathrm{Gal}(K_{f_\psi}/K).$$

Then the image $\theta(\mathrm{Gal}(K_{f_\psi} L_\psi / L_\psi))$ is a normal subgroup of $\mathrm{Gal}(K_{f_\psi}/K)$ of order a power of 2 by Proposition 6.3. $\theta(\mathrm{Gal}(K_{f_\psi} L_\psi / L_\psi))$ is trivial by Lemma 6.7 so that $\mathrm{Gal}(K_{f_\psi} L_\psi / L_\psi)$ is trivial. It concludes $K_{f_\psi} \subset L_\psi$. $\square$

Proof of Theorem 6.8. Consider the canonical surjection $\theta : \mathrm{Gal}(L_\psi/K) \to \mathrm{Gal}(K_{f_\psi}/K)$ by Lemma 6.9. The order of the kernel θ is a multiple of a power of 2 and a power of 3 by Proposition 6.4. Since our hypothesis of the irreducibility of f_ψ implies that $\deg(K_{f_\psi}/K)$ is divided by 5, the kernel θ must be trivial by Lemma 6.7. $\square$

6.5. Disappearance of $1+t^2+t^4$.

We confirm Property 6.1.

Theorem 6.10. *If $a_{\psi,q}$ is even, then so is $b_{\psi,q}$.*

Proof. First we prove the assertion when f_ψ is irreducible. Suppose $a_{\psi,v}$ is even and $b_{\psi,v}$ is odd. Then the order of the image $\bar{\rho}_{\psi,2}(\mathrm{Frob}_v)$ of geometric Frobenius is either 3 or 6. Since $\mathrm{Gal}(K_{f_\psi}/K) \cong \mathrm{Im}(\bar{\rho}_{\psi,2})$ by Theorem 6.8, the type of polynomial f_ψ has a factor of degree 3 over $\mathbb{F}_v$. It contradicts the congruence $a_{\psi,v} \equiv n(f_\psi, v)+1 \pmod 2$ in Proposition 5.1 since $n(f_\psi, q_v) = 0$ or 2.

In general there exists an element $\psi' \in K$ such that $\psi' \equiv \psi \pmod v$ and $f_{\psi'}$ is irreducible over K by the weak approximation theorem and Eisenstein's criterion of irreducibility for a place w of K above 5. Since $P_{\psi,v}(t) = P_{\psi'.v}(t)$, the assertion follows from that of the irreducible case. □

7. Rational points on some Diophantine equations

In this section, we will prove the following with an elementary method without using Coleman–Chabauty:

Theorem 7.1. *For each $\psi \in \mathbb{Q} \setminus \{0,1\}$ such that $f_\psi(x) = 4x^5 - 5\psi x^4 + 1$ is irreducible over $\mathbb{Q}$, it holds that $\mathrm{Gal}(\mathbb{Q}_{f_\psi}/\mathbb{Q}) \simeq S_5$.*

It follows from Theorem 7.2 and Theorem 7.3. To exclude the possible types of $\mathrm{Im}(\bar{\rho}_{\psi,2})$ other than S_5 we relate it with rational points on some Diophantine equations.

7.1. On D_{10} and F_{20}.

Let $\bar{\rho} = \bar{\rho}_{\psi,2} : G_\mathbb{Q} \to \mathrm{GSp}_4(\mathbb{F}_2)$ be the mod 2 Galois representation associated to W_ψ with $\psi \in \mathbb{Q} \setminus \{0,1\}$. Assume that f_ψ is irreducible over $\mathbb{Q}$ and this condition yields $\mathrm{Gal}(\mathbb{Q}_{f_\psi}/\mathbb{Q}) \not\simeq C_5$, since f_ψ has complex roots which are not real. By Theorem 1.1, $\mathrm{Im}(\bar{\rho}) \simeq \mathrm{Gal}(\mathbb{Q}_{f_\psi}/\mathbb{Q}) \subset S_5$. Assume further that for the complex conjugation c of $G_\mathbb{Q}$, $\bar{\rho}(c)$ is of type $(2,2)$ as an element of S_5. This is equivalent to $\psi < 1$. As is proved later that the discriminant of f_ψ is non-square in $\mathbb{Q}^\times$. In particular, this excludes the cases of D_{10} and A_5 among possible types of $\mathrm{Im}(\bar{\rho})$. However, below, we also treat D_{10} for the consistency of the method.

Let us first observe the cases of D_{10} and F_{20}. Put $g_\psi(x) := x^5 f_\psi(x^{-1}) = x^5 - 5\psi x + 4$. Suppose that g_ψ is of type D_{10}. As explained in [42, second paragraph in p. 138], due to Weber and Chebotarev, there exist two rational functions $f_1(\lambda,\mu)$, $f_2(\lambda,\mu)$ in two variables λ, μ with $\lambda \neq 1$ and $\mu \neq 0$ such that

$$f_1(\lambda,\mu) := \frac{5^5\lambda\mu^4}{(\lambda-1)^4(\lambda^2-6\lambda+25)} = -5\psi,$$

$$f_2(\lambda,\mu) := \frac{5^5\lambda\mu^5}{(\lambda-1)^4(\lambda^2-6\lambda+25)} = 4.$$

Regarding the second equation $f_2(\lambda, \mu) = 4$, let us substitute the variables suitably we have the following affine equation

$$\begin{aligned} &Y^2 = X^{10} + 11X^5 - 1, \\ &(X, Y) = \left(\frac{-8(-3+\lambda)(-1+\lambda)^5 + 5^5(-1+2\lambda)\mu^5}{2^5(\lambda-1)^5}, \frac{5\mu}{2(-1+\lambda)} \right). \end{aligned}$$

Next we consider the case of F_{20}. Assume that $\mathrm{Gal}(\mathbb{Q}_{f_\psi}/\mathbb{Q}) \simeq F_{20}$. Applying Theorem 1 of [19] to g_ψ, we have the equation

$$\begin{aligned} 0 = x^6 - 40x^5\psi + 1000x^4\psi^2 - 20000x^3\psi^3 + 250000x^2\psi^4 \\ + 4000000\psi(3+\psi^5) - 800000x(1+2\psi^5). \end{aligned}$$

Notice that $x = 10\psi$ implies $\psi = 0$ in which case we have $\mathrm{Gal}(\mathbb{Q}_{f_\psi}/\mathbb{Q}) \simeq F_{20}$. Therefore, we may assume that $\psi \neq 0$ and hence $x \neq 10\psi$. Substituting variables we have

$$\begin{aligned} Y^2 = X^{10} + 11X^5 - 1, \quad X = \frac{10}{x - 10\psi}, \\ Y = \frac{x\{800000 - (x-10\psi)^5\} - 10000000\psi}{20(x-10\psi)^5\psi} \end{aligned}$$

again.

Let C be a unique smooth completion of the affine hyperelliptic curve $W: Y^2 = X^{10}+11X^5-1$ and J be its Jacobian. Clearly, $C(\mathbb{Q}) = W(\mathbb{Q}) \cup \{\infty_\pm\}$. For each positive integer n, let $J[n]$ be the group scheme consisting of n-torsion points.

Theorem 7.2. *It holds that $C(\mathbb{Q}) = \{\infty_\pm\}$. In particular, $W(\mathbb{Q}) = \emptyset$.*

Proof. Put $F = \mathbb{Q}(\zeta_5)$. Notice that 11 is split completely in F and for each finite place w lying over 11, D has good reduction at w. Pick such a place w. Notice that $\mathbb{F}_w \simeq \mathbb{F}_{11}$ and we fix this isomorphism. Since C is of genus greater than 1, we have an injection

$$r_{\infty_+} : C(\overline{\mathbb{Q}}) \hookrightarrow J(\overline{\mathbb{Q}}), \quad Q \longmapsto Q - \infty_+$$

which is defined over $\mathbb{Q}$. By using Magma [8], we see that $J(\mathbb{Q})$ is of Mordell–Weil rank 0. Hence $J(\mathbb{Q}) = J(\mathbb{Q})_{\mathrm{tor}}$ where the subscript "tor" means the maximal torsion subgroup of $J(\mathbb{Q})$. Put $T =: \{(x,0) \in W(\overline{\mathbb{Q}})\} \cup \{\infty_\pm\}$. Then $T \subset C(F)$ since

$$X^{10} + 11X^5 - 1 = \prod_{i=0}^{4}(X - \zeta_5^i\varepsilon_+)(X - \zeta_5^i\varepsilon_-), \quad \varepsilon_\pm = \frac{-1 \pm \sqrt{5}}{2}.$$

Clearly, $|T| = 12$. Further, it is easy to see that $r_{\infty_+}(T) \subset J[2](F) \subset J(F)_{\mathrm{tor}}$. The composition $C(\mathbb{Q}) \xrightarrow{r_{\infty_+}} J(\mathbb{Q}) = J(\mathbb{Q})_{\mathrm{tor}} \subset J(F)_{\mathrm{tor}}$ is injective, since $J(\mathbb{Q}) = J(\mathbb{Q})_{\mathrm{tor}}$ as mentioned before. It yields a natural commutative diagram:

$$\begin{tikzcd}
 & T \arrow[r, "r_{\infty_+}"] \arrow[d, "\cap"'] & J(F)_{\mathrm{tor}} \arrow[d, "\cap"] \\
C(\mathbb{Q}) \arrow[r, "\subset"'] \arrow[d] \arrow[urr, bend left, "r_{\infty_+}"] & C(F) \arrow[r, "r_{\infty_+}"] \arrow[d] & J(F) \arrow[d] \\
\widetilde{C}(\mathbb{F}_{11}) \arrow[r, "="'] & \widetilde{C}(\mathbb{F}_w) \arrow[r, "r_{\infty_+}"] & \widetilde{J}(\mathbb{F}_w)
\end{tikzcd}$$

where the vertical arrows to the bottom line stands for the reduction maps to good reductions $\widetilde{C}$ and $\widetilde{J}$ respectively. Notice that $J(F)_{\mathrm{tor}}$ can be extended to a finite etale group scheme in the Neron model of J over $\mathcal{O}_F$. Therefore, the composition $J(F)_{\mathrm{tor}} \to \widetilde{J}(\mathbb{F}_w) = \widetilde{J}(\mathbb{F}_{11})$ of the most right vertical arrows is injective since the $F_w = \mathbb{Q}_{11}$ is trivially unramified over $\mathbb{Q}_{11}$ (this can be also checked by observing $11 \nmid |J(\mathbb{F}_v)|$ for another finite place v not lying over 11 of F such that J has good reduction at v). It follows from this that the reduction maps $C(\mathbb{Q}) \to \widetilde{C}(\mathbb{F}_{11})$ and $T \to \widetilde{C}(\mathbb{F}_w) = \widetilde{C}(\mathbb{F}_{11})$ are injective. By computation, $|\widetilde{C}(\mathbb{F}_{11})| = 12$. Hence $T \xrightarrow{\sim} \widetilde{C}(\mathbb{F}_w) = \widetilde{C}(\mathbb{F}_{11})$. Thus, the natural inclusion $C(\mathbb{Q}) \subset C(F)$ factors through T. Hence, $C(\mathbb{Q}) = C(\mathbb{Q}) \cap T = \{\infty_\pm\}$ as desired. $\square$

7.2. On A_5 and D_{10}. Next we consider the case of A_5 or D_{10} though the latter case is done already. This case can be excluded by observing the discriminant as below. Let $\psi \in \mathbb{Q} \setminus \{1\}$. Recall $f_\psi(x) = 4x^5 - 5\psi x^4 + 1$ with the discriminant $D_\psi := 2^8 5^5 (1 - \psi^5)$. If f_ψ is irreducible over $\mathbb{Q}$ and $D_\psi \notin (\mathbb{Q}^\times)^2$, then we can exclude the cases of D_{10} (see [42, proof of Theorem 1]) and A_5 (see [26, Theorem 5]) for the Galois group of f_ψ over $\mathbb{Q}$. To confirm this it suffices to prove the following. Let C be a unique smooth completion of the affine hyperelliptic curve $W : Y^2 = 5(1 - X^5)$ and J be its Jacobian. Clearly, $C(\mathbb{Q}) = W(\mathbb{Q}) \cup \{\infty\}$.

Theorem 7.3. *The affine hyperelliptic curve* $W : Y^2 = 5(1 - X^5)$ *has no* $\mathbb{Q}$*-rational solution except for* $(X, Y) = (1, 0)$.

Proof. By using Magma [8] again, we see that $J(\mathbb{Q}) = J(\mathbb{Q})_{\mathrm{tor}}$. Let $r_\infty : C(\overline{\mathbb{Q}}) \to J(\overline{\mathbb{Q}})$, $Q \mapsto Q - \infty$. Working on $F = \mathbb{Q}(\zeta_5)$, the claim is similarly proved as in the proof of Theorem 7.2. In this case, we consider the set $T = \{(x, 0) \in W(\overline{\mathbb{Q}})\} \cup \{(0, \pm\sqrt{5})\} \cup \{\infty\} \subset C(F)$. Clearly, $r_\infty((x, 0)) \in J[2](F)$

for each $(x,0) \in T$ and $r_\infty((0,\pm\sqrt{5})) \in J[5](F)$ since $(y+\sqrt{5})(y-\sqrt{5}) = 5x^5$. It can be checked that the reduction map induces $T \xrightarrow{\sim} \widetilde{C}(\mathbb{F}_{11})$ since $r_\infty(T) \subset J[10](F) \subset J(F)_{\mathrm{tor}}$ and $|T| = |\widetilde{C}(\mathbb{F}_{11})| = 8$. The details are omitted. $\square$

Remark 7.4. *Regarding above proofs, we apply Magma* [8] *to check the Mordell–Weil rank of $J(\mathbb{Q})$ is zero. Therefore, Theorem 7.1 is as reliable as its system thought the authors in this paper are responsible for the contents in this section in any points.*

8. A variant

In this section, we discuss a variant of the Dwork quintic family and results similar to main theorems (Theorem 1.1 and Theorem 1.2). We omit the proof of them because they are proved without any changes.

Let us consider the family of the Calabi-Yau threefolds over K defined by

$$X_{\psi,\phi} : X_0^5 + X_1^5 + X_2^5 + X_3^5 + \phi X_4^5 - 5\psi X_0X_1X_2X_3X_4 = 0 \tag{8.1}$$

as a family of smooth projective hypersurface in $\mathbb{P}^4$. It is a twisted version of the Dwork quintic family. For each $\psi, \phi \in \overline{K}$ with $\phi(\psi^5\phi - 1) \neq 0$, the fiber is smooth. Let $Y_{\psi,\phi}$ be the singular mirror symmetry of $X_{\psi,\phi}$ which is defined by the closure of the smooth affine variety

$$U_{\psi,\phi} : x_1 + x_2 + x_3 + x_4 + \frac{\phi}{x_1x_2x_3x_4} - 5\psi = 0. \tag{8.2}$$

Then a smooth mirror symmetry $W_{\psi,\phi}$ of $X_{\psi,\phi}$ is similarly constructed from $Y_{\psi,\phi}$ such that $W_{\psi,\phi}$ has good reduction at each finite place v of K satisfying $v \nmid 5\phi$ and $\psi^5\phi - 1$ is a v-adic unit. We introduce the quintic trinomial

$$f_{\psi,\phi}(x) := 4x^5 - 5\psi x^4 + \phi$$

over K and denote by $K_{f_{\psi,\phi}}$ the decomposition field of $f_{\psi,\phi}$ over K. By replacing (x,ψ,ϕ) with $(\frac{1}{x}, a, b)$ where $(a,b) = (-\frac{5\psi}{\phi}, \frac{4}{\phi})$, we have $K_{f_{\psi,\phi}} = K_{g_{a,b}}$ for

$$g_{a,b}(x) = x^5 + ax + b.$$

Let $\bar{\rho}_{\psi,\phi,2} : G_K \to \mathrm{GSp}_4(\mathbb{F}_2)$ be the mod 2 Galois representation associated to $H^3_{\mathrm{\acute{e}t}}(Y_{\psi,\phi,\overline{K}}, \mathbb{F}_2)$. Note that $H^3(Y_{\psi,\phi}(\mathbb{C}), \mathbb{Z})$ (and also $H^3_{\mathrm{\acute{e}t}}(Y_{\psi,\phi,\overline{K}}, \mathbb{Z}_2)$) is torsion free since $Y_{\psi,\phi}(\mathbb{C})$ is isomorphic to a smooth fiber of the Dwork quintic family.

Theorem 8.1. *Let $\psi, \phi \in K$ with $\phi(\psi^5\phi - 1) \neq 0$. Assume that $f_{\psi,\phi}$ is irreducible over K. Then it holds that*

1. $\mathrm{Im}(\bar{\rho}_{\psi,\phi,2}) \simeq \mathrm{Gal}(K_{f_{\psi,\phi}}/K)$ *and* $\mathrm{Im}(\bar{\rho}_{\psi,\phi,2})$ *contains no element of type* $(3,3)$ *under the fixed isomorphism* $\mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$*. In particular, the image is regarded as a subgroup of the 5-th symmetric group* S_5 *whose order is divisible by five;*
2. $\bar{\rho}_{\psi,\phi,2}$ *is irreducible over* $\mathbb{F}_2$ *and hence* $\bar{\rho}_{\psi,\phi,2} \simeq \bar{\rho}^{\mathrm{ss}}_{\psi,\phi,2}$*. Further, it is absolutely irreducible in which case the image is isomorphic to* $F_{20} = C_4 \ltimes C_5, A_5$ *or* S_5 *unless the image is isomorphic to* C_5 *or* $D_{10} = C_2 \ltimes C_5$*.*

Theorem 8.2. *Keep the assumption on $f_{\psi,\phi}$ as in Theorem 8.1. Suppose that $K = F$ is a totally real field and $f_{\psi,\phi}$ is irreducible over F. Assume that* $\mathrm{Gal}(F_{f_{\psi,\phi}}/F) \simeq F_{20}$*, A_5 or S_5 and each complex conjugation in* $\mathrm{Gal}(F_{f_{\psi,\phi}}/F)$ *corresponds to an element of type $(2,2)$. Further assume $[F:\mathbb{Q}]$ is even if* $\mathrm{Gal}(F_{f_{\psi,\phi}}/F) \simeq A_5$*. Let M/F be the totally real quadratic extension associated to the kernel of* $G_F \to \mathrm{Im}(\bar{\rho}_{\psi,\phi,2}) \to S_5 \xrightarrow{\mathrm{sgn}} \{\pm 1\}$ *if* $\mathrm{Gal}(F_{f_{\psi,\phi}}/F) \simeq S_5$ *and $M = F$ otherwise. Put $d = [M:\mathbb{Q}]$. Then there exists a holomorphic Hilbert–Siegel Hecke eigen cusp form h on $\mathcal{H}_2^d$ of parallel weight three such that $\bar{\rho}_{\psi,\phi,2}|_{G_M} \simeq \bar{\rho}_{h,2}$.*

8.1. An example. Let $(\psi,\phi) = (-\frac{4}{5}, -\frac{1}{4})$ which satisfies the condition of both Theorem 8.1 and Theorem 8.2 with the Galois group $\mathrm{Gal}(\mathbb{Q}_{f_{\psi,\phi}}/\mathbb{Q}) \simeq S_5$. Notice that $\mathbb{Q}_{f_{\psi,\phi}} = \mathbb{Q}_g$ with $g(x) = x^5 - x - 1$ and the reciprocity of this polynomial has been studied in [29]. Let $M/\mathbb{Q}$ be the quadratic extension in Theorem 8.2. Then $M = \mathbb{Q}(\sqrt{19 \cdot 151})$. It follows from Theorem 8.2 that there exists a holomorphic Hilbert–Siegel Hecke eigen cusp form h on $\mathcal{H}^2$ of weight $(3,3)$ characterizing mod 2 reciprocity of $f_{\psi,\phi}(x)$ (and also of $g(x)$) over M.

References

[1] A. Ash, P. E. Gunnells & M. McConnell, “Mod 2 homology for GL(4) and Galois representations.”, *J. Number Theory* **146** (2015), p. 4-22.

[2] T. Barnet-Lamb, “Meromorphic continuation for the zeta function of a Dwork hypersurface”, *Algebra Number Theory* **4** (2010), no. 7, p. 839-854.

[3] 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.

[4] V. V. Batyrev, “Dual polyhedral and mirror symmetry for Calabi–Yau hypersurfaces in toric varieties”, *J. Algebr. Geom.* **3** (1994), no. 3, p. 493-535.

[5] ———, “Birational Calabi–Yau n-folds have equal Betti numbers”, in *New trends in algebraic geometry (Warwick, 1996)*, London Mathematical Society Lecture Note Series, vol. 264, Cambridge University Press, 1996, p. 1-11.

[6] V. V. Batyrev & M. Kreuzer, “Integral cohomology and mirror symmetry for Calabi–Yau 3-folds”, in *Mirror symmetry V*, AMS/IP Studies in Advanced Mathematics, vol. 38, American Mathematical Society, 2006, p. 255-270.

[7] T. BERGER, “Oddness of residually reducible Galois representations”, *Int. J. Number Theory* **14** (2018), no. 5, p. 1329-1345.

[8] 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.

[9] A. BRUMER, A. PACETTI, C. POOR, G. TORNARÍA, J. VOIGHT & D. 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 ℓ Galois representations over totally real fields”, *Duke Math. J.* **155** (2010), no. 1, p. 105-161.

[11] K. BUZZARD & T. GEE, “The conjectural connections between automorphic representations and Galois representations”, in *Automorphic forms and Galois representations*, London Mathematical Society Lecture Note Series, vol. 1, Cambridge University Press, 2014, p. 135-187.

[12] F. CALEGARI, “The Artin conjecture for some S_5-extensions”, *Math. Ann.* **356** (2013), no. 1, p. 191-207.

[13] P. CANDELAS, X. DE LA OSSA & F. RODRIGUEZ-VILLEGAS, “Calabi–Yau manifolds over finite fields. II”, in *Calabi–Yau varieties and mirror symmetry (Toronto, ON, 2001)*, Fields Institute Communications, vol. 38, American Mathematical Society, 2001, p. 121-157.

[14] P. DELIGNE & J.-P. SERRE, “Formes modulaires de poids 1”, *Ann. Sci. Éc. Norm. Supér. (4)* **7** (1974), p. 507-530.

[15] L. DEMBÉLÉ, “Explicit computations of Hilbert modular forms on $\mathbb{Q}(\sqrt{5})$”, *Exp. Math.* **14** (2005), no. 4, p. 457-466.

[16] L. DEMBÉLÉ, D. LOEFFLER & A. PACETTI, “Non-paritious Hilbert modular forms”, *Math. Z.* **92** (2019), no. 1-2, p. 361-385.

[17] M. DIMITROV, “Galois representations modulo p and cohomology of Hilbert modular varieties”, *Ann. Sci. Éc. Norm. Supér. (4)* **38** (2005), no. 4, p. 505-551.

[18] ———, “Arithmetic aspects of Hilbert modular forms and varieties”, in *Elliptic curves, Hilbert modular forms and Galois deformations*, Advanced Courses in Mathematics – CRM Barcelona, Birkhäuser, 2013, p. 119-134.

[19] D. S. DUMMIT, “Solving solvable quintics”, *Math. Comput.* **57** (1991), no. 195, p. 387-401.

[20] B. EDIXHOVEN, “Computing the residual Galois representations”, in *Computational aspects of modular forms and Galois representations. How one can compute in polynomial time the value of Ramanujan’s tau at a prime*, Annals of Mathematics Studies, vol. 176, Princeton University Press, 2011, p. 371-382.

[21] W. T. GAN & S. TAKEDA, “The local Langlands conjecture for GSp(4)”, *Ann. Math. (2)* **173** (2011), no. 3, p. 1841-1882.

[22] THE GAP GROUP, “GAP — Groups, Algorithms, and Programming, Version 4.4.12”, 2008, `https://www.gap-system.org`.

[23] T. GEE, F. HERZIG & D. SAVITT, “General Serre weight conjectures”, *J. Eur. Math. Soc.* **20** (2018), no. 12, p. 2859-2949.

[24] T. GEE & O. TAÏBI, “Arthur’s multiplicity formula for GSp_4 and restriction to Sp_4”, *J. Éc. Polytech., Math.* **6** (2019), p. 469-535.

[25] P. GOUTET, “On the zeta function of a family of quintics”, *J. Number Theory* **130** (2010), no. 3, p. 478-492.

[26] K.-I. HASHIMOTO & H. TSUNOGAI, “Generic polynomials over Q with two parameters for the transitive groups of degree five”, *Proc. Japan Acad., Ser. A* **79** (2003), no. 9, p. 142-145.

[27] F. JARVIS, “On Galois representations associated to Hilbert modular forms”, *J. Reine Angew. Math.* **491** (1997), p. 199-216.

[28] G. KEMPF, F. KNUDSEN, D. MUMFORD & B. SAINT-DONAT, *Toroidal embeddings. I.*, Lecture Notes in Mathematics, vol. 339, Springer, 1973, 209 pages.

[29] C. B. KHARE, A. F. LA ROSA & G. WIESE, “Splitting fields of $X^n - X - 1$ (particularly for $n = 5$), prime decomposition and modular forms”, *Expo. Math.* **41** (2023), no. 3, p. 475-491.

[30] C. B. KHARE & J. A. THORNE, “Automorphy of some residually S_5 Galois representations”, *Math. Z.* **286** (2017), no. 1-2, p. 399-429.

[31] H. H. KIM & F. SHAHIDI, “Symmetric cube L-functions for GL_2 are entire”, *Ann. Math. (2)* **150** (1999), no. 2, p. 645-662.

[32] M. Kisin, "Modularity of 2-adic Barsotti–Tate representations", *Invent. Math.* **178** (2009), no. 3, p. 587-634.

[33] ———, "Moduli of finite flat group schemes, and modularity", *Ann. Math. (2)* **170** (2009), no. 3, p. 1085-1180.

[34] C. P. Mok, "Galois representations attached to automorphic forms on GL_2 over CM fields", *Compos. Math.* **150** (2014), no. 4, p. 523-567.

[35] S. Patrikis, "On the sign of regular algebraic polarizable automorphic representations", *Math. Ann.* **362** (2015), no. 1-2, p. 147-171.

[36] S. Patrikis & R. Taylor, "Automorphy and irreducibility of some l-adic representations", *Compos. Math.* **151** (2015), no. 2, p. 207-229.

[37] 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.

[38] D. Ramakrishnan, "Modularity of the Rankin-Selberg L-series, and multiplicity one for SL(2)", *Ann. Math. (2)* **151** (2000), no. 1, p. 45-111.

[39] B. Roberts, "Global L-packets for GSp(2) and theta lifts", *Doc. Math.* **6** (2001), p. 247-314.

[40] B. Roberts & R. Schmidt, *Local Newforms for* GSp(4), Lecture Notes in Mathematics, vol. 1918, Springer, 2007, viii+307 pages.

[41] 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.

[42] G. Roland, N. Yui & D. Zagier, "A parametric family of quintic polynomials with Galois group D_5", *J. Number Theory* **15** (1982), no. 1, p. 137-142.

[43] 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.

[44] R. Taylor, "On the meromorphic continuation of degree two L-functions", *Doc. Math.* **Extra Vol.** (2006), p. 729-779.

[45] J. A. Thorne, "A 2-adic automorphy lifting theorem for unitary groups over CM fields", *Math. Z.* **285** (2017), no. 1-2, p. 1-38.

[46] D. Wan, "Mirror symmetry for zeta functions", in *Mirror symmetry V*, AMS/IP Studies in Advanced Mathematics, vol. 38, American Mathematical Society, 2006, p. 159-184.

[47] R. Weissauer, "Existence of Whittaker models related to four dimensional symplectic Galois representations", in *Modular forms on Schiermonnikoog*, Cambridge University Press, 2008, p. 285-310.

[48] T. Yamauchi, "The residual monodromy for the Dwork family in even characteristic and its applications to Galois representations", 2025, `https://arxiv.org/abs/2506.23938`.

Nobuo Tsuzuki
Mathematical Institute, Graduate School of Science, Tohoku University
6-3, Aoba, Aramaki, Aoba-Ku, Sendai 980-8578, Japan
E-mail: `tsuzuki@math.tohoku.ac.jp`

Takuya Yamauchi
Mathematical Institute, Graduate School of Science, Tohoku University
6-3, Aoba, Aramaki, Aoba-Ku, Sendai 980-8578, Japan
E-mail: `takuya.yamauchi.c3@tohoku.ac.jp`