ON THE PARAMODULARITY OF TYPICAL ABELIAN SURFACES (AND REDUCTION OF G-COVARIANT BILINEAR FORMS)

ARMAND BRUMER, ARIEL PACETTI, CRIS POOR, GONZALO TORNARÍA, JOHN VOIGHT, AND DAVID S. YUEN
(APPENDIX BY J.P. SERRE)

Abstract. Generalizing the method of Faltings–Serre, we rigorously verify that certain abelian surfaces without extra endomorphisms are paramodular. To compute the required Hecke eigenvalues, we develop a method of specialization of Siegel paramodular forms to modular curves. In the appendix, Serre proves a result extending his work on the reduction of G-invariant bilinear forms modulo primes to the case of G-covariant forms.

Contents

1. Introduction

1.1. **Paramodularity.** The Langlands program predicts deep connections between geometry and automorphic forms, encoded in associated L-functions and Galois representations. The celebrated modularity of elliptic curves E over $\mathbb{Q}$ [60, 58, 4] provides an important instance of this program: to the isogeny class of E of conductor N, we associate a classical cuspidal newform $f \in S_2(\Gamma_0(N))$ of weight 2 and level N with rational Hecke eigenvalues such that $L(E,s) = L(f,s)$, and conversely. In particular, $L(E,s)$ shares the good analytic properties of $L(f,s)$ including analytic continuation and functional equation, and the ℓ-adic Galois representations of E and of f are equivalent. More generally, by work of Ribet [48] and the proof of Serre's conjecture by Khare–Wintenberger [38, 39], isogeny classes of abelian varieties A of dimension d, of GL_2-type over $\mathbb{Q}$, and of conductor N^d are in bijection with Galois orbits of classical cuspidal newforms $f \in S_2(\Gamma_1(N))$, with matching (imprimitive) L-functions and ℓ-adic Galois representations.

Date: November 23, 2020.
2010 *Mathematics Subject Classification.* 11F46, 11Y40.

Continuing this program, let A be an abelian surface over $\mathbb{Q}$; for instance, we may take $A = \mathrm{Jac}(X)$ the Jacobian of a curve of genus 2 over $\mathbb{Q}$. We suppose that $\mathrm{End}(A) = \mathbb{Z}$, i.e., A has minimal endomorphisms defined over $\mathbb{Q}$, and in particular A is *not* of GL_2-type over $\mathbb{Q}$. For example, if A has prime conductor, then $\mathrm{End}(A) = \mathbb{Z}$ by a theorem of Ribet (see Lemma 4.1.2). A conjecture of H. Yoshida [61, 62] compatible with the Langlands program is made precise by a conjecture of Brumer–Kramer [7, Conjecture 1.1], restricted here for simplicity.

Conjecture 1.1.1 (Brumer–Kramer)**.** *To every abelian surface A over $\mathbb{Q}$ of conductor N with $\mathrm{End}(A) = \mathbb{Z}$, there exists a cuspidal Siegel paramodular newform f of degree 2, weight 2, and level N with rational Hecke eigenvalues that is not a Gritsenko lift, such that*

$$L(A, s) = L(f, s, \mathrm{spin}). \tag{1.1.2}$$

Moreover, f is unique up to (nonzero) scaling and depends only on the isogeny class of A; and if N is squarefree, then this association is bijective.

Conjecture 1.1.1 is often referred to as the *paramodular conjecture*; in what follows, we say *nonlift* for not a Gritsenko lift. As pointed out by Frank Calegari, in general it is necessary to include abelian fourfolds with quaternionic multiplication for the converse assertion: for a precise statement for arbitrary N and further discussion, see Brumer–Kramer [9].

Extensive experimental evidence [7, 46] supports Conjecture 1.1.1. There is also theoretical evidence for this conjecture when the abelian surface A is potentially of GL_2-type, acquiring extra endomorphisms over a quadratic field: see Johnson-Leung–Roberts [33] for real quadratic fields, Berger–Dembélé–Pacetti–Şengün [5] for imaginary quadratic fields, and Dembélé–Kumar [17] for explicit examples. For a complete treatment of the many possibilities for the association of modular forms to abelian surfaces with potentially extra endomorphisms, see work of Booker–Sijsling–Sutherland–Voight–Yasaki [11]. What remains is the case where $\mathrm{End}(A_{\mathbb{Q}^{\mathrm{al}}}) = \mathbb{Z}$, which is to say that A has minimal endomorphisms defined over the algebraic closure $\mathbb{Q}^{\mathrm{al}}$; we say then that A is *typical*. (We do not say *generic*, since it is not a Zariski open condition on the moduli space.)

Recently, there has been dramatic progress in modularity lifting theorems for nonlift Siegel modular forms (i.e., forms not *of endoscopic type*): see Pilloni [43] for p-adic overconvergent modularity lifting, as well as recent work by Calegari–Geraghty [12, §1.2], Berger–Klosin with Poor–Shurman–Yuen [2] establishing modularity in the reducible case when certain congruences are provided, and a recent manuscript by Boxer–Calegari–Gee–Pilloni [6] establishing potential modularity over totally real fields.

1.2. **Main result.** For all *prime* levels $N < 277$, the paramodular conjecture is known: there are no paramodular forms of the specified type by work of Poor–Yuen [46, Theorem 1.2], and correspondingly there are no abelian surfaces by work of Brumer–Kramer [7, Proposition 1.5]. At level $N = 277$, there exists a cuspidal, nonlift Siegel paramodular cusp form, unique up to scalar multiple, by work of Poor–Yuen [46, Theorem 1.3]: this form is given explicitly as a rational function in Gritsenko lifts of ten weight 2 theta blocks—see (6.2.2).

Our main result is as follows.

Theorem 1.2.1. *Let X be the curve over $\mathbb{Q}$ defined by*

$$y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x;$$

let $A = \mathrm{Jac}(X)$ be its Jacobian, a typical abelian surface over $\mathbb{Q}$ of conductor 277. Let f be the cuspidal, nonlift Siegel paramodular form of genus 2, weight 2, and conductor 277, unique up to scalar multiple. Then

$$L(A, s) = L(f, s, \mathrm{spin}).$$

Theorem 1.2.1 is not implied by any of the published or announced results on paramodularity, and its announcement in October 2015 makes it the first established typical case of the paramodular conjecture. More recently, Berger–Klosin with Poor–Shurman–Yuen [2] recently established the paramodularity of an abelian surface of conductor 731 using a congruence with a Siegel Saito–Kurokawa lift.

Returning to the paramodular conjecture, by work of Brumer–Kramer [8, Theorem 1.2] there is a unique isogeny class of abelian surfaces (LMFDB label 277.a) of conductor 277. Therefore, the proof of Conjecture 1.1.1 for $N = 277$ is completed by Theorem 1.2.1. (More generally, Brumer–Kramer [7] also consider odd semistable conductors at most 1000.)

The theorem implies, and we prove directly, the equality of polynomials $L_p(A, T) = Q_p(f, T)$ for all primes p arising in the Euler product for the corresponding L-series. These equalities are useful in two ways. On the one hand, the Euler factors $L_p(A, T)$ can be computed much more efficiently than for $Q_p(f, T)$: without modularity, to compute the eigenvalues of a Siegel modular form f is difficult and sensitive to the manner in which f was constructed, whereas computing $L_p(A, T)$ can be done in average polynomial time [30] and also efficiently in practice [31]. On the other hand, the L-series $L(A, s)$ is endowed with the good analytic properties of $L(f, s, \mathrm{spin})$: without (potential) modularity, one knows little about $L(A, s)$ beyond convergence in a right half-plane.

By work of Johnson-Leung–Roberts, there are infinitely many quadratic characters χ such that the twist f_χ of the paramodular cusp form by χ is nonzero [34, Main Theorem]. By a local calculation [35, Theorem 3.1], we have $Q_p(f_\chi, T) = Q_p(f, \chi(p)T)$ and similarly $L_p(A_\chi, T) = L_p(A, \chi(p)T)$ for good primes p. Consequently, we have $L(A_\chi, s) = L(f_\chi, s, \mathrm{spin})$ for infinitely many characters χ, and in this way we also establish the paramodularity of infinitely many twists.

We also establish paramodularity for two other isogeny classes in this article of conductors $N = 353$ and $N = 587$, and our method is general enough to establish paramodularity in a wide variety of cases.

1.3. **The method of Faltings–Serre.** We now briefly discuss the method of proof and a few relevant details. Let $\mathrm{Gal}_{\mathbb{Q}} := \mathrm{Gal}(\mathbb{Q}^{\mathrm{al}} \mid \mathbb{Q})$ be the absolute Galois group of $\mathbb{Q}$. To establish paramodularity, we associate 2-adic Galois representations $\rho_A, \rho_f \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{Q}_2^{\mathrm{al}})$ to A and f, and then we prove by an extension of the Faltings–Serre method that these Galois representations are equivalent. The Galois representation for A arises via its Tate module. By contrast, the construction of the Galois representation for the Siegel paramodular form—for which the archimedean component of the associated automorphic representation is a holomorphic limit of discrete series—is much deeper: see Theorem 4.3.4 for a precise statement, attribution, and further discussion.

The first step in carrying out the Faltings–Serre method is to prove equivalence modulo 2, which can be done using information on $\overline{\rho}_f$ obtained by computing $Q_p(f, T)$ modulo 2 for a few small primes p. For example, $p = 3, 5$ are enough for $N = 277$ (see Lemma 7.1.4) and

in this case the mod 2 residual Galois representations

$$\overline{\rho}_A, \overline{\rho}_f \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$$

have common image $S_5(b)$ up to conjugation. (There are two nonconjugate subgroups of S_6 isomorphic to S_5, interchanged by an outer automorphism of S_6: see (5.1.8).)

The second step is to show that the traces of the two representations agree for an effectively computable set of primes p. For example, to finish the proof of Theorem 1.2.1 in level $N = 277$, it suffices to show equality of traces for primes $p \leq 43$.

We also carry out this strategy to prove paramodularity for two other isogeny classes of abelian surfaces. For $N = 353$, we have the isogeny class with LMFDB label 353.a; we again represent the paramodular form as a rational function in Gritsenko lifts; and the common mod 2 image is instead the wreath product $S_3 \wr S_2$ of order 72. For $N = 587$, we have the class with label 587.a; instead, we represent the form as a Borcherds product; and in this case the mod 2 image is the full group S_6.

1.4. **Contributions and organization.** Our contributions in this article are threefold. First, we show how to extend the Faltings–Serre method from GL_2 to a general algebraic group when the residual mod ℓ representations are absolutely irreducible. We then discuss making this practical by consideration of core-free subgroups in a general context, and we hope this will be useful in future investigations. We then make these extensions explicit for GSp_4 and $\ell = 2$. Whereas for GL_2, Serre's original "quartic method" considers extensions whose Galois groups are no larger than S_4, for GSp_4 we must contemplate large polycyclic extensions of S_6-extensions—accordingly, the Galois theory and class field theory required to make the method explicit and to work in practice are much more involved. It would be much more difficult (perhaps hopeless) to work with GL_4 instead of GSp_4, so our formulation is crucial for practical implementation.

By other known means, the task of calculating the required traces for ρ_f would be extremely difficult. Our second contribution in this article is to devise and implement a method of *specialization* of the Siegel modular form to a classical modular form, making this calculation a manageable task.

Our third contribution is to carry out the required computations. There are nine absolutely irreducible subgroups of $\mathrm{GSp}_4(\mathbb{F}_2)$. The three examples we present cover each of the three possibilities for the residual image when it is absolutely irreducible and the level is squarefree (see Lemma 5.2.1). Our methods work for any abelian surface whose mod 2 image is absolutely irreducible, as well as situations for paramodular forms of higher weight. Our implementations are suitable for further investigations along these lines.

The paper is organized as follows. In section 2, we explain the extension of the method of Faltings–Serre in a general (theoretical) algorithmic context; we continue in section 3 by noting a practical extension of this method using some explicit Galois theory. We then consider abelian surfaces, paramodular forms, and their associated Galois representations tailored to our setting in section 4. Coming to our intended application, we provide in section 5 the group theory and Galois theory needed for the Faltings–Serre method for $\mathrm{GSp}_4(\mathbb{Z}_2)$. In section 6, we explain a method to compute Hecke eigenvalues of Siegel paramodular forms using restriction to a modular curve. Finally, in section 7, we combine these to complete our task and verify paramodularity.

1.5. **Acknowledgements.** The authors would like to thank several people for helpful conversations: Frank Calegari, Jennifer Johnson-Leung, Kenneth Kramer, Chung Pang Mok, David P. Roberts (in particular for Proposition 5.2.4), Drew Sutherland, and Eric Urban (in particular for help with showing that the representation is symplectic in Theorem 4.3.4). We also thank Fordham University's Academic Computing Environment for the use of its servers. Thanks also to the anonymous referees for their feedback. Pacetti was partially supported by PIP 2014-2016 11220130100073 and Voight was supported by an NSF CAREER Award (DMS-1151047) and a Simons Collaboration Grant (550029).

This large collaborative project was made possible by the generous support of several host institutes, to which we express our thanks: the Institute for Computational and Experimental Research in Mathematics (ICERM), the International Centre for Theoretical Physics (ICTP), and the Hausdorff Institute of Mathematics (HIM).

2. A general Faltings–Serre method

In this section, from the point of view of general algorithmic theory, we formulate the Faltings–Serre method to show that two ℓ-adic Galois representations are equivalent, under the hypothesis that the residual representations are absolutely irreducible. A practical method for the group $\mathrm{GSp}_4(\mathbb{Z}_2)$ is given in section 5. For further reading on the Faltings–Serre method, see the original criterion given by Serre [53] for elliptic curves over $\mathbb{Q}$, an extension for residually reducible representations by Livné [41, §4], the general overview for GL_2 over number fields by Dieulefait–Guerberoff–Pacetti [18, §4], and the description for GL_n by Schütt [52, §5]. For an algorithmic approach in the pro-p setting, see Grenié [25].

2.1. **Trace computable representations.** Let F be a number field with ring of integers $\mathbb{Z}_F$. Let F^{al} be an algebraic closure of F; we take all algebraic extensions of F inside F^{al}. Let $\mathrm{Gal}_F := \mathrm{Gal}(F^{\mathrm{al}} \mid F)$ be the absolute Galois group of F. Let S be a finite set of places of F, let $\mathrm{Gal}_{F,S}$ be the Galois group of the maximal subextension of $F^{\mathrm{al}} \supseteq F$ unramified away from S. By a *prime* of F we mean a nonzero prime ideal $\mathfrak{p} \subset \mathbb{Z}_F$, or equivalently, a finite place of F.

Let $\mathrm{G} \subseteq \mathrm{GL}_n$ be an embedded algebraic group over $\mathbb{Q}$. Let ℓ be a prime of good reduction for the inclusion $\mathrm{G} \subseteq \mathrm{GL}_n$. A *representation* $\mathrm{Gal}_{F,S} \to \mathrm{G}(\mathbb{Z}_\ell)$ is a continuous homomorphism.

Definition 2.1.1. Let $\rho_1, \rho_2 \colon \mathrm{Gal}_{F,S} \to \mathrm{G}(\mathbb{Z}_\ell)$ be two representations. We say ρ_1 and ρ_2 are (GL_n-)*equivalent*, and we write $\rho_1 \simeq \rho_2$, if there exists $g \in \mathrm{GL}_n(\mathbb{Z}_\ell)$ such that

$$\rho_1(\sigma) = g\rho_2(\sigma)g^{-1}, \quad \text{for all } \sigma \in \mathrm{Gal}_{F,S}.$$

Definition 2.1.2. A representation $\rho \colon \mathrm{Gal}_{F,S} \to \mathrm{G}(\mathbb{Z}_\ell)$ is *trace computable* there exists a deterministic algorithm to compute $\mathrm{tr}(\mathrm{Frob}_\mathfrak{p})$ for $\mathfrak{p} \notin S$, where $\mathrm{Frob}_\mathfrak{p}$ denotes the conjugacy class of the Frobenius automorphism at $\mathfrak{p}$.

In particular, if ρ is trace computable then the values $\mathrm{tr}\,\rho(\mathrm{Frob}_\mathfrak{p})$ belong to a computable subring of $\mathbb{Z}_\ell$. For precise definitions and a thorough survey of the subject of computable rings, see Stoltenberg-Hansen–Tucker [55]. See Cohen [14] for background on algorithmic number theory.

Remark 2.1.3. Galois representations arising in arithmetic geometry are often trace computable. For example, by counting points over finite fields, we may access the trace of

Frobenius acting on Galois representations arising from the étale cohomology of a nice variety: then the trace takes values in $\mathbb{Z} \subseteq \mathbb{Z}_\ell$ (independent of ℓ). Similarly, algorithms to compute modular forms give as output Hecke eigenvalues, which can then be interpreted in terms of the trace of Frobenius on the associated Galois representation.

Looking only at the trace of a representation is justified in certain cases by the following theorem, a cousin to the Brauer–Nesbitt theorem. For $r \geq 1$, write

$$\rho \bmod \ell^r \colon \operatorname{Gal}_{F,S} \to \mathrm{G}(\mathbb{Z}/\ell^r\mathbb{Z})$$

for the reduction of ρ modulo ℓ^r, and as a shorthand write

$$\overline{\rho} \colon \operatorname{Gal}_{F,S} \to \mathrm{G}(\mathbb{F}_\ell)$$

for the residual representation $\overline{\rho} = \rho \bmod \ell$. Given two representations $\rho_1, \rho_2 : \operatorname{Gal}_{F,S} \to \mathrm{G}(\mathbb{Z}_\ell)$, we write $\rho_1 \simeq \rho_2 \pmod{\ell^r}$ to mean that $(\rho_1 \bmod \ell^r) \simeq (\rho_2 \bmod \ell^r)$ are equivalent as in Definition 2.1.1 but over $\mathbb{Z}/\ell^r\mathbb{Z}$; we write $\rho_1 \equiv \rho_2 \pmod{\ell^r}$ to mean that $(\rho_1 \bmod \ell^r) = (\rho_2 \bmod \ell^r)$; and we write $\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \pmod{\ell^r}$ if $\operatorname{tr}\rho_1(\sigma) \equiv \operatorname{tr}\rho_2(\sigma) \pmod{\ell^r}$ for all $\sigma \in \operatorname{Gal}_{F,S}$. Finally, we say that $\overline{\rho}$ is *absolutely irreducible* if the representation $\operatorname{Gal}_{F,S} \to \mathrm{G}(\mathbb{F}_\ell) \hookrightarrow \mathrm{GL}_n(\mathbb{F}_\ell)$ is absolutely irreducible.

Theorem 2.1.4 (Carayol)**.** *Let $\rho_1, \rho_2 : \operatorname{Gal}_{F,S} \to \mathrm{G}(\mathbb{Z}_\ell)$ be two representations such that $\overline{\rho}_1$ is absolutely irreducible and let $r \geq 1$. Then $\rho_1 \simeq \rho_2 \bmod \ell^r$ if and only if $\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \pmod{\ell^r}$.*

Proof. See Carayol [13, Théorème 1]. □

We now state the main result of this section. We say that a prime $\mathfrak{p}$ of F is a *witness* to the fact that $\rho_1 \not\simeq \rho_2$ if $\operatorname{tr}\rho_1(\mathrm{Frob}_\mathfrak{p}) \neq \operatorname{tr}\rho_2(\mathrm{Frob}_\mathfrak{p})$.

Theorem 2.1.5. *There is a deterministic algorithm that takes as input*

$$\begin{gathered} \text{an algebraic group } \mathrm{G} \text{ over } \mathbb{Q}\text{, a number field } F\text{,} \\ \text{a finite set } S \text{ of primes of } F\text{, a prime } \ell\text{,} \\ \text{and } \rho_1, \rho_2 \colon \operatorname{Gal}_{F,S} \to \mathrm{G}(\mathbb{Z}_\ell) \text{ trace computable representations} \\ \text{with } \overline{\rho}_1, \overline{\rho}_2 \text{ absolutely irreducible,} \end{gathered} \tag{2.1.6}$$

and gives as output

$$\begin{gathered} \texttt{true} \text{ if } \rho_1 \simeq \rho_2\text{; or} \\ \texttt{false} \text{ and a witness prime } \mathfrak{p} \notin S \text{ if } \rho_1 \not\simeq \rho_2. \end{gathered}$$

The algorithm does not operate on the representations ρ_1, ρ_2 themselves, only their traces. The proof of Theorem 2.1.5 will occupy us throughout this section.

2.2. **Testing equivalence of residual representations.** We first prove a variant of our theorem for the residual representations. For a finite extension $K_0 \supseteq F$ of fields with $[K_0 : F] = n$ and with Galois closure K, we write $\operatorname{Gal}(K_0 \,|\, F) \leq S_n$ for the Galois group $\operatorname{Gal}(K \,|\, F)$ as a permutation group on the roots of a minimal polynomial of a primitive element for K_0.

Lemma 2.2.1. *There exists a deterministic algorithm that takes as input*

$$\begin{gathered} \text{a number field } F\text{,} \\ \text{a finite set } S \text{ of places of } F\text{,} \\ \text{and a transitive group } G \leq S_n\text{,} \end{gathered}$$

and gives as output

$$\begin{gathered}\textit{all extensions } K_0 \supseteq F \textit{ (up to isomorphism) of degree } n \\ \textit{unramified at all places } v \notin S \\ \textit{such that } \mathrm{Gal}(K_0 \,|\, F) \simeq G \textit{ as permutation groups.}\end{gathered}$$

Moreover, every Galois extension $K \supseteq F$ unramified outside S such that $\mathrm{Gal}(K \,|\, F) \simeq G$ as groups appears as the Galois closure of at least one such $K_0 \supseteq F$.

Proof. The extensions K_0 have degree n and are unramified away from S, so they have effectively bounded discriminant by Krasner's lemma. Therefore, there are finitely many such fields up to isomorphism, by a classical theorem of Hermite. The enumeration can be accomplished algorithmically by a *Hunter search*: see Cohen [15, §9.3]. The computation and verification of Galois groups can also be accomplished effectively.

The second statement follows from basic Galois theory. □

Remark 2.2.2. For theoretical purposes, it is enough to consider $G \hookrightarrow S_n$ in its regular representation ($n = \#G$), for which the algorithm yields Galois extensions $K = K_0 \supseteq F$. For practical purposes, it is crucial to work with small permutation representations.

Algorithm 2.2.3. The following algorithm takes as input the data (2.1.6) and gives as output

$$\begin{gathered}\texttt{true} \text{ if } \overline{\rho}_1 \simeq \overline{\rho}_2\text{; or} \\ \texttt{false} \text{ and a witness prime } \mathfrak{p} \notin S \text{ if } \overline{\rho}_1 \not\simeq \overline{\rho}_2.\end{gathered}$$

1. Using the algorithm of Lemma 2.2.1, enumerate all Galois extensions $K \supseteq F$ up to isomorphism that are unramified away from S and such that $\mathrm{Gal}(K \,|\, F)$ is isomorphic to a subgroup of $\mathrm{G}(\mathbb{F}_\ell)$.
2. For each of these finitely many fields, enumerate all injective group homomorphisms $\theta\colon \mathrm{Gal}(K \,|\, F) \hookrightarrow \mathrm{G}(\mathbb{F}_\ell)$ up to conjugation by $\mathrm{GL}_n(\mathbb{F}_\ell)$.
3. Looping over primes $\mathfrak{p} \notin S$ of F, rule out pairs (K, θ) such that
$$\operatorname{tr} \rho_1(\mathrm{Frob}_\mathfrak{p}) \not\equiv \operatorname{tr} \theta(\mathrm{Frob}_\mathfrak{p}) \pmod{\ell}$$
for some $\mathfrak{p}$ until only one possibility (K_1, θ_1) remains.
4. Let $\mathcal{P}$ be the set of primes used in Step 3. If
$$\operatorname{tr} \rho_2(\mathrm{Frob}_\mathfrak{p}) \equiv \operatorname{tr} \theta_1(\mathrm{Frob}_\mathfrak{p}) \pmod{\ell}$$
for all $\mathfrak{p} \in \mathcal{P}$, return `true`; otherwise, return `false` and a prime $\mathfrak{p} \in \mathcal{P}$ such that $\operatorname{tr} \rho_2(\mathrm{Frob}_\mathfrak{p}) \not\equiv \operatorname{tr} \theta_1(\mathrm{Frob}_\mathfrak{p})$.

Proof of correctness. Let K_1 be the fixed field under $\ker \overline{\rho}_1$; then K_1 is unramified away from S, and we have an injective homomorphism $\overline{\rho}_1\colon \mathrm{Gal}(K_1 \,|\, F) \hookrightarrow \mathrm{G}(\mathbb{F}_\ell)$. Thus $(K_1, \overline{\rho}_1)$ is among the finite list of pairs (K, θ) computed in Step 2.

Combining Theorem 2.1.4 (for $r = 1$) and the Chebotarev density theorem, we can effectively determine if $\overline{\rho}_1 \not\simeq \theta$ by finding a prime $\mathfrak{p}$ such that $\operatorname{tr} \rho_1(\mathrm{Frob}_\mathfrak{p}) \not\equiv \operatorname{tr} \theta(\mathrm{Frob}_\mathfrak{p}) \pmod{\ell}$. So by looping over the primes $\mathfrak{p} \notin S$ of F in Step 3, we will eventually rule out all of the finitely many candidates except one (K_1', θ_1') and, in the style of Sherlock Holmes, we must have $K_1 = K_1'$ and $\overline{\rho}_1 \simeq \theta_1$.

For the same reason, if $\operatorname{tr} \rho_2(\mathrm{Frob}_\mathfrak{p}) \equiv \operatorname{tr} \theta_1(\mathrm{Frob}_\mathfrak{p}) \pmod{\ell}$ for all $\mathfrak{p} \in \mathcal{P}$ we must have $\overline{\rho}_2 \simeq \theta_1 \simeq \overline{\rho}_1$. Otherwise, we find a witness prime $\mathfrak{p} \in \mathcal{P}$. □

Remark 2.2.4. In practice, we may also use the characteristic polynomial of $\overline{\rho}_i(\mathrm{Frob}_{\mathfrak{p}})$ when it is computable, since it gives more information about the residual image and thereby limits the possible subgroups of $\mathrm{G}(\mathbb{F}_\ell)$ we need to consider in Step 1. This allows for a smaller list of pairs (K, θ) and a smaller list of primes: see Lemma 7.1.4 for an example.

2.3. **Faltings–Serre and deformation.** With the residual representations identified, we now explain the key idea of the Faltings–Serre method: we exhibit another representation that measures the failure of two representations to be equivalent. This construction is quite natural when viewed in the language of deformation theory: see Gouvêa [24, Lecture 4] for background.

For the remainder of this section, let $\rho_1, \rho_2 \colon \mathrm{Gal}_{F,S} \to \mathrm{G}(\mathbb{Z}_\ell)$ be representations such that $\rho_1 \simeq \rho_2 \pmod{\ell^r}$ for some $r \geq 1$. Conjugating ρ_2, we may assume $\rho_1 \equiv \rho_2 \pmod{\ell^r}$, and we write $\overline{\rho} := \overline{\rho}_1 = \overline{\rho}_2$ for the common residual representation modulo ℓ. We suppose throughout that $\overline{\rho}$ is absolutely irreducible.

Let $\mathrm{Lie}(\mathrm{G}) \leq \mathrm{M}_n$ be the Lie algebra of G over $\mathbb{Q}$ as a commutative algebraic group. Attached to $\overline{\rho}$ is the *adjoint residual representation*

$$\begin{aligned} \mathrm{ad}\,\overline{\rho} \colon \mathrm{Gal}_{F,S} &\to \mathrm{Aut}_{\mathbb{F}_\ell}(\mathrm{M}_n(\mathbb{F}_\ell)) \\ \sigma &\mapsto \sigma_{\mathrm{ad}} \end{aligned} \tag{2.3.1}$$

defined by $\sigma_{\mathrm{ad}}(a) := \overline{\rho}(\sigma) a \overline{\rho}(\sigma)^{-1}$ for $a \in \mathrm{M}_n(\mathbb{F}_\ell)$. The adjoint residual representation $\mathrm{ad}\,\overline{\rho}$ also restricts to take values in $\mathrm{Aut}_{\mathbb{F}_\ell}(\mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell))$, but we will not need to introduce new notation for this restriction.

Because we consider representations with values in G up to equivalence in GL_n, it is natural that our deformations will take values in $\mathrm{Lie}(\mathrm{G})$ up to equivalence in M_n. With this in mind, we define the group of *cocycles*

$$\begin{aligned} &\mathrm{Z}^1(F, \mathrm{ad}\,\overline{\rho}; \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell)) := \\ &\quad \left\{(\mu \colon \mathrm{Gal}_{F,S} \to \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell)) : \mu(\sigma\tau) = \mu(\sigma) + \sigma_{\mathrm{ad}}(\mu(\tau)) \text{ for all } \sigma, \tau \in \mathrm{Gal}_{F,S}\right\} \end{aligned} \tag{2.3.2}$$

and the subgroup of *coboundaries*

$$\begin{aligned} &\mathrm{B}^1(F, \mathrm{ad}\,\overline{\rho}; \mathrm{M}_n(\mathbb{F}_\ell)) := \\ &\quad \big\{\mu \in \mathrm{Z}^1(F, \mathrm{ad}\,\overline{\rho}; \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell)) : \text{there exists } a \in \mathrm{M}_n(\mathbb{F}_\ell) \text{ such that} \\ &\qquad\qquad \mu(\sigma) = a - \sigma_{\mathrm{ad}}(a) \text{ for all } \sigma \in \mathrm{Gal}_{F,S}\big\}. \end{aligned} \tag{2.3.3}$$

From the exact sequence

$$1 \to 1 + \ell^r \,\mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell) \to \mathrm{G}(\mathbb{Z}/\ell^{r+1}\mathbb{Z}) \to \mathrm{G}(\mathbb{Z}/\ell^r\mathbb{Z}) \to 1, \tag{2.3.4}$$

we conclude that for all $\sigma \in \mathrm{Gal}_{F,S}$ there exists $\mu(\sigma) \in \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell)$ such that

$$\rho_1(\sigma) \equiv (1 + \ell^r \mu(\sigma))\rho_2(\sigma) \pmod{\ell^{r+1}}. \tag{2.3.5}$$

Lemma 2.3.6. *The following statements hold.*

(a) *The map $\sigma \mapsto \mu(\sigma)$ defined by (2.3.5) is a cocycle $\mu \in \mathrm{Z}^1(F, \mathrm{ad}\,\overline{\rho}; \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell))$.*
(b) *We have $\rho_1 \simeq \rho_2 \pmod{\ell^{r+1}}$ if and only if $\mu \in \mathrm{B}^1(F, \mathrm{ad}\,\overline{\rho}; \mathrm{M}_n(\mathbb{F}_\ell))$.*

Proof. We verify the cocycle condition as follows:

$$\begin{aligned}\rho_1(\sigma\tau) = \rho_1(\sigma)\rho_1(\tau) &\equiv (1+\ell^r\mu(\sigma))\rho_2(\sigma)(1+\ell^r\mu(\tau))\rho_2(\tau)\\ &\equiv (1+\ell^r(\mu(\sigma)+\rho_2(\sigma)\mu(\tau)\rho_2(\sigma)^{-1}))\rho_2(\sigma)\rho_2(\tau)\\ &\equiv (1+\ell^r\mu(\sigma\tau))\rho_2(\sigma\tau) \pmod{\ell^{r+1}}\end{aligned}$$

so $\mu(\sigma\tau) = \mu(\sigma) + \sigma_{\mathrm{ad}}(\mu(\tau))$ as claimed. For the second statement, by definition $\rho_1 \simeq \rho_2 \pmod{\ell^{r+1}}$ if and only if there exists $a_r \in \mathrm{GL}_n(\mathbb{Z}/\ell^{r+1}\mathbb{Z})$ such that for all $\sigma \in \mathrm{Gal}_{F,S}$ we have

$$\rho_1(\sigma) \equiv a_r\rho_2(\sigma)a_r^{-1} \pmod{\ell^{r+1}}. \tag{2.3.7}$$

Since $\rho_1(\sigma) \equiv \rho_2(\sigma) \pmod{\ell^r}$, the image of a_r in $\mathrm{GL}_n(\mathbb{Z}/\ell^r\mathbb{Z})$ centralizes the image of $\rho \pmod{\ell^r}$. Since the image is irreducible, by Schur's lemma we have $a_r \bmod \ell^r$ is scalar, so without loss of generality we may suppose $a_r \equiv 1 \pmod{\ell^r}$, so that $a_r = 1 + \ell^r a$ for some $a \in \mathrm{M}_n(\mathbb{F}_\ell)$. Expanding (2.3.7) then yields

$$\begin{aligned}\rho_1(\sigma) &\equiv (1+\ell^r a)\,\rho_2(\sigma)\,(1+\ell^r a)^{-1} \equiv (1+\ell^r a)\,\rho_2(\sigma)\,(1-\ell^r a)\\ &\equiv (1+\ell^r a - \ell^r\rho_2(\sigma)a\rho_2(\sigma)^{-1})\rho_2(\sigma)\\ &\equiv (1+\ell^r(a-\sigma_{\mathrm{ad}}(a)))\rho_2(\sigma) \pmod{\ell^{r+1}}\end{aligned}$$

so $\mu(\sigma) = a - \sigma_{\mathrm{ad}}(a)$ by definition (2.3.5). □

Our task now turns to finding an effective way to detect when μ is a coboundary. For this purpose, we work with extensions of our representations using explicit parabolic groups. The adjoint action of GL_n on M_n gives an exact sequence

$$0 \to \mathrm{M}_n \to \mathrm{M}_n \rtimes \mathrm{GL}_n \to \mathrm{GL}_n \to 1 \tag{2.3.8}$$

which extends to a linear representation via the *parabolic subgroup*, as follows. We embed

$$\begin{aligned}\mathrm{M}_n \rtimes \mathrm{GL}_n &\hookrightarrow \mathrm{GL}_{2n}\\ (a,g) &\mapsto \begin{pmatrix}1 & a\\ 0 & 1\end{pmatrix}\begin{pmatrix}g & 0\\ 0 & g\end{pmatrix} = \begin{pmatrix}g & ag\\ 0 & g\end{pmatrix}\end{aligned} \tag{2.3.9}$$

(on points, realizing $\mathrm{M}_n \rtimes \mathrm{GL}_n$ as an algebraic matrix group). The embedding (2.3.9) is compatible with the exact sequence (2.3.8): the natural projection map

$$\pi\colon \mathrm{M}_n \rtimes \mathrm{GL}_n \to \mathrm{GL}_n \tag{2.3.10}$$

corresponds to the projection onto the top left entry, it is split by the diagonal embedding $\mathrm{GL}_n \hookrightarrow \mathrm{GL}_{2n}$, and it has kernel isomorphic to M_n in the upper-right entry. We will identify $\mathrm{M}_n \rtimes \mathrm{GL}_n$ and its subgroups with their image in GL_{2n}.

Let $\mathrm{utr}\colon (\mathrm{M}_n \rtimes \mathrm{GL}_n)(\mathbb{F}_\ell) \to \mathbb{F}_\ell$ denote the trace of the upper right $n \times n$-block.

Lemma 2.3.11. *The map* utr *is well-defined on conjugacy classes in* $(\mathrm{M}_n \rtimes \mathrm{GL}_n)(\mathbb{F}_\ell)$.

Proof. For all $g, h \in \mathrm{GL}_n(\mathbb{F}_\ell)$ and $a, b \in \mathrm{M}_n(\mathbb{F}_\ell)$ we have

$$\begin{pmatrix}h & bh\\ 0 & h\end{pmatrix}\begin{pmatrix}g & ag\\ 0 & g\end{pmatrix}\begin{pmatrix}h^{-1} & -h^{-1}b\\ 0 & h^{-1}\end{pmatrix} = \begin{pmatrix}hgh^{-1} & hagh^{-1} + bhgh^{-1} - hgh^{-1}b\\ 0 & hgh^{-1}\end{pmatrix} \tag{2.3.12}$$

so the upper trace is $\mathrm{tr}(hagh^{-1} + bhgh^{-1} - hgh^{-1}b) = \mathrm{tr}(ag)$. □

For $\mu \in \mathrm{Z}^1(F, \operatorname{ad}\overline{\rho}; \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell))$ we define

$$\begin{aligned} \varphi_\mu \colon \mathrm{Gal}_{F,S} &\to (\mathrm{Lie}(\mathrm{G}) \rtimes \mathrm{G})(\mathbb{F}_\ell) \leq \mathrm{GL}_{2n}(\mathbb{F}_\ell) \\ \sigma &\mapsto (\mu(\sigma), \overline{\rho}(\sigma)) = \begin{pmatrix} \overline{\rho}(\sigma) & \mu(\sigma)\overline{\rho}(\sigma) \\ 0 & \overline{\rho}(\sigma) \end{pmatrix}. \end{aligned} \tag{2.3.13}$$

Proposition 2.3.14. *Let $\mu \in \mathrm{Z}^1(F, \operatorname{ad}\overline{\rho}; \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell))$. Then the following statements hold.*

(a) *The map φ_μ defined by (2.3.13) is a group homomorphism, and $\pi \circ \varphi_\mu = \overline{\rho}$.*

(b) *We have $\mu \in \mathrm{B}^1(F, \operatorname{ad}\overline{\rho}; \mathrm{M}_n(\mathbb{F}_\ell))$ if and only if φ_μ is conjugate to $\varphi_0 = \left(\begin{smallmatrix} \overline{\rho} & 0 \\ 0 & \overline{\rho} \end{smallmatrix}\right)$ by an element of $\mathrm{M}_n(\mathbb{F}_\ell) \leq (\mathrm{M}_n \rtimes \mathrm{GL}_n)(\mathbb{F}_\ell)$.*

$$\operatorname{utr} \varphi_\mu(\sigma) = \operatorname{tr}\big(\mu(\sigma)\overline{\rho}(\sigma)\big) \equiv \frac{\operatorname{tr}\rho_1(\sigma) - \operatorname{tr}\rho_2(\sigma)}{\ell^r} \pmod{\ell}. \tag{2.3.15}$$

Proof. For (a), the cocycle condition implies that φ_μ is a group homomorphism: the upper right entry of $\varphi_\mu(\sigma\tau)$ is

$$\mu(\sigma\tau)\overline{\rho}(\sigma\tau) = (\mu(\sigma) + \overline{\rho}(\sigma)\mu(\tau)\overline{\rho}(\sigma)^{-1})\overline{\rho}(\sigma)\overline{\rho}(\tau) = \mu(\sigma)\overline{\rho}(\sigma)\overline{\rho}(\tau) + \overline{\rho}(\sigma)\mu(\tau)\overline{\rho}(\tau)$$

which is equal to the upper right entry of $\varphi_\mu(\sigma)\varphi_\mu(\tau)$ obtained by matrix multiplication.

For (b), the calculation

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \overline{\rho}(\sigma) & 0 \\ 0 & \overline{\rho}(\sigma) \end{pmatrix} \begin{pmatrix} 1 & -a \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} \overline{\rho}(\sigma) & a\overline{\rho}(\sigma) - \overline{\rho}(\sigma)a \\ 0 & \overline{\rho}(\sigma) \end{pmatrix} \tag{2.3.16}$$

shows that $\varphi_\mu = a\varphi_0 a^{-1}$ for $a \in \mathrm{M}_n(\mathbb{F}_\ell)$ if and only if $\mu(\sigma)\overline{\rho}(\sigma) = a\overline{\rho}(\sigma) - \overline{\rho}(\sigma)a$ for all $\sigma \in \mathrm{Gal}_{F,S}$. Multiplying on the right by $\overline{\rho}(\sigma)^{-1}$, we see this is equivalent to $\mu(\sigma) = a - \sigma_{\mathrm{ad}}(a)$ for all $\sigma \in \mathrm{Gal}_{F,S}$.

Finally, (c) follows directly from (2.3.5). □

Definition 2.3.17. Let K be the fixed field under $\overline{\rho}$. We say a pair (L, φ) *extends* $(K, \overline{\rho})$ if

$$\varphi \colon \mathrm{Gal}_{F,S} \to (\mathrm{Lie}(\mathrm{G}) \rtimes \mathrm{G})(\mathbb{F}_\ell) \leq \mathrm{GL}_{2n}(\mathbb{F}_\ell)$$

is a representation with fixed field L such that $\pi \circ \varphi = \overline{\rho}$.

If (L, φ) extends $(K, \overline{\rho})$, then $L \supseteq K$ is an ℓ-elementary abelian extension unramified outside S, since φ induces an injective group homomorphism $\mathrm{Gal}(L \,|\, K) \hookrightarrow \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell)$.

Definition 2.3.18. A pair (L, φ) extending $(K, \overline{\rho})$ is *obstructing* if $\operatorname{utr}\varphi \not\equiv 0 \pmod{\ell}$, and we call the group homomorphism φ an *obstructing extension* of $\overline{\rho}$. An element $\sigma \in \mathrm{Gal}(L \,|\, F)$ such that $\operatorname{utr}\varphi(\sigma) \not\equiv 0 \pmod{\ell}$ is called *obstructing* for φ.

We note the following corollary of Proposition 2.3.14.

Corollary 2.3.19. *Let μ be defined by (2.3.5) and φ_μ by (2.3.13). Then φ_μ extends $\overline{\rho}$, and φ_μ is obstructing if and only if $\mu \notin \mathrm{B}^1(F, \operatorname{ad}\overline{\rho}; \mathrm{M}_n(\mathbb{F}_\ell))$.*

Proof. The map φ_μ extends $\overline{\rho}$ by Proposition 2.3.14(a). We prove the contrapositive of the second statement: $\mu \in \mathrm{B}^1(F, \operatorname{ad}\overline{\rho}; \mathrm{M}_n(\mathbb{F}_\ell))$ if and only if $\operatorname{utr}\varphi_\mu \equiv 0 \pmod{\ell}$. The implication ($\Rightarrow$) is immediate from Proposition 2.3.14(b) and the invariance of utr by conjugation (Lemma 2.3.11). For ($\Leftarrow$), if $\operatorname{utr}\varphi_\mu \equiv 0 \pmod{\ell}$ then $\operatorname{tr}\rho_1 \equiv \operatorname{tr}\rho_2 \pmod{\ell^{r+1}}$ by Proposition 2.3.14(c). Now Theorem 2.1.4 implies $\rho_1 \simeq \rho_2 \pmod{\ell^{r+1}}$, hence $\mu \in \mathrm{B}^1(F, \operatorname{ad}\overline{\rho}; \mathrm{M}_n(\mathbb{F}_\ell))$ by Lemma 2.3.6(b). □

Before we conclude this section, we note the following important improvement. Let $\mathrm{Lie}^0(\mathrm{G}) \leq \mathrm{Lie}(\mathrm{G})$ be the subgroup of trace zero matrices, and note that $\mathrm{Lie}^0(\mathrm{G})(\mathbb{F}_\ell)$ is invariant by the adjoint residual representation.

Lemma 2.3.20. *If* $\det \rho_1 = \det \rho_2$, *then* μ *takes values in* $\mathrm{Lie}^0(\mathrm{G})(\mathbb{F}_\ell)$.

Proof. By (2.3.5), we have $1 = \det(\rho_1 \rho_2^{-1}) = \det(1 + \ell^r \mu) \equiv 1 + \ell^r \operatorname{tr} \mu \pmod{\ell^{2r}}$ so accordingly $\operatorname{tr} \mu(\sigma) \equiv 0 \pmod{\ell}$ and $\mu(\sigma) \in \mathrm{Lie}^0(\mathrm{G})(\mathbb{F}_\ell)$ for all $\sigma \in \mathrm{Gal}_{F,S}$. □

In view of Lemma 2.3.20, we note that Proposition 2.3.14 and Corollary 2.3.19 hold when replacing $\mathrm{Lie}(\mathrm{G})$ by $\mathrm{Lie}^0(\mathrm{G})$.

2.4. **Testing equivalence of representations.** We now use Corollary 2.3.19 to prove Theorem 2.1.5.

Algorithm 2.4.1. The following algorithm takes as input the data (2.1.6) and gives as output

`true` if $\rho_1 \simeq \rho_2$; or
`false` and a witness prime $\mathfrak{p}$ if $\rho_1 \not\simeq \rho_2$.

1. Apply Algorithm 2.2.3; if $\overline{\rho}_1 \not\simeq \overline{\rho}_2$, return `false` and the witness prime $\mathfrak{p}$. Otherwise, let K be the fixed field under the common residual representation $\overline{\rho}$.
2. Using the algorithm of Lemma 2.2.1, enumerate all ℓ-elementary abelian extensions $L \supseteq K$ unramified away from S and such that $\mathrm{Gal}(L \mid F)$ is isomorphic to a subgroup of $(\mathrm{Lie}(\mathrm{G}) \rtimes \mathrm{G})(\mathbb{F}_\ell)$.
3. For each of these finitely many fields L, by enumeration of injective group homomorphisms $\mathrm{Gal}(L \mid F) \hookrightarrow (\mathrm{Lie}(\mathrm{G}) \rtimes \mathrm{G})(\mathbb{F}_\ell)$, find all obstructing pairs (L, φ) extending $(K, \overline{\rho})$ up to conjugation by $(\mathrm{M}_n \rtimes \mathrm{GL}_n)(\mathbb{F}_\ell)$.
4. For each such pair (L, φ), find a prime $\mathfrak{p} \notin S$ such that $\operatorname{utr} \varphi(\mathrm{Frob}_\mathfrak{p}) \not\equiv 0 \pmod{\ell}$.
5. Check if $\operatorname{tr} \rho_1(\mathrm{Frob}_\mathfrak{p}) = \operatorname{tr} \rho_2(\mathrm{Frob}_\mathfrak{p})$ for the primes in Step 4. If equality holds for all primes, return `true`; if equality fails for $\mathfrak{p}$, return `false` and the prime $\mathfrak{p}$.

Remark 2.4.2. In Step 2, we may instead use algorithmic class field theory (and we will do so in practice). Moreover, if we know that $\det \rho_1 = \det \rho_2$, then we can replace $\mathrm{Lie}(\mathrm{G})$ by $\mathrm{Lie}^0(G)$ by Lemma 2.3.20.

Proof of correctness. By the Chebotarev density theorem, in Step 4 we will eventually find a prime $\mathfrak{p} \notin S$, since utr is well-defined on conjugacy classes by Lemma 2.3.11. In the final step, if equality does not hold for some prime $\mathfrak{p}$, we have found a witness, and we correctly return `false`.

Otherwise, we return `true` and we claim that $\rho_1 \simeq \rho_2$ so the output is correct. Indeed, assume for purposes of contradiction that $\rho_1 \not\simeq \rho_2$. Then there exists $r \geq 1$ such that $\rho_1 \simeq \rho_2 \pmod{\ell^r}$ but $\rho_1 \not\simeq \rho_2 \pmod{\ell^{r+1}}$. We can assume as before that $\rho_1 \equiv \rho_2 \pmod{\ell^r}$. We define μ by (2.3.5) and φ_μ by (2.3.13). Let L_μ be the fixed field of φ_μ. By Lemma 2.3.6 we have $\mu \notin \mathrm{B}^1(F, \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell); \mathrm{M}_n(\mathbb{F}_\ell))$, hence by Corollary 2.3.19 φ_μ extends $\overline{\rho}$ and is obstructing. It follows that the pair (L_μ, φ_μ) is, up to conjugation by $(\mathrm{M}_n \rtimes \mathrm{GL}_n)(\mathbb{F}_\ell)$, among the pairs computed in Step 3. In particular there is a prime $\mathfrak{p}$ in Step 4 such that $\operatorname{utr} \varphi_\mu(\mathrm{Frob}_\mathfrak{p}) \not\equiv 0 \pmod{\ell}$. But then by (2.3.15) we would have $\operatorname{tr} \rho_1(\mathrm{Frob}_\mathfrak{p}) \neq \operatorname{tr} \rho_2(\mathrm{Frob}_\mathfrak{p})$, contradicting the verification carried out in Step 5. □

The correctness of Algorithm 2.4.1 then proves Theorem 2.1.5.

Remark 2.4.3. In the case $\mathrm{G} = \mathrm{GSp}_{2g}$, using an effective version of the Chebotarev density theorem, Achter [1, Lemma 1.2] has given an effective upper bound in terms of the conductor and genus to detect when two abelian surfaces are isogenous. This upper bound is of theoretical interest, but much too large to be useful in practice. In a similar way, following the above strategy one could give theoretical (but practically useless) upper bounds to detect when two Galois representations are equivalent.

3. Core-free subextensions

The matrix groups arising in the previous section are much too large to work with in practice. In this section, we find comparatively small extensions whose Galois closure give rise to the desired representations.

3.1. Core-free subgroups.

We begin with a condition that arises naturally in group theory and Galois theory.

Definition 3.1.1. Let G be a finite group. A subgroup $H \leq G$ is *core-free* if G acts faithfully on the cosets G/H.

Equivalently, $H \leq G$ is core-free if and only if $\bigcap_{g \in G} gHg^{-1} = \{1\}$. For example, the subgroup $\{1\}$ is core-free.

Definition 3.1.2. Let $K \supseteq F$ be a finite Galois extension of fields with $G = \mathrm{Gal}(K \mid F)$. A subextension $K \supseteq K_0 \supseteq F$ is *core-free* if $\mathrm{Gal}(K \mid K_0) \leq G$ is a core-free subgroup.

Lemma 3.1.3. *The subextension $K \supseteq K_0 \supseteq F$ is core-free if and only if K is the Galois closure of K_0 over F.*

Proof. Immediate. □

If $K \supseteq K_0 \supseteq F$ is a core-free subextension of $K \supseteq F$ with $K_0 = F(\alpha)$, then by definition the action of $\mathrm{Gal}(K \mid F)$ on the conjugates of α defines a faithful permutation representation, equivalent to its action on the left cosets of $\mathrm{Gal}(K \mid K_0)$.

We slightly augment the notion of core-free subextension for two-step extensions of fields, as follows.

Definition 3.1.4. Let

$$1 \to V \to E \xrightarrow{\pi} G \to 1 \tag{3.1.5}$$

be an exact sequence of finite groups. A core-free subgroup $D \leq E$ is *exact* (*relative to* (3.1.5)) if $\pi(D)$ is a core-free subgroup of G.

If $D \leq E$ is an exact core-free subgroup we let $H := \pi(D)$ and $W := V \cap D = \ker \pi|_D$, so there is an exact subsequence

$$1 \to W \to D \xrightarrow{\pi} H \to 1 \tag{3.1.6}$$

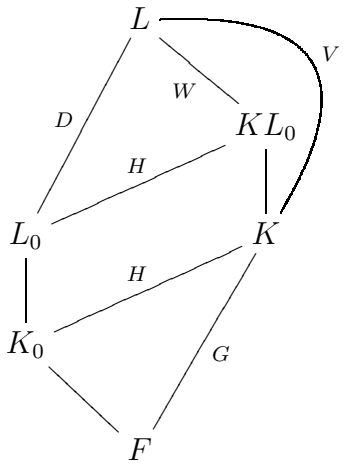
with both $D \leq E$ and $H \leq G$ core-free. (We do not assume that $W \leq V$ is core-free.)

Now let $L \supseteq K \supseteq F$ be a two-step Galois extension with $V := \mathrm{Gal}(L \mid K)$, $E := \mathrm{Gal}(L \mid F)$, $G := \mathrm{Gal}(K \mid F)$ and $\pi : E \to G$ the restriction, so we have an exact sequence as in (3.1.5).

Definition 3.1.7. We say $L_0 \supseteq K_0 \supseteq F$ is an *exact core-free subextension* of $L \supseteq K \supseteq F$ if $L_0 = L^D$ and $K_0 = K^{\pi(D)}$ where $D \leq E$ is an exact core-free subgroup.

Let $L_0 \supseteq K_0 \supseteq F$ be an exact core-free subextension of $L \supseteq K \supseteq F$, so that $\mathrm{Gal}(L \mid L_0) = D$. As above we let $H := \pi(D) = \mathrm{Gal}(K \mid K_0)$ and $W := V \cap D = \mathrm{Gal}(L \mid KL_0)$. By (3.1.6) we have $H \simeq D/W = \mathrm{Gal}(KL_0 \mid L_0)$, and we have the following field diagram:

(3.1.8)



By Lemma 3.1.3, L is the Galois closure of L_0 over F, and K is the Galois closure of K_0 over F. We read the diagram (3.1.8) as giving us a way to reduce the Galois theory of the extension $L \supseteq K \supseteq F$ to $L_0 \supseteq K_0 \supseteq F$: the larger we can make D, the smaller the extension $L_0 \supseteq K_0 \supseteq F$, and the better for working explicitly with the corresponding Galois groups.

3.2. **Application to Faltings–Serre.** We now specialize the preceding discussion to our case of interest; although working with core-free extensions does not improve the theoretical understanding, it is a crucial simplification in practice.

In Steps 2–3 of Algorithm 2.4.1, we are asked to enumerate obstructing pairs (L, φ) extending $(K, \overline{\rho})$, with $\varphi\colon \mathrm{Gal}(L \mid F) \hookrightarrow (\mathrm{Lie}(\mathrm{G}) \rtimes \mathrm{G})(\mathbb{F}_\ell)$.

Let $G := \mathrm{img}\,\overline{\rho} \leq \mathrm{G}(\mathbb{F}_\ell)$. Given (L, φ), the image of φ is a subgroup $E \leq \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell) \rtimes G$ with $\pi(E) = G$; letting $V := \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell) \cap E$ we have an exact sequence

$$1 \to V \to E \xrightarrow{\pi} G \to 1 \tag{3.2.1}$$

arising from (2.3.8).

So we enumerate the subgroups $E \leq \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell) \rtimes G$ with $\pi(E) = G$, up to conjugation by $\mathrm{M}_n(\mathbb{F}_\ell) \rtimes G$. The enumeration of these subgroups depends only on G, so it may be done as a precomputation step, independent of the representations.

For each such E, let D be an exact core-free subgroup relative to (3.2.1). We let $L_0 = L^D$ and $K_0 = K^{\pi(D)}$, hence $L_0 \supseteq K_0 \supseteq F$ is an exact core-free subextension of $L \supseteq K \supseteq F$ and we have the field diagram (3.1.8) where $H = \pi(D)$ and $W = V \cap D$ as before. Since V is abelian, $KL_0 \supseteq K$ is Galois and hence $L_0 \supseteq K_0$ is also Galois, with common abelian Galois group $\mathrm{Gal}(L_0 \mid K_0) \simeq \mathrm{Gal}(KL_0 \mid K) \simeq V/W$. So better than a Hunter search as in Lemma 2.2.1, we can use algorithmic class field theory (see Cohen [15, Chapter 4]) to enumerate the possible fields $L_0 \supseteq K_0$.

Accordingly, we modify Steps 2–3 of Algorithm 2.4.1 then as follows.

2′. Enumerate the subgroups $E \leq \mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell) \rtimes G$ with $\pi(E) = G$, up to conjugation by $\mathrm{M}_n(\mathbb{F}_\ell) \rtimes G$, such that $\mathrm{utr}(E) \not\equiv 0 \pmod{\ell}$. For each such subgroup E, perform the following steps.

a. Compute a set of representatives ξ of (outer) automorphisms of E such that ξ acts by an inner automorphism on G, modulo inner automorphisms by elements of $\mathrm{M}_n(\mathbb{F}_\ell) \rtimes G$.
b. Find an exact core-free subgroup $D \leq E$ and let W, H be as in (3.1.6).
c. Let $K_0 = K^H$ and use algorithmic class field theory to enumerate all possible extensions $L_0 \supseteq K_0$ unramified away from S such that $\mathrm{Gal}(L_0 \mid K_0) \simeq V/W$.

3′. For each extension L_0 from Step 2′c and for each E, perform the following steps.
a. Compute an isomorphism of groups $\varphi_0 \colon \mathrm{Gal}(L \mid F) \xrightarrow{\sim} E$ extending $\overline{\rho}$; if no such isomorphism exists, proceed to the next group E.
b. Looping over ξ computed in Step 2′a, let $\varphi := \xi \circ \varphi_0$, and record the pair (L, φ).

Proof of equivalence with Steps 2–3. We show that these steps enumerate all obstructing pairs (L, φ) up to equivalence.

Let L be an obstructing extension. For an obstructing extension φ of $\overline{\rho}$, the image $E = \operatorname{img} \varphi$ arises up to conjugation in the list computed in Step 2′; such conjugation gives an equivalent representation. So we may restrict our attention to the set Φ of obstructing extensions φ whose image is *equal* to E.

With respect to the core-free subgroup D, the field L arises as the Galois closure of the field $L_0 = L^D$, and so L_0 will appear in the list computed in Step 2′c. An exact core-free subgroup always exists as we can always take D the trivial group.

In Step 3′a, we compute one obstructing extension $\varphi_0 \in \Phi$. Any other obstructing extension $\varphi \in \Phi$ is of the form $\varphi = \xi \circ \varphi_0$ where ξ is an automorphism of E that induces an inner automorphism on G; when ξ arises from conjugation by an element of $\mathrm{Lie}(\mathrm{G})(\mathbb{F}_\ell) \rtimes G$, we obtain a representation equivalent to φ_0, so the representatives ξ computed in Step 2′a cover all possible extensions φ up to equivalence. □

We now explain in a bit more detail Steps 2′a and 3′a—in these steps, we need to understand how $\mathrm{Gal}(L \mid F)$ restricts to $\mathrm{Gal}(K \mid F)$ via its permutation representation. The simplest thing to do is just to ignore the conditions on ξ, i.e., in Step 2′a allow all outer automorphisms and in Step 3′a take any isomorphism of groups: *a fortiori*, we will still encounter every one satisfying the extra constraint. To nail it down precisely, we compute the group $\mathrm{Aut}(L_0 \mid F)$ of F-automorphisms of the field L_0, for each automorphism τ of order 2 compute the fixed field, until we find a field isomorphic to K_0: then $\mathrm{Gal}(K \mid F)$ is the stabilizer of $\{\beta, \tau(\beta)\}$, and so we can look up the indices of these roots in the permutation representation of $\mathrm{Gal}(L \mid F)$.

In the above, we may also use $\mathrm{Lie}^0(\mathrm{G})$ in place of $\mathrm{Lie}(\mathrm{G})$ if we are also given $\det \rho_1 = \det \rho_2$, by the discussion at the end of section 2.3.

3.3. **Computing conjugacy classes, in stages.** We now discuss Step 4 of Algorithm 2.4.1, where we are given (L, φ) and we are asked to find a witness prime. In theory, to accomplish this task we compute the conjugacy class of $\mathrm{Frob}_\mathfrak{p}$ in $\mathrm{Gal}(L \mid K)$ using an algorithm of Dokchitser–Dokchitser [19] and then calculate $\operatorname{utr} \varphi(\sigma)$ for any σ in this conjugacy class.

In practice, because of the enormity of the computation, we may not want to spend time computing the conjugacy class if we can get away with less. In particular, we would like to minimize the amount of work done per field. So we now describe in stages ways to find obstructing primes; each stage gives correct output, but in refining the previous stage we

may be able to find smaller primes. Each of these stages involves a precomputation step that only depends of the group-theoretic data.

In Step 2′ above, we enumerate subgroups E and identify an exact core-free subgroup D. We identify E with the permutation representation on the cosets E/D.

In Step 3′ above, we see the extension $L \supseteq K \supseteq F$ via a core-free extension $L_0 \supseteq K_0 \supseteq F$, and these fields are encoded by minimal polynomials of primitive elements. We may compute $\mathrm{Gal}(L \mid F)$ as a permutation group with respect to some numbering of the roots, and then insist that the isomorphism $\varphi_0 \colon \mathrm{Gal}(L \mid F) \xrightarrow{\sim} E$ computed in Step 3′a is an isomorphism of permutation representations.

For $\mathfrak{p} \notin S$, for the conjugacy class $\mathrm{Frob}_\mathfrak{p}$, the cycle type $c(\mathrm{Frob}_\mathfrak{p}, L_0)$ can be computed very quickly by factoring the minimal polynomial of L_0 modulo a power $\mathfrak{p}^k$ where it is separable (often but not always $k = 1$ suffices). This cycle type may not uniquely identify the conjugacy class, but we can try to find a cycle type which is *guaranteed* to be obstructing as follows.

4′. Perform the following steps.

a. For each group E computed in Step 2′ with core-free subgroup D, identify E with the permutation representation on the cosets E/D. For each ξ computed in Step 2′a for E, compute the set of cycle types

$$\mathrm{Obc}(E, \xi) := \{c(\xi(\gamma)) : \gamma \in E \text{ and } \mathrm{utr}\,\gamma \not\equiv 0 \pmod{\ell}\} \smallsetminus \{c(\xi(\gamma)) : \gamma \in E \text{ and } \mathrm{utr}\,\gamma \equiv 0 \pmod{\ell}\}.$$

b. For each field (L, φ), with L encoded by the core-free subfield L_0 and $\varphi \leftrightarrow \xi$ as computed in Step 3′b, find a prime $\mathfrak{p}$ such that $c(\mathrm{Frob}_\mathfrak{p}, L_0) \in \mathrm{Obc}(E, \xi)$.

In computing $\mathrm{Obc}(E, \xi)$, of course it suffices to restrict to γ in a set of conjugacy classes for E.

Step 4′ gives correct output because the set of cycle types in $\mathrm{Obc}(E, \xi)$ are precisely those for which *every* conjugacy class in E with the given cycle type is obstructing. It is the simplest version, and it is the quickest to compute provided that $\mathrm{Obc}(E, \xi)$ is nonempty.

Remark 3.3.1. In Step 4′a, there may be a cycle type which arises in two ways, from $\gamma, \gamma' \in E$, with $\mathrm{utr}\,\gamma \not\equiv 0 \pmod{\ell}$ and $\mathrm{utr}\,\gamma' \equiv 0 \pmod{\ell}$; such a cycle type is not guaranteed to be obstructing.

Remark 3.3.2. In a situation where there are many outer automorphisms ξ to consider, it may be more efficient (but give potentially larger primes and possibly fail more often) to work with the set

$$\mathrm{Obc}(E) := \bigcap_{\xi} \mathrm{Obc}(E, \xi) \tag{3.3.3}$$

consisting of cycle types with the property that every conjugacy class in E under *every* outer automorphism ξ is obstructing. In this setting, in Step 4′b, we can loop over just the fields L and look for $\mathfrak{p}$ with $c(\mathrm{Frob}_\mathfrak{p}) \in \mathrm{Obc}(E)$.

In the next stage, we seek to combine also cycle type information from $\mathrm{Gal}(K \mid F)$, arising as a permutation group from the field K_0. Via the isomorphism $\varphi \colon \mathrm{Gal}(L \mid F) \xrightarrow{\sim} E$ and the construction of the core-free extension, as a permutation group $\mathrm{Gal}(L \mid F)$ is isomorphic to the permutation representation of E on the cosets of D. (The numbering might be different, but there is a renumbering for which the representations are equal.) In the same way, the

group $\mathrm{Gal}(K \mid F)$ is isomorphic as a permutation group to the permutation representation of $\pi(E) = G$ on the cosets of the subgroup $\pi(D) = H$, where $\pi\colon E \to G$ is the projection. So we have the following second stage.

4″. Perform the following steps.

a. For each group E computed in Step 2′ and each ξ computed in Step 2′a for E, compute the set of pairs of cycle types

$$\mathrm{Obc}(E, G, \xi) := \{(c(\xi(\gamma)), c(\pi(\gamma))) : \gamma \in E \text{ and } \operatorname{utr}\gamma \not\equiv 0 \pmod{\ell}\} \smallsetminus \{(c(\xi(\gamma)), c(\pi(\gamma))) : \gamma \in E \text{ and } \operatorname{utr}\gamma \equiv 0 \pmod{\ell}\}.$$

b. For each field (L, φ), with L encoded by L_0 and $\varphi \leftrightarrow \xi$, find a prime $\mathfrak{p}$ such that

$$(c(\mathrm{Frob}_{\mathfrak{p}}, L_0), c(\mathrm{Frob}_{\mathfrak{p}}, K_0)) \in \mathrm{Obc}(E, G, \xi).$$

Step 4″ works for the same reason as in Step 4′: the cycle type pairs in $\mathrm{Obc}(E, G, \xi)$ are precisely those for which every conjugacy class in E with the given pair of cycle types is obstructing. The precomputation is a bit more involved in this case, but the check for each field is still extremely fast.

Remark 3.3.4. Instead of the cycle type, a weaker alternative to Step 4″ would be to record the order of $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Gal}(K \mid F)$.

Remark 3.3.5. Assuming that $\operatorname{tr}\overline{\rho}(\mathrm{Frob}_p)$ can be computed efficiently, one additional piece of data that may be appended to the pair of cycle types is $\operatorname{tr}\overline{\rho}(\gamma)$.

Remark 3.3.6. If L arises from several different choices of core-free subgroup, then these subgroups give different (but conjugate) fields L_0. Because we are not directly accessing the conjugacy class above, but only cycle type information, it is possible that replacing L_0 by a conjugate field will give smaller witnesses. In other words, in Step 4′b or 4″b above, we could loop over the core-free subgroups D and take the smallest witness among them.

Finally, we may go all the way and compute conjugacy classes. Write $[\gamma]_E$ for the conjugacy class of a group element $\gamma \in E$.

4‴. Perform the following steps.

a. For each group E computed in Step 2′ and each ξ computed in Step 2′a for E, compute the set of obstructing conjugacy classes

$$\mathrm{Ob}(E, \xi) := \{[\gamma]_E : \gamma \in E \text{ and } \operatorname{utr}\gamma \not\equiv 0 \pmod{\ell}\}$$

b. For each field (L, φ), with L encoded by L_0 and $\varphi \leftrightarrow \xi$, find a prime $\mathfrak{p}$ such that $\mathrm{Frob}_{\mathfrak{p}} \in \mathrm{Ob}(E, G, \xi)$.

We now explain some examples in detail which show the difference between these stages.

Example 3.3.7. Anticipating one of our three core cases, we consider $\mathrm{G} = \mathrm{GSp}_4$ and $\ell = 2$ over $F = \mathbb{Q}$. (The reader may wish to skip ahead and read sections 4–5 to read the details of the setup, but this example is still reasonably self-contained.) We consider the case of a residual representation with image $G = S_5(b) \leq \mathrm{GSp}_4(\mathbb{F}_2)$ (see (5.1.8)), and then a subgroup $E \leq \mathsf{sp}_4 \rtimes G$ with $\dim_{\mathbb{F}_2} V = 10$. We find a core-free subgroup D where $\#H = 10$ and $[V : W] = 2$.

We compute in Step 2′a that we need to consider 8 automorphisms ξ, giving rise to 8 homomorphisms φ. With respect to one such ξ, we find that there are 48 conjugacy classes

that are obstructing. Among these, computing as in Step 4′a, we find that 17 are recognized by their L_0-cycle type:

$$\begin{aligned}\mathrm{Obc}(E;\xi) = \{&3^6 2^1, 4^1 2^4 1^8, 4^1 2^5 1^6, 4^3 1^8, 4^3 2^1 1^6, 6^1 3^4 2^1,\\ &8^1 4^2 2^2, 8^1 4^3, 10^2, 12^1 3^2 2^1, 12^1 6^1 2^1\}.\end{aligned} \tag{3.3.8}$$

If instead we call Step 4″a, we find that $35 = \#\,\mathrm{Obc}(E, G, \xi)$ are recognized by the pair of L_0, K_0-cycle types (and 22 recognized by L_0-cycle type and K_0-order). This leaves 13 conjugacy classes that cannot be recognized purely by cycle type considerations, for which Step 4‴ would be required.

For the other choices of ξ, we obtain similar numbers but different cycle types. If we restrict to just L_0-cycle types that work for *all* such as in Remark 3.3.2, we are reduced to a set of 8:

$$\mathrm{Obc}(E) = \{4^1 2^4 1^8, 4^1 2^5 1^6, 4^3 1^8, 4^3 2^1 1^6, 6^1 3^4 2^1, 8^1 4^2 2^2, 8^1 4^3, 10^2\}. \tag{3.3.9}$$

To see how this plays out with respect to the sizes of primes, we work with the field K arising as the Galois closure of $K_0 = K^H$ defined by a root of the polynomial

$$x^{10} + 3x^9 + x^8 - 10x^7 - 17x^6 - 7x^5 + 11x^4 + 18x^3 + 13x^2 + 5x + 1$$

and similarly $L_0 = L^D$ by a root of

$$x^{20} + 3x^{18} + 5x^{16} + 2x^{14} - 5x^{12} - 13x^{10} - 13x^8 - 6x^6 + x^4 + x^2 - 1.$$

If we restrict to the cycle types in (3.3.8) (or (3.3.9)), we obtain the multiset of witnesses $\{5, 5, 5, 5, 23, 23, 29, 29\}$. If we work with $\mathrm{Obc}(E, G, \xi)$, we find $\{5, 5, 5, 5, 19, 19, 23, 23\}$ instead; the difference is two cases where the witness $p = 29$ is replaced by $p = 19$, so we dig a bit deeper into one of these two cases.

In L_0, the factorization pattern of 19 is $6^2 3^2 2^1$. But apparently we cannot be guaranteed to have $\mathrm{utr}(\mathrm{Frob}_p) \equiv 1 \pmod 2$ just looking at cycle type. Indeed, there are three conjugacy classes with this cycle type: one of order 1280 and two of order 2560, represented by the permutations

$$\begin{aligned}&(1\,9\,18)(2\,15\,6\,12\,5\,16)(3\,20\,7\,13\,10\,17)(4\,14)(8\,11\,19),\\ &(1\,19\,8\,11\,9\,18)(2\,15\,6\,12\,5\,16)(3\,20\,17)(4\,14)(7\,13\,10),\\ &(1\,10\,2\,3\,8\,4)(5\,9\,6)(7\,17)(11\,20\,12\,13\,18\,14)(15\,19\,16)\end{aligned}$$

in S_{20} mapping respectively to the matrices

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

So precisely the first two conjugacy classes have upper trace 1 and are obstructing, whereas the third has upper trace 0 and is not obstructing. So by cycle types in L_0 alone, indeed, we cannot proceed.

But we recover using the K_0-cycle type. For the obstructing classes, the cycle type in the permutation representation of G is $3^3 1^1$, whereas for the nonobstructing class the cycle type is $6^1 3^1 1^1$. We compute that the factorization pattern for 19 in K_0 is type $3^3 1^1$, which means 19 belongs to an obstructing class. If we go all the way to the end, we can compute that the conjugacy class of Frob_{19} in fact belongs to the second case.

4. Abelian surfaces, paramodular forms, and Galois representations

We pause now to set up notation and input from the theory of abelian surfaces, paramodular forms, and Galois representations in our case of interest.

4.1. **Galois representations from abelian surfaces.** Let A be a polarized abelian variety over $\mathbb{Q}$. For example, if X is a nice (smooth, projective, geometrically integral) genus g curve over $\mathbb{Q}$, then its Jacobian $\operatorname{Jac} X$ with its canonical principal polarization is a principally polarized abelian variety over $\mathbb{Q}$ of dimension g. Let $N := \operatorname{cond}(A)$ be the conductor of A. We say A is *typical* if $\operatorname{End}(A^{\mathrm{al}}) = \mathbb{Z}$, where $A^{\mathrm{al}} := A_{\mathbb{Q}^{\mathrm{al}}}$ is the base change of A to $\mathbb{Q}^{\mathrm{al}}$.

Lemma 4.1.1. *Let A be a simple, semistable abelian surface over $\mathbb{Q}$ with nonsquare conductor. Then A is typical.*

Proof. By Albert's classification, either $\operatorname{End}(A) = \mathbb{Z}$ or $\operatorname{End}(A)$ is an order in a quadratic field. In the latter case, $\operatorname{cond}(A)$ is a square by the conductor formula (see Brumer–Kramer [7, Lemma 3.2.9]), a contradiction. Therefore $\operatorname{End}(A) = \mathbb{Z}$. Since A is semistable, all endomorphisms of A^{al} are defined over $\mathbb{Q}$ by a result of Ribet [47, Corollary 1.4]. Thus $\operatorname{End}(A^{\mathrm{al}}) = \operatorname{End}(A) = \mathbb{Z}$, and A is typical. □

Lemma 4.1.2. *An abelian surface over $\mathbb{Q}$ of prime conductor is typical.*

Proof. If A is not simple over $\mathbb{Q}$, then we have any isogeny $A \sim A_1 \times A_2$ over $\mathbb{Q}$ to the product of abelian varieties A_1, A_2 over $\mathbb{Q}$, and $\operatorname{cond}(A) = \operatorname{cond}(A_1)\operatorname{cond}(A_2)$. But since A is prime, without loss of generality $\operatorname{cond}(A_1) = 1$, contradicting the result of Fontaine [22] that there is no abelian variety over $\mathbb{Q}$ with everywhere good reduction. Therefore A is simple over $\mathbb{Q}$. Since $N = \operatorname{cond}(A)$ is prime, A is semistable at N, and the result then follows from Lemma 4.1.1. □

From now on, suppose that $g = 2$ and A is a polarized abelian surface over $\mathbb{Q}$. Let ℓ be a prime with $\ell \nmid N$ and ℓ coprime to the degree of the polarization on A. Let S be a finite set of places of $\mathbb{Q}$ containing ℓ, ∞ and the primes of bad reduction of A. Let

$$\chi_\ell \colon \operatorname{Gal}_{\mathbb{Q},S} \to \mathbb{Z}_\ell^\times$$

denote the ℓ-adic cyclotomic character, so that $\chi_\ell(\operatorname{Frob}_p) = p$. Then the action of $\operatorname{Gal}_{\mathbb{Q}}$ on the ℓ-adic Tate module

$$T_\ell(A) := \varprojlim_n A[\ell^n] \simeq \mathrm{H}^1_{\text{ét}}(A, \mathbb{Z}_\ell)^\vee \simeq \mathbb{Z}_\ell^4$$

(where $A[\ell^n]$ denotes the ℓ^n-torsion of A) provides a continuous Galois representation

$$\rho_{A,\ell} \colon \operatorname{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(\mathbb{Z}_\ell) \tag{4.1.3}$$

with determinant χ_ℓ^2 and similitude character χ_ℓ that is unramified outside ℓN. We may reduce the representation (4.1.3) modulo ℓ to obtain a residual representation

$$\overline{\rho}_{A,\ell} \colon \operatorname{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(\mathbb{F}_\ell),$$

which can be concretely understood via the Galois action on the field $\mathbb{Q}(A[\ell])$.

For a prime $p \neq \ell$, slightly more generally we define

$$L_p(A, T) := \det(1 - T \operatorname{Frob}_p^* \mid \mathrm{H}^1_{\text{ét}}(A^{\mathrm{al}}, \mathbb{Q}_\ell)^{I_p}) \tag{4.1.4}$$

where Frob_p^* is the geometric Frobenius automorphism, $I_p \leq \mathrm{Gal}_{\mathbb{Q},S}$ is an inertia group at p, and the definition is independent of the auxiliary prime $\ell \neq p$ (by the semistable reduction theorem of Grothendieck [29, Exp. IX, Théorème 4.3(b)]). In particular, when $p \nmid \ell N$, we have

$$\det(1 - \rho_{A,\ell}(\mathrm{Frob}_p)T) = L_p(A,T) = 1 - a_pT + b_{p^2}T^2 - pa_pT^3 + p^2T^4 \in 1 + T\mathbb{Z}[T]. \tag{4.1.5}$$

Moreover, if $A = \mathrm{Jac}\, X$ and p does not divide the minimal discriminant Δ of X, then

$$Z(X \bmod p, T) := \exp\left(\sum_{r=1}^{\infty} \#X(\mathbb{F}_{p^r})\frac{T^r}{r}\right) = \frac{L_p(A,T)}{(1-T)(1-pT)}$$

so the polynomials $L_p(A,T)$ may be efficiently computed by counting points on X over finite fields. We define

$$L(A,s) := \prod_p L_p(A, p^{-s})^{-1}; \tag{4.1.6}$$

this series converges for $s \in \mathbb{C}$ in a right half-plane.

4.2. **Paramodular forms.** We follow Freitag [23] for the theory of Siegel modular forms. Let $\mathcal{H}_2 \subset \mathrm{M}_2(\mathbb{C})$ be the Siegel upper half-space. We write matrices $M = \left(\begin{smallmatrix} A & B \\ C & D \end{smallmatrix}\right) \in \mathrm{GL}_4(\mathbb{R})$ as block matrices, in particular $J := \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right) \in \mathrm{GL}_4(\mathbb{R})$ as usual. We write $^{\mathsf{T}}$ for the transpose. Define

$$\mathrm{GSp}_4^+(\mathbb{R}) := \{M \in \mathrm{GL}_4(\mathbb{R}) : M^{\mathsf{T}}JM = \mu J \text{ for some } \mu \in \mathbb{R}_{>0}\}.$$

For $M \in \mathrm{GSp}_4^+(\mathbb{R})$, we have $\mu = \det(M)^{1/2} > 0$.

For a holomorphic function $f\colon \mathcal{H}_2 \to \mathbb{C}$ and $M \in \mathrm{GSp}_4^+(\mathbb{R})$ and $k \in \mathbb{Z}_{\geq 0}$, we define the classical slash

$$(f \mid_k M)(Z) := \mu^{2k-3} \det(CZ + D)^{-k} f((AZ + B)(CZ + D)^{-1}). \tag{4.2.1}$$

Let $\Gamma \leq \mathrm{Sp}_4(\mathbb{R})$ be a subgroup commensurable with $\mathrm{Sp}_4(\mathbb{Z})$. We denote by

$$M_k(\Gamma) := \{f\colon \mathcal{H}_2 \to \mathbb{C} : (f \mid_k \gamma)(Z) = f(Z) \text{ for all } \gamma \in \Gamma\}$$

the $\mathbb{C}$-vector space of Siegel modular forms with respect to Γ, and $S_k(\Gamma) \subseteq M_k(\Gamma)$ the subspace of forms vanishing at the cusps of Γ, called the space of cuspforms.

To each double coset $\Gamma M \Gamma$ with $M \in \mathrm{GSp}_4^+(\mathbb{Q}) := \mathrm{GSp}_4(\mathbb{Q}) \cap \mathrm{GSp}_4^+(\mathbb{R})$, we define the *Hecke operator*

$$\mathrm{T}(\Gamma M \Gamma)\colon M_k(\Gamma) \to M_k(\Gamma) \tag{4.2.2}$$

as follows: from a decomposition $\Gamma M \Gamma = \bigsqcup_j \Gamma M_j$ of the double coset into disjoint single cosets, we define $f \mid_k \mathrm{T}(\Gamma M \Gamma) = \sum_j f \mid_k M_j$. The action is well-defined, depending only on the double coset, and $\mathrm{T}(\Gamma M \Gamma)$ maps $S_k(\Gamma)$ to $S_k(\Gamma)$.

Let $N \in \mathbb{Z}_{\geq 1}$. The *paramodular group* $K(N)$ of level N in degree two is defined by

$$K(N) := \begin{pmatrix} \mathbb{Z} & N\mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ \mathbb{Z} & \mathbb{Z} & \mathbb{Z} & N^{-1}\mathbb{Z} \\ \mathbb{Z} & N\mathbb{Z} & \mathbb{Z} & \mathbb{Z} \\ N\mathbb{Z} & N\mathbb{Z} & N\mathbb{Z} & \mathbb{Z} \end{pmatrix} \cap \mathrm{Sp}_4(\mathbb{Q}). \tag{4.2.3}$$

The paramodular group $K(N)$ has a normalizing *paramodular Fricke involution*, $\mu_N \in \mathrm{Sp}_4(\mathbb{R})$, given by

$$\mu_N = \begin{pmatrix} (F_N^{-1})^{\mathsf{T}} & 0 \\ 0 F_N & \end{pmatrix},$$

where $F_N = \frac{1}{\sqrt{N}}\left(\begin{smallmatrix} 0 & 1 \\ -N & 0 \end{smallmatrix}\right)$ is the Fricke involution for $\Gamma_0(N)$. Consequently, for all k we may decompose

$$M_k(K(N)) = M_k(K(N))^+ \oplus M_k(K(N))^- \tag{4.2.4}$$

into plus and minus μ_N-eigenspaces.

Write $e(z) = \exp(2\pi\sqrt{-1}z)$ for $z \in \mathbb{C}$. The Fourier expansion of $f \in M_k(K(N))$ is

$$f(Z) = \sum_{T \geq 0} a(T; f) e(\mathrm{tr}(TZ)) \tag{4.2.5}$$

for $Z \in \mathcal{H}_2$ and the sum over semidefinite matrices

$$T = \begin{pmatrix} n & r/2 \\ r/2 & Nm \end{pmatrix} \in \mathrm{M}_2^{\mathrm{sym}}(\mathbb{Q})_{\geq 0} \text{ with } n, r, m \in \mathbb{Z}.$$

For a subring $R \subseteq \mathbb{C}$, we denote by

$$M_k(K(N), R) := \{f \in M_k(K(N)) : a(T; f) \in R \text{ for all } T \geq 0\} \tag{4.2.6}$$

the R-module of paramodular forms whose Fourier coefficients all lie in R, and similarly we write $S_k(K(N), R)$ for cusp forms and $S_k(K(N), R)^{\pm}$ for the eigenspaces under the Fricke involution. The ring of paramodular forms with coefficients in R

$$M(K(N), R) := \bigoplus_{k=0}^{\infty} M_k(K(N), R)$$

is a graded R-algebra.

For a prime $p \nmid N$, the first (more familiar) Hecke operator we will use is

$$T(p) := \mathrm{T}(K(N)\,\mathrm{diag}(1, 1, p, p)K(N)) \tag{4.2.7}$$

whose decomposition into left cosets is given by

$$\begin{aligned} &K(N)\,\mathrm{diag}(1,1,p,p)K(N) \\ &\quad = K(N)\begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p & 0 & 0 \\ & & 1 & 0 \\ & & 0 & 1 \end{pmatrix} + \sum_{i \bmod p} K(N)\begin{pmatrix} 1 & 0 & i & 0 \\ 0 & p & 0 & 0 \\ & & p & 0 \\ & & 0 & 1 \end{pmatrix} \\ &\qquad + \sum_{i,j \bmod p} K(N)\begin{pmatrix} p & 0 & 0 & 0 \\ i & 1 & 0 & j \\ & & 1 & -i \\ & & 0 & p \end{pmatrix} + \sum_{i,j,k \bmod p} K(N)\begin{pmatrix} 1 & 0 & i & j \\ 0 & 1 & j & k \\ & & p & 0 \\ & & 0 & p \end{pmatrix} \end{aligned} \tag{4.2.8}$$

with indices taken over residue classes modulo p. Writing $T[u] = u^{\mathsf{T}} T u$ for $T, u \in \mathrm{M}_2(\mathbb{Q})$, the action of $T(p)$ on Fourier coefficients $a(T; f)$ is given by

$$\begin{aligned} a(T; f \mid_k T(p)) = a(pT; f) + p^{k-2} \sum_{j \bmod p} a\left(\frac{1}{p} T \begin{bmatrix} 1 & 0 \\ j & p \end{bmatrix}; f\right) \\ + p^{k-2} a\left(\frac{1}{p} T \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}; f\right) + p^{2k-3} a\left(\frac{1}{p} T; f\right). \end{aligned} \tag{4.2.9}$$

Hence for $k \geq 2$, the Hecke operator $T(p)$ stabilizes $S_k(K(N), R)$. In particular, taking $R = \mathbb{Z}$ we see that if f has integral Fourier coefficients, then $f \mid_k T(p)$ has integral Fourier coefficients for $k \geq 2$.

We will also make use of another, perhaps less familiar, Hecke operator. For $K(N)$ and a prime $p \nmid N$, we define

$$T_1(p^2) = \mathrm{T}(K(N) \operatorname{diag}(1, p, p^2, p) K(N)). \tag{4.2.10}$$

Lemma 4.2.11. *The coset decomposition for $T_1(p^2)$ is given by:*

$$\begin{aligned} &K(N) \operatorname{diag}(1, p, p^2, p) K(N) \\ &= K(N) \begin{pmatrix} p & 0 & 0 & 0 \\ 0 & p^2 & 0 & 0 \\ & & p & 0 \\ & & 0 & 1 \end{pmatrix} + \sum_{i \bmod p} K(N) \begin{pmatrix} p^2 & 0 & 0 & 0 \\ pi & p & 0 & 0 \\ & & 1 & -i \\ & & 0 & p \end{pmatrix} \\ &\quad + \sum_{i \not\equiv 0 \bmod p} K(N) \begin{pmatrix} p & 0 & i & 0 \\ 0 & p & 0 & 0 \\ & & p & 0 \\ & & 0 & p \end{pmatrix} + \sum_{\substack{i \bmod p, \\ j \not\equiv 0 \bmod p}} K(N) \begin{pmatrix} p & 0 & i^2 j & ij \\ 0 & p & ij & j \\ & & p & 0 \\ & & 0 & p \end{pmatrix} \\ &\quad + \sum_{\substack{i \bmod p, \\ j \bmod p^2}} K(N) \begin{pmatrix} 1 & 0 & j & i \\ 0 & p & pi & 0 \\ & & p^2 & 0 \\ & & 0 & p \end{pmatrix} + \sum_{\substack{i,j \bmod p, \\ k \bmod p^2}} K(N) \begin{pmatrix} p & 0 & 0 & pj \\ i & 1 & j & k \\ & & p & -pi \\ & & 0 & p^2 \end{pmatrix} \end{aligned} \tag{4.2.12}$$

Proof. The cosets are from Roberts–Schmidt [50, (6.6)] after swapping rows one and two and columns one and two, applying an inverse, and multiplying by the similitude p^2. □

Define the indicator function $\mathbf{1}(p \mid y)$ by 1 if $p \mid y$ and by 0 if $p \nmid y$. Then the action of $T_1(p^2)$ on the Fourier coefficients is:

$$\begin{aligned} a(T; f \mid_k T_1(p^2)) = p^{k-3} \sum_{x \bmod p} a(T \begin{bmatrix} 1 & 0 \\ x & p \end{bmatrix}; f) + p^{k-3} a\left(T \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}; f\right) \\ + p^{3k-6} \sum_{j \bmod p} a\left(\frac{1}{p^2} T \begin{bmatrix} 1 & 0 \\ j & p \end{bmatrix}; f\right) + p^{3k-6} a\left(\frac{1}{p^2} T \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}; f\right) \\ + p^{2k-6} \left(p \, \mathbf{1}\left(p \mid T \begin{bmatrix} 1 \\ 0 \end{bmatrix}\right) - 1\right) a(T; f) \\ + p^{2k-6} \sum_{\lambda \bmod p} \left(p \, \mathbf{1}\left(p \mid T \begin{bmatrix} \lambda \\ 1 \end{bmatrix}\right) - 1\right) a(T; f). \end{aligned} \tag{4.2.13}$$

Hence for $k \geq 3$, the Hecke operator $T_1(p^2)$ stabilizes $S_k(K(N), R)$. In particular, if f has integral Fourier coefficients, then $f|_k T_1(p^2)$ has integral Fourier coefficients for $k \geq 3$. However, for $k = 2$, we only know that $p^2 f|_k T_1(p^2)$ is integral when f is (and there are examples where $f|_2 T_1(p^2)$ has p^2 in the denominator of some Fourier coefficients).

Summarizing the above, we have:

$$\begin{aligned} T(p) &= \mathrm{T}(K(N)\,\mathrm{diag}(1,1,p,p)K(N)); \qquad \deg T(p) = (1+p)(1+p^2) \\ T_1(p^2) &= \mathrm{T}(K(N)\,\mathrm{diag}(1,p,p^2,p)K(N)); \quad \deg T_1(p^2) = (1+p)(1+p^2)p. \end{aligned} \tag{4.2.14}$$

We define two new operators:

$$\begin{aligned} T_2(p^2) &:= \mathrm{T}(K(N)\,\mathrm{diag}(p,p,p,p)K(N)) = p^{2k-6}\mathrm{id} \\ B(p^2) &:= p(T_1(p^2) + (1+p^2)T_2(p^2)) \end{aligned} \tag{4.2.15}$$

If f is an eigenform of weight k for the operators $T(p)$ and $T_1(p^2)$, with corresponding eigenvalues $a_p(f), a_{1,p^2}(f) \in \mathbb{C}$, then f is an eigenform for the operator $B(p^2)$ with eigenvalue

$$b_{p^2}(f) := p\, a_{1,p^2}(f) + p^{2k-5}(1+p^2). \tag{4.2.16}$$

Lemma 4.2.17. *If $k = 2$ and f has integral Fourier coefficients, then $b_{p^2}(f) \in \mathbb{Z}$.*

Proof. We have observed that $p^2 a_{1,p^2}(f) \in \mathbb{Z}$. From 4.2.13, we observe the congruence

$$p^2(f|_2 T_1(p^2)) = p^2 a_{1,p^2}(f) f \equiv -f \pmod{p}.$$

so $p \mid (p^2 a_{1,p^2}(f) + 1)$. Therefore

$$b_{p^2}(f) = p\, a_{1,p^2}(f) + (1+p^2)/p = (p^2 a_{1,p^2}(f) + 1)/p + p \in \mathbb{Z}. \qquad \square$$

Following Roberts–Schmidt [49, 50], to f we then assign the *spinor Euler factor* at $p \nmid N$ in the arithmetic normalization by

$$Q_p(f,T) := 1 - a_p(f)T + b_{p^2}(f)T^2 - p^{2k-3}a_p(f)T^3 + p^{4k-6}T^4 \in 1 + T\mathbb{C}[T]. \tag{4.2.18}$$

We will also call $Q_p(f,T)$ the *spinor Hecke polynomial* at p. If f has integral Fourier coefficients, then by Lemma 4.2.17 we have $Q_p(f,T) \in 1 + T\mathbb{Z}[T]$.

4.3. **Galois representations from Siegel modular forms.** We now seek to match the Galois representation coming from an abelian surface with one coming from an automorphic form. In this section, we explain the provenance of the latter.

We follow the presentation of Schmidt [51] for the association of an automorphic representation to a paramodular eigenform. Let $\Gamma \leq \mathrm{GSp}_4(\mathbb{Q})^+$ be a subgroup commensurable with $\mathrm{Sp}_4(\mathbb{Z})$ and let $f \in S_k(\Gamma)$ be a cuspidal eigenform at all but finitely many places. In general, the representation π_f generated by the adelization of f may be reducible and hence not an automorphic representation at all. It is still possible however, to associate a global Arthur parameter for $\mathrm{GSp}_4(\mathbb{A})$ to f as follows. Because f is cuspidal, the representation π_f decomposes as the direct sum of a finite number of automorphic representations, and each summand has the same global Arthur parameter among one of six types: the general type **(G)**, the Yoshida type **(Y)**, the finite type **(F)**, or types **(P)**, **(Q)** or **(B)** named after parabolic subgroups. Thus we may associate a global Arthur parameter directly to a paramodular eigenform f. The only type of global Arthur parameter that concerns us here is type **(G)** given by the formal tensor $\mu \boxtimes 1$, where μ is a cuspidal, self-dual, symplectic, unitary, automorphic representation of $\mathrm{GL}_4(\mathbb{A})$ and 1 is the trivial representation of $\mathrm{SU}_2(\mathbb{A})$.

Remark 4.3.1. One can consider the eigenforms of type **(G)** to be those that *genuinely* belong on GSp_4.

Second, when f is of type **(G)** or **(Y)**, the associated representation π_f is irreducible and f is necessarily an eigenform at all good primes. Third, the type of f may be determined by checking *one* Euler factor at a good prime. We state the paramodular case $\Gamma = K(N)$.

Proposition 4.3.2 (Schmidt)**.** *Let $f \in S_k(K(N))$ be a cuspidal eigenform for all primes $p \nmid N$. Let $p \nmid N$ be prime and let $Q_p(f,T)$ be the Hecke polynomial of f at p defined in (4.2.18) in the arithmetic normalization. Then f is of type* **(G)** *if and only if all reciprocal roots of $Q_p(f,T)$ have complex absolute value $p^{k-\frac{3}{2}}$.*

Proof. Converting from analytic to arithmetic normalization, by Schmidt [51, Proposition 2.1] the stated local factor condition implies that f is of type **(G)** or **(Y)**, but paramodular cusp forms cannot be type **(Y)** also by Schmidt [51, Lemma 2.5]. □

Fourth, continuing in the paramodular case $\Gamma = K(N)$, the global conductor of π_f divides N, and is equal to N if and only if f is a newform. Finally, if f is a newform—see Roberts–Schmidt [49] for the global newform theory of paramodular forms—then f is a Hecke eigenform at all primes and for all paramodular Atkin-Lehner involutions.

We need one final bit of notation, concerning archimedian L-parameters. The real Weil group is $W(\mathbb{R}) = \mathbb{C}^\times \cup \mathbb{C}^\times j$, with $j^2 = -1$ and $jzj^{-1} = \bar{z}$ for $z \in \mathbb{C}^\times$. For $w, m_1, m_2 \in \mathbb{Z}$ with $m_1 > m_2 \geq 0$ and $w + 1 \equiv m_1 + m_2 \pmod 2$, we define the *archimedean L-parameter* $\phi(w, m_1, m_2)\colon W(\mathbb{R}) \to \mathrm{GSp}_4(\mathbb{R})$ by sending $z \in \mathbb{C}^\times$ to the diagonal matrix

$$|z|^{-w} \operatorname{diag}\left(\left(\frac{z}{\bar{z}}\right)^{\frac{m_1+m_2}{2}}, \left(\frac{z}{\bar{z}}\right)^{\frac{m_1-m_2}{2}}, \left(\frac{z}{\bar{z}}\right)^{\frac{m_2-m_1}{2}}, \left(\frac{z}{\bar{z}}\right)^{\frac{-(m_1+m_2)}{2}} \right) \tag{4.3.3}$$

and j to the antidiagonal matrix $\operatorname{antidiag}((-1)^{w+1}, (-1)^{w+1}, 1, 1)$. The archimedean L-packet of $\mathrm{GSp}_4(\mathbb{R})$ corresponding to $\phi(w, m_1, m_2)$ has two elements, one holomorphic and one generic: for $m_2 > 0$ these are both discrete series representations, whereas for $m_2 = 0$ they are limits of discrete series.

We are now ready to associate a Galois representation to a paramodular eigenform of type **(G)**.

Theorem 4.3.4 (Taylor–Laumon–Weissauer–Schmidt–Mok)**.** *Let $f \in S_k(K(N))$ be a Siegel paramodular newform of weight $k \geq 2$ and level N. Suppose that f is of type* **(G)***. Then for any prime $\ell \nmid N$, there exists a continuous, semisimple Galois representation*

$$\rho_{f,\ell}\colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GSp}_4(\mathbb{Q}_\ell^{\mathrm{al}})$$

with the following properties:

(i) $\det(\rho_{f,\ell}) = \chi_\ell^{4k-6}$;
(ii) *The similitude character of $\rho_{f,\ell}$ is χ_ℓ^{2k-3};*
(iii) *$\rho_{f,\ell}$ is unramified outside ℓN;*
(iv) $\det(1 - \rho_{f,\ell}(\mathrm{Frob}_p)T) = Q_p(f,T)$ *for all $p \nmid \ell N$; and*
(v) *The local Langlands correspondence holds for all primes $p \neq \ell$, up to semisimplification.*

By (v), we mean that the Weil–Deligne representations associated to the restriction of the Galois representation $\rho_{f,\ell}$ to $\mathrm{Gal}(\mathbb{Q}_p^{\mathrm{al}} \mid \mathbb{Q}_p)$ agrees with that associated to the $\mathrm{GL}_n(\mathbb{Q}_p)$-representation π_p attached by the local Langlands correspondence up to semisimplification *without* information about the nilpotent operator N: in the notation of Taylor–Yoshida [57, p. 468] we mean $(V, r, N)^{\mathrm{ss}} = (V, r^{\mathrm{ss}}, 0)$.

Proof. The existence and properties (i)–(ii) follow from the construction and an argument of Taylor [56, Example 1, section 1.3]. Properties (iii) and (iv) are provided by Berger–Klosin [2, Theorem 8.2] (they claim in the subsequent Remark 8.3 that the result is "well-known").

We now sketch the construction, and we use the argument of Mok to conclude also property (v). By the discussion above, following Schmidt [51], we may attach to f a cuspidal automorphic representation Π_f of $\mathrm{GSp}_4(\mathbb{A})$ of type **(G)**. The hypothesis that f is of type **(G)** assures that the automorphic representation Π_f is irreducible. If $k \geq 3$, then the automorphic representation is of cohomological type, and from a geometric construction we obtain a Galois representation $\rho_{f,\ell} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GSp}_4(E)$ by work of Laumon [40] and Weissauer [59, Theorems I and IV], where E is the finite extension of $\mathbb{Q}_\ell$ containing the Hecke eigenvalues of f (choosing an isomorphism between the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and in $\mathbb{Q}_\ell^{\mathrm{al}}$): one shows that the representation takes values in $\mathrm{GL}_4(E)$ and that it preserves a nondegenerate symplectic bilinear form invariant under $\rho_{f,\ell}(\mathrm{Gal}_{\mathbb{Q}})$ so lands in $\mathrm{GSp}_4(E)$. Thereby, properties (i)–(iv) are verified.

For all $k \geq 2$, with the above conventions (including archimedean L-parameters) we verify that Π_f satisfies the hypotheses of a theorem of Mok [42, Theorem 4.14]: from this theorem we obtain a unique, continuous semisimple representation $\rho_{f,\ell} \colon \mathrm{Gal}_{\mathbb{Q}} \to \mathrm{GL}_4(\mathbb{Q}_\ell^{\mathrm{al}})$ where $\mathbb{Q}_\ell^{\mathrm{al}}$ is an algebraic closure of $\mathbb{Q}_\ell$. For $k = 2$, Mok constructs the representation by ℓ-adic deformation using Hida theory from those of Laumon and Weissauer, and so properties (i)–(iv) and the fact that the representation is symplectic continue to hold in the limit; and property (v) is a conclusion of his theorem.

To illustrate this convergence argument, we show that the representation is symplectic. Let $\{f_n\}_n$ be a sequence of Siegel paramodular forms of weights $k_n > 2$ such that f_n converge p-adically to f (for example, multiplying by powers of the Hasse invariant). By the previous paragraph, each f_n is symplectic with representation ρ_n so

$$\bigwedge^2 \rho_n(3 - 2k_n) \simeq \rho_{\mathrm{triv}} \oplus \psi_n \tag{4.3.5}$$

is equivalent to the direct sum of the trivial representation ρ_{triv} of degree 1 and the representation ψ of degree 5 with values in $\mathrm{SO}_5(\mathbb{Q}_\ell^{\mathrm{al}})$. The sequence $\mathrm{Tr}\,\psi_n$ of pseudorepresentations converges to a pseudorepresentation by (4.3.5) and continuity of the trace, and this limit is the trace of a representation ψ. From this identity of traces, we conclude

$$\bigwedge^2 \rho(-1) \simeq \rho_{\mathrm{triv}} \oplus \psi$$

and thus ρ is symplectic with cyclotomic similitude character.

Mok's theorem relies on work of Arthur in a crucial way. For further attribution and discussion, see Mok [42, About the proof, pp. 524ff] and the overview of the method by Jorza [37, §§1–3]. □

Let f be as in Theorem 4.3.4, with Galois representation $\rho_{f,\ell} \colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(\mathbb{Q}_\ell^{\mathrm{al}})$ where $S := \{p : p \mid N\} \cup \{\ell, \infty\}$. By the Baire category theorem, we may descend the representation to a finite extension $E' \subseteq \mathbb{Q}_\ell^{\mathrm{al}}$ of $\mathbb{Q}_\ell$. Let $\mathfrak{l}'$ be the prime above ℓ in the valuation ring R'

of E' and let k' be the residue field of R'. Choose a stable R'-lattice in the representation space $V' := (E')^4$ and reduce modulo $\mathfrak{l}'$; the semisimplification yields a semisimple residual representation $\overline{\rho}^{\mathrm{ss}}_{f,\ell}\colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GL}_4(k')$, unique up to equivalence.

Applying a recent result of Serre, we now show that the residual representation is symplectic.

Lemma 4.3.6. *The semisimplification $\overline{\rho}^{\mathrm{ss}}_{f,\ell}\colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GL}_4(k')$ is compatible with a nondegenerate alternating form with similitude character $\overline{\chi}_\ell^{2k-3}$; in particular, up to equivalence its image lies in $\mathrm{GSp}_4(k')$.*

Proof. We refer to Serre [54] and to the Appendix. Let $\langle\ ,\ \rangle$ be the alternating form on V' with similitude character $\epsilon := \chi_\ell^{2k-3}$ provided by Theorem 4.3.4. Then V' is a finite-dimensional E'-vector space equipped with a continuous action by $\mathrm{Gal}_{\mathbb{Q},S}$ via $\rho_{f,\ell}$. Moreover, for all $\sigma \in \mathrm{Gal}_{\mathbb{Q},S}$ and all $x, y \in V'$ we have

$$\langle \sigma x, \sigma y\rangle = \chi_\ell^{2k-3}(\sigma)\langle x, y\rangle; \tag{4.3.7}$$

i.e., the pairing $\langle\ ,\ \rangle$ is χ_ℓ^{2k-3}-covariant under the action of $\mathrm{Gal}_{\mathbb{Q},S}$. Let $V'_{k'}$ be the k'-vector space underlying the semisimplification $\overline{\rho}^{\mathrm{ss}}_{f,\ell}$. Then Serre proves in Theorem 1 in the Appendix that there exists a nondegenerate k'-bilinear alternating form on $V'_{k'}$ that again is covariant with respect to (the reduction of) χ_ℓ^{2k-3} under the action of $\mathrm{Gal}_{\mathbb{Q},S}$.

The final statement holds because, up to equivalence by $\mathrm{GL}_4(k')$, we may assume the alternating form is the standard form, so now the image lands in $\mathrm{GSp}_4(k')$, as claimed. □

Next, we seek descent preserving the symplectic form. Let E be the extension of $\mathbb{Q}_\ell$ generated by the Hecke eigenvalues of f (with respect to a choice of isomorphism between the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$ and in $\mathbb{Q}_\ell^{\mathrm{al}}$); then E also contains all coefficients of the Hecke polynomials $Q_p(f,T)$. Let R be the valuation ring of E and let k be its residue field. We have $E \subseteq E'$, and we would like to be able to descend the representation to take values in $\mathrm{GSp}_4(E)$. However, there is a possible obstruction coming from the Brauer group of $\mathbb{Q}_\ell$; such an obstruction arises for example in the Galois representation afforded by a QM abelian fourfold at a prime ℓ dividing the discriminant of the quaternion algebra B, which has image in $\mathrm{GL}_2(B \otimes \mathbb{Q}_\ell)$ and not $\mathrm{GSp}_4(\mathbb{Q}_\ell)$. Under an additional hypothesis, we may ensure descent following Carayol and Serre as follows.

Lemma 4.3.8. *With hypotheses as in Theorem 4.3.4, the following statements hold.*

(a) *The semisimplified residual representation $\overline{\rho}^{\mathrm{ss}}_{f,\ell}$ descends to*

$$\overline{\rho}^{\mathrm{ss}}_{f,\ell}\colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(k)$$

up to equivalence.

(b) *If $\overline{\rho}^{\mathrm{ss}}_{f,\ell} = \overline{\rho}_{f,\ell}$ is absolutely irreducible, then $\rho_{f,\ell}$ descends to*

$$\rho_{f,\ell}\colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(E)$$

up to equivalence, where E is the extension of $\mathbb{Q}_\ell$ generated by the Hecke eigenvalues of f as above.

Proof. We begin with (a). First, a semisimple representation into $\mathrm{GL}_4(k')$ is determined by its traces, and so up to equivalence we may descend $\overline{\rho}^{\mathrm{ss}}_{f,\ell}$ to take values in $\mathrm{GL}_4(k) \subseteq \mathrm{GL}_4(k')$ (for a complete proof, see e.g. Taylor [56, Lemma 2, part 2]). The semisimplification $\overline{\rho}^{\mathrm{ss}}_{f,\ell}$ was

only well-defined up to equivalence (in $\mathrm{GL}_4(k')$) anyway, so Lemma 4.3.6 still applies and the underlying space $V_k = k^4$ of $\overline{\rho}^{\mathrm{ss}}_{f,\ell}$ has the property that its extension $V_{k'} = (k')^4$ to k' carries an alternating form with k-valued similitude character $\overline{\chi}_\ell^{2k-3}$. The set of such alternating forms with fixed similitude character is defined by linear conditions over k since the image of $\overline{\rho}_{f,\ell}$ belongs to $\mathrm{GL}_4(k)$; therefore, the existence of a form defined on $V_{k'}$ implies the existence of such a form on V_k with the same similitude character. Again up to equivalence, the image of $\overline{\rho}^{\mathrm{ss}}_{f,\ell}$ may be taken to lie in $\mathrm{GSp}_4(k)$.

For statement (b), by a theorem of Carayol [13, Théorème 2] under the hypothesis that the *residual representation is absolutely irreducible*, the representation $\rho_{f,\ell}$ takes values in $\mathrm{GL}_4(E)$. Again we have a nondegenerate alternating form compatible with $\mathrm{Gal}_{\mathbb{Q},S}$, and repeating the first part of the argument in the previous paragraph we may assume it takes values in E; conjugating, we conclude that the image is in $\mathrm{GSp}_4(E)$. □

Remark 4.3.9. The statement of Theorem 4.3.4 is not the most general statement that could be proven (in several respects), but it is sufficient for our purposes.

Berger–Klosin [2, Theorem 8.2] attach to any paramodular newform f a Galois representation into $\mathrm{GL}_4(\mathbb{Q}_\ell^{\mathrm{al}})$, not just those of type **(G)**. The remaining types are related to constructions of automorphic representations from those in $\mathrm{GL}_2(\mathbb{A})$, where the local Langlands correspondence is known. We do not know a reference for a complete argument for these remaining cases. In this article, we are only concerned with forms of type **(G)**.

A consequence of Mok's proof of Theorem 4.3.4(v) is encoded in the following result.

Lemma 4.3.10. *Let K be the fixed field of $\ker \overline{\rho}_{f,\ell}$ and let $\mathrm{cond}(\overline{\rho}_{f,\ell})$ be the Artin conductor of the representation $\overline{\rho}_{f,\ell}$ of $\mathrm{Gal}(K \mid \mathbb{Q})$. If $p \parallel N$ is odd, then $\mathrm{ord}_p(\mathrm{cond}(\overline{\rho}_{f,\ell})) \leq 1$.*

Proof. The proof of Theorem 4.3.4(v) is only up to semisimplification, so we do not know the complete statement of local Langlands under the patching argument that is employed. However, in specializing the family to the accumulation point f in the family, there is nevertheless an *upper bound* on the level: the representation is necessarily either unramified or is Steinberg with level p, and accordingly the conductor has p-valuation 0 or 1. □

5. Group theory and Galois theory for $\mathrm{GSp}_4(\mathbb{F}_2)$

In this section, we carry out the needed Galois theory for the group $\mathrm{GSp}_4(\mathbb{F}_2)$. Specifically, we carry out the task outlined in section 3.2: given $G = \mathrm{img}\,\overline{\rho} \leq \mathrm{GSp}_4(\mathbb{F}_2)$, and for each obstructing extension φ extending $\overline{\rho}$, we compute an exact core-free subgroup $D \leq E$ (as large as possible) and the list of E-conjugacy classes of elements whose upper trace is nonzero. The arguments provided in this section are done once and for all for the group $\mathrm{GSp}_4(\mathbb{F}_2)$; we apply these to our examples in section 7.

Since any similitude factor from $\mathrm{GSp}_4(\mathbb{F}_2)$ belongs to $\mathbb{F}_2^\times$ and is therefore trivial, we have an equality $\mathrm{Sp}_4(\mathbb{F}_2) = \mathrm{GSp}_4(\mathbb{F}_2)$. Rather than writing one or the other throughout, we use the notation that seems natural to us in the given context.

5.1. **Symplectic group as permutation group.** We pause for some basic group theory. We have an isomorphism $\iota\colon S_6 \xrightarrow{\sim} \mathrm{Sp}_4(\mathbb{F}_2)$, where S_6 is the symmetric group on 6 letters, which we make explicit in the following manner. Let $U := \mathbb{F}_2^6$, and equip U with the coordinate action of S_6 and the standard nondegenerate alternating (equivalently, symmetric) bilinear form $\langle x, y\rangle = \sum_{i=1}^6 x_i y_i$ visibly compatible with the S_6-action. Let $U^0 \subset U$ be the

trace 0 hyperplane, let L be the $\mathbb{F}_2$-span of $(1,\dots,1)$, and let $Z := U^0/L$ be the quotient, so $\dim_{\mathbb{F}_2} Z = 4$. Then Z inherits both an action of S_6 and a symplectic pairing, which remains nondegenerate: specifically, the images

$$e_1 := (1,1,0,0,0,0),\ e_2 := (0,0,1,1,0,0),\ e_3 := (0,0,0,1,1,0),\ e_4 := (0,1,0,0,0,1) \in Z$$

are a basis for Z in which the Gram matrix of the induced pairing is the anti-identity matrix, so e.g. $\langle e_1, e_4\rangle = \langle e_2, e_3\rangle = 1$. (An alternating pairing over $\mathbb{F}_2$ is symmetric, and we have chosen the standard such form.) We compute that

$$\begin{aligned} \iota\colon S_6 &\to \mathrm{Sp}_4(\mathbb{F}_2) \\ (1\ 2\ 3\ 4\ 5), (1\ 6) &\mapsto \begin{pmatrix} 1&0&0&1\\0&0&1&0\\1&1&0&1\\1&0&1&0 \end{pmatrix}, \begin{pmatrix} 0&0&0&1\\0&1&0&0\\0&0&1&0\\1&0&0&0 \end{pmatrix}. \end{aligned} \tag{5.1.1}$$

We have

$$\mathrm{Lie}^0(\mathrm{GSp}_4)(\mathbb{F}_2) = \mathsf{sp}_4(\mathbb{F}_2) = \{A \in \mathrm{M}_4(\mathbb{F}_2) : A^{\mathsf{T}} J + JA = 0\} \simeq \mathbb{F}_2^{10} \tag{5.1.2}$$

where $J \in \mathrm{M}_4(\mathbb{F}_2)$ is the anti-identity matrix (with 1 along the anti-diagonal), and we have an exact sequence

$$1 \to \mathsf{sp}_4(\mathbb{F}_2) \to \mathsf{sp}_4(\mathbb{F}_2) \rtimes G \xrightarrow{\pi} G \to 1 \tag{5.1.3}$$

with $\pi\colon \mathsf{sp}_4(\mathbb{F}_2) \rtimes G \to G$ the natural projection map. As in (2.3.9) we identify

$$\begin{aligned} \mathsf{sp}_4(\mathbb{F}_2) \rtimes G \le \mathrm{M}_4(\mathbb{F}_2) \rtimes G &\hookrightarrow \mathrm{GL}_8(\mathbb{F}_2) \\ (a,g) &\mapsto \begin{pmatrix} 1&a\\0&1 \end{pmatrix}\begin{pmatrix} g&0\\0&g \end{pmatrix} = \begin{pmatrix} g&ag\\0&g \end{pmatrix}. \end{aligned} \tag{5.1.4}$$

The following lemmas follow from straightforward computation.

Lemma 5.1.5. *The group* $\mathrm{Sp}_4(\mathbb{F}_2)$ *has elements of orders* $1,\dots,6$ *with the following possibilities for their characteristic polynomials:*

Order	Characteristic polynomial
$1,2,4$	x^4+1
$3,6$	x^4+x^2+1 or x^4+x^3+x+1
5	$x^4+x^3+x^2+x+1$

(5.1.6)

There is a unique outer automorphism of S_6 up to inner automorphisms [32]; it sends transpositions to products of three transpositions, and interchanges the trace of some order 3 and order 6 elements.

Lemma 5.1.7. *There are, up to inner automorphism, exactly* 9 *subgroups of* $\mathrm{Sp}_4(\mathbb{F}_2) \simeq S_6$ *with absolutely irreducible image. They are listed in the following table with a property that determines them uniquely (where '–' indicates there is a unique conjugacy class of subgroup with that order):*

(5.1.8)

Subgroup	Order	Element orders	Distinguishing property
S_6	720	$1,\dots,6$	–
A_6	360	$1,\dots,5$	–
$S_5(a)$	120	$1,\dots,6$	Elements of order $3,6$ have trace 0
$S_5(b)$	120	$1,\dots,6$	Elements of order $3,6$ have trace 1
$S_3 \wr S_2$	72	$1,2,3,4,6$	–
$A_5(b)$	60	$1,2,3,5$	Elements of order 3 have trace 1
$C_3^2 \rtimes C_4$	36	$1,2,3,4$	No elements of order 6
$S_3(a)^2$	36	$1,2,3,6$	Elements of order 6 have trace 0
$C_5 \rtimes C_4$	20	$1,2,4,5$	–

Example 5.1.9. The conjugacy classes of subgroups $S_5(a), S_5(b) \leq S_6$ are exchanged by the outer automorphism of S_6. For example, under the restriction of (5.1.1), we have

(5.1.10)
$$\iota\colon S_5(b) \to \mathrm{Sp}_4(\mathbb{F}_2)$$
$$(1\ 2\ 3\ 4\ 5), (1\ 2), (1\ 2\ 3) \mapsto \begin{pmatrix} 1&0&0&1\\0&0&1&0\\1&1&0&1\\1&0&1&0 \end{pmatrix}, \begin{pmatrix} 1&0&0&1\\0&1&0&0\\0&0&1&0\\0&0&0&1 \end{pmatrix}, \begin{pmatrix} 1&0&0&1\\0&1&0&0\\1&1&1&1\\1&1&0&0 \end{pmatrix}.$$

Another way to distinguish $S_5(a)$ from $S_5(b)$ is that $\iota(S_5(b))$ has transvections while $\iota(S_5(a))$ does not.

Example 5.1.11. There is a subgroup $A_5(a) \leq S_6$ that is similarly exchanged with $A_5(b)$ but that is not absolutely irreducible.

5.2. **Images and discriminants.** For the purposes of establishing the first typical cases of the paramodular conjecture, we observe the following.

Lemma 5.2.1. *Suppose N is odd and squarefree and let A be an abelian surface over $\mathbb{Q}$ of conductor N equipped with a polarization of odd degree. Then the residual representation*

$$\overline{\rho}_{A,2}\colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(\mathbb{F}_2)$$

(where $S = \{p : p \mid N\} \cup \{\ell, \infty\}$) is absolutely irreducible if and only if its image is isomorphic to $S_5(b)$, S_6, or $S_3 \wr S_2$.

Proof. By work of Brumer–Kramer [7, §7.3], whenever N is not a square, the image is either S_5, S_6, or $S_3 \wr S_2$. To force $S_5(b)$, it suffices that there is a prime $p \mid N$ such that A_p has toroidal dimension one (i.e., $p \parallel N$) and that p be ramified in $\mathbb{Q}(A[2])$. If A is semistable and the Galois group is $S_5(a)$, then the toroidal dimension at the bad primes is 2 since there are no transvections. □

Remark 5.2.2. In general, if $A[2]$ is absolutely irreducible, then the degree of any *minimal* polarization on A is odd.

Next, we convert the upper bound from Lemma 4.3.10 on the conductor into an upper bound on the discriminant. We first recall the following standard result.

Lemma 5.2.3. *Let $a(x) \in \mathbb{Q}[x]$ be irreducible and let Ω be the set of roots of $a(x)$ in $\mathbb{Q}^{\mathrm{al}}$. Let $\alpha \in \Omega$, let $K_0 = \mathbb{Q}(\alpha)$, and let K be the normal closure of K_0. Let $\mathfrak{p}$ be a prime of K*

that is tamely ramified in the extension $K \supseteq \mathbb{Q}$, and let $p \in \mathbb{Z}$ be the prime lying below $\mathfrak{p}$. Finally, let $I_{\mathfrak{p}} \leq \mathrm{Gal}(K \mid \mathbb{Q})$ denote the inertia group at $\mathfrak{p}$. Then

$$\mathrm{ord}_p(d_{K_0}) = \deg a(x) - \#\Omega/I_{\mathfrak{p}}$$

where $\#\Omega/I_{\mathfrak{p}}$ denotes the number of orbits of $I_{\mathfrak{p}}$ acting on Ω.

We now specialize to our case of interest.

Proposition 5.2.4. *Let $p \parallel N$ be odd. Let K be the fixed field of $\ker \overline{\rho}_{f,2}$.*

(a) *If $\mathrm{Gal}(K \mid \mathbb{Q}) \simeq S_3 \wr S_2$ (resp., S_m with $m = 5, 6$), then K is the normal closure of a field K_0 of degree 6 (respectively, m) with $\mathrm{ord}_p d_{K_0} \leq 1$.*

(b) *If $\mathrm{Gal}(K \mid \mathbb{Q}) \simeq A_m$, with $m = 5, 6$, then K is the normal closure of a field K_0 of degree m with p unramified in K_0 (i.e., $\mathrm{ord}_p d_{K_0} = 0$).*

Proof. Decomposing the Weil–Deligne representation at p, we see by Lemma 4.3.10 that the image of inertia is either trivial or a 2×2-Jordan block. If trivial, the extension is unramified and the result holds, so suppose we are in the latter case. Under the isomorphism $\mathrm{GSp}_4(\mathbb{F}_2) \simeq S_6$ above (5.1.1), nontrivial elements of this Jordan block correspond to cycle decomposition 2+2+2 or 2+1+1+1+1, and these are exchanged by an outer automorphism.

For (a), by a faithful permutation representation on the cosets of a core-free subgroup, a field K_0 of the given degree exists. If the residual image inside S_6 is invariant under such an automorphism (which holds for S_6 and $S_3 \wr S_2$), then we can choose our subfield K_0 corresponding to the latter case, and conclude $\mathrm{ord}_p d_{K_0} \leq 1$ by Lemma 5.2.3. If $\mathrm{Gal}(K \mid \mathbb{Q}) \simeq S_5$, we have only the possibility $2 + 1 + 1 + 1$ again giving $\mathrm{ord}_p d_{K_0} \leq 1$.

Finally, for (b) and the groups A_5, A_6, we find no possibilities and reach a contradiction, so we conclude that K_0 is unramified at p. □

5.3. **Core-free extensions and obstructing elements.** We will compute all obstructing extensions $\varphi\colon \mathrm{Gal}(L \mid F) \hookrightarrow E$ extending $\overline{\rho}$ (Definition 2.3.17); we represent $L \supseteq K \supseteq F$ by an exact core-free subextension $L_0 \supseteq K_0 \supseteq F$ (Definition 3.1.7) arising from an exact core-free subgroup $D \leq E$ which is as large as possible, to make the degree of the subextension as small as possible.

For each G in (5.1.8), we therefore first seek subgroups $\varphi\colon E \hookrightarrow \mathsf{sp}_4(\mathbb{F}_2) \rtimes G$ such that $\pi(E) = G$; such extensions are obstructing (Definition 2.3.18) if they have nonzero upper trace in the matrix realization (5.1.4).

Consider first the case $G = S_5(b)$.

Theorem 5.3.1. *For $G = S_5(b)$, there are exactly 10 extension groups E up to conjugacy in $\mathrm{M}_4(\mathbb{F}_2) \rtimes G$, with $\#V = [E : G] = 2^k$ where $k = 0, 0, 1, 4, 4, 5, 5, 6, 9, 10$, respectively.*

Furthermore, let

$$H = D_6(b) := \langle (1\ 2), (1\ 3), (4\ 5) \rangle \leq G;$$

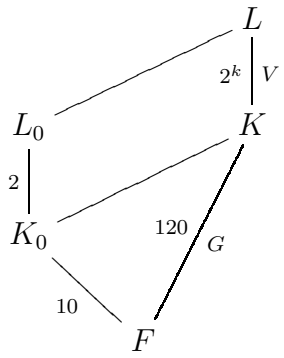
then for all $E \not\simeq G$, there is an exact core-free subgroup $D \leq E$ of index 2 such that $\pi(D) = H$ as in (3.1.6).

Proof. This theorem is proven by explicit computation in Magma [3]; the code is available online [10] together with the verbose output. There are exactly 18 conjugacy classes of subgroups $\varphi\colon E \hookrightarrow \mathsf{sp}_4(\mathbb{F}_2) \rtimes G$ with $\pi(E) = G$; these subgroups fall into 10 conjugacy classes in $\mathrm{M}_4(\mathbb{F}_2) \rtimes G$. Let $H = D_6(b) := \langle (1\ 2), (1\ 3), (4\ 5) \rangle \leq G$ be as in the statement. Then H is dihedral of order $\#H = 12$ and index $[G : H] = 10$ and it can be verified that for

each such $E \not\geq G$, there is at least one subgroup $W \leq V$ of index 2 such that $D \leq E$ is an exact core-free subgroup. □

The somewhat complicated field diagram (3.1.8) in our case simplifies to:

(5.3.2)



We understand the large extension $L \supseteq K \supseteq F$ as the Galois closure of the exact core-free subextension $L_0 \supseteq K_0 \supseteq F$, with $L_0 \supseteq K_0$ quadratic. The extension K_0 is realized explicitly as follows: if $K \supseteq F$ is the splitting field of a quintic polynomial $f(x)$ with roots $\alpha_1, \ldots, \alpha_5$ permuted by S_5, then $K_0 = K^H = F(\alpha_4 + \alpha_5)$.

In a similar way, we have the result for the remaining two groups.

Theorem 5.3.3.

(a) *For $G = S_3 \wr S_2 \leq \mathrm{GSp}_4(\mathbb{F}_2)$, there are exactly 20 extension groups E up to conjugacy in $\mathrm{M}_4(\mathbb{F}_2) \rtimes G$, with $\#V = [E : G] = 2^k$ and*

$$k = 0, 0, 1, 1, 2, 4, 4, 4, 4, 5, 5, 5, 5, 6, 6, 8, 8, 9, 9, 10.$$

Let $H = C_2^2 \leq G$ with $[G : H] = 18$. Then for each such E, there is an exact core-free subgroup $D \leq E$ such that $\pi(D) = H$.

(b) *For $G = S_6 \simeq \mathrm{GSp}_4(\mathbb{F}_2)$, the analogous statement to* (a) *holds, with 7 groups having $k = 0, 0, 1, 5, 5, 6, 10$ and $H = S_3(b)^2$.*

Remark 5.3.4. With reference to computing conjugacy classes in stages as in section 3.3, we note that the index 2 subgroups of the 18 subgroups C_2^2 of $S_3 \wr S_2$ are not sufficient to find obstructing classes for all 20 extension groups if one applies the more limited strategy exhibited in Remark 3.3.2.

Remark 5.3.5. The remaining cases of subgroups $G \leq \mathrm{GSp}_4(\mathbb{F}_2)$ may be computed with the same method and the same code.

6. Computing Hecke eigenvalues by specialization

Having set up the required Galois theory, we now compute Hecke eigenvalues of particular Siegel paramodular newforms. In this section, we use the technique of restriction to a modular curve to accomplish these eigenvalue computations. We continue the notation from section 4.2.

6.1. **Jacobi forms and Borcherds products.** We construct our paramodular forms using Gritsenko lifts of Jacobi forms and Borcherds products. In this section, we quickly review what we need from these theories.

We begin with Jacobi forms; we refer to Eichler–Zagier [20] for further reference. Each Jacobi form $\phi \in J_{k,N}$ of weight k and index N has a Fourier expansion

$$\phi(\tau, z) = \sum_{n,r\in\mathbb{Z}} c(n, r; \phi) q^n \zeta^r, \tag{6.1.1}$$

where $q = e(\tau)$ and $\zeta = e(z)$. We write $\phi \in J_{k,N}(R)$ if all the Fourier coefficients of ϕ lie in a ring $R \subseteq \mathbb{C}$. We will need the level-raising operators $V_m \colon J_{k,N} \to J_{k,mN}$ (see Eichler–Zagier [20, p. 41]) that act on $\phi \in J_{k,N}$ via

$$c(n, r; \phi \,|\, V_m) = \sum_{\delta|\gcd(n,r,m)} \delta^{k-1} c\left(\frac{mn}{\delta^2}, \frac{r}{\delta}; \phi\right). \tag{6.1.2}$$

The Gritsenko lift [26]

$$\mathrm{Grit} \colon J^{\mathrm{cusp}}_{k,N} \to S_k(K(N))$$

lifts a Jacobi cusp form ϕ to a paramodular form f by the rule

$$a\left(\left(\begin{smallmatrix} n & r/2 \\ r/2 & Nm \end{smallmatrix}\right); \mathrm{Grit}(\phi)\right) = c(n, r; \phi \,|\, V_m).$$

We also have $\mathrm{Grit}(\phi)|_k \, \mu_N = (-1)^k \, \mathrm{Grit}(\phi)$, so that a Gritsenko lift has paramodular Fricke sign $(-1)^k$.

One convenient way to construct Jacobi forms is to use the theta blocks created by Gritsenko–Skoruppa–Zagier [28]. Recall the Dedekind η-function and the Jacobi ϑ-function

$$\eta(\tau) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) = \sum_{n=1}^{\infty} \left(\frac{12}{n}\right) q^{n^2/24},$$

$$\vartheta(\tau, z) = \sum_{n=-\infty}^{\infty} (-1)^n q^{(2n+1)^2/8} \zeta^{(2n+1)/2} = q^{1/8}(\zeta^{1/2} - \zeta^{-1/2}) \sum_{n=1}^{\infty} (-1)^{n+1} q^{\binom{n}{2}} \sum_{j=-(n-1)}^{n-1} \zeta^j.$$

For $d \in \mathbb{Z}_{>0}$ let $\vartheta_d(\tau, z) = \vartheta(\tau, dz)$. For $d_1, \dots, d_\ell \in \mathbb{Z}_{>0}$ and $k \in \mathbb{Z}$, define the *theta block*

$$\mathrm{TB}_k[\mathbf{d}] = \mathrm{TB}_k[d_1, d_2, \dots, d_\ell] = \eta^{2k} \prod_{j=1}^{\ell} \frac{\vartheta_{d_j}}{\eta}. \tag{6.1.3}$$

The theta block $\mathrm{TB}_k[\mathbf{d}]$ defines a meromorphic Jacobi form (with multiplier) of weight k and index $m = \frac{1}{2}(d_1^2 + \cdots + d_\ell^2)$. Moreover [20] (compare Poor–Yuen [46, Theorem 4.3]), the theta block $\mathrm{TB}_k[\mathbf{d}]$ is a Jacobi cusp form if

$$12 \mid (k + \ell) \quad \text{and} \quad \frac{k}{12} + \frac{1}{2} \sum_{j=1}^{\ell} \bar{B}_2(d_j x) > 0, \tag{6.1.4}$$

where $B_2(x) := x^2 - x + \frac{1}{6}$ and $\bar{B}_2(x) := B_2(x - \lfloor x \rfloor)$.

Second, we use Borcherds products in the construction of paramodular forms. Let ψ be a weakly holomorphic Jacobi form of weight 0 and index N with integral Fourier coefficients

on singular indices with Fourier expansion (6.1.1). Define

$$A(\psi) := \frac{1}{24}\sum_{r\in\mathbb{Z}} c(0,r;\psi), \quad B(\psi) := \frac{1}{2}\sum_{r\geq 1} rc(0,r;\psi), \quad C(\psi) := \frac{1}{4}\sum_{r\in\mathbb{Z}} r^2 c(0,r;\psi).$$

Then $A(\psi), B(\psi), C(\psi) \in \mathbb{Q}$. The Borcherds product of ψ is a meromorphic paramodular form $\mathrm{Borch}(\psi)$, perhaps with nontrivial character on $K(N)$, with

$$\mathrm{Borch}(\psi) = q^{A(\psi)}\zeta^{B(\psi)}\xi^{C(\psi)} \prod_{n,r,m} (1-q^n\zeta^r\xi^{mN})^{c(mn,r;\psi)}, \tag{6.1.5}$$

where the product is over $n, r, m \in \mathbb{Z}$ such that: (i) $m \geq 0$; (ii) if $m = 0$, then $n \geq 0$; and (iii) if $m = n = 0$, then $r < 0$. Borcherds products are not always holomorphic and, when holomorphic, not always cuspidal.

6.2. **Construction of newforms.** In this section, we define the nonlift paramodular newforms of interest to this article, with levels $277, 353, 587$. We will see later that this way of writing paramodular forms makes the computation of Hecke eigenvalues feasible.

We refer to section 4.2 for notation. We now define the nonlift paramodular form $f_{277} \in S_2(K(277),\mathbb{Z})^+$ following Poor–Yuen [46, Theorem 7.1]. Define the following ten theta blocks:

$$\begin{aligned}
\Xi_1 &:= \mathrm{TB}_2(2,4,4,4,5,6,8,9,10,14) & \Xi_6 &:= \mathrm{TB}_2(2,3,3,5,5,7,8,10,10,13)\\
\Xi_2 &:= \mathrm{TB}_2(2,3,4,5,5,7,7,9,10,14) & \Xi_7 &:= \mathrm{TB}_2(2,3,3,4,5,6,7,9,10,15)\\
\Xi_3 &:= \mathrm{TB}_2(2,3,4,4,5,7,8,9,11,13) & \Xi_8 &:= \mathrm{TB}_2(2,2,4,5,6,7,7,9,11,13)\\
\Xi_4 &:= \mathrm{TB}_2(2,3,3,5,6,6,8,9,11,13) & \Xi_9 &:= \mathrm{TB}_2(2,2,4,4,6,7,8,10,11,12)\\
\Xi_5 &:= \mathrm{TB}_2(2,3,3,5,5,8,8,8,11,13) & \Xi_{10} &:= \mathrm{TB}_2(2,2,3,5,6,7,9,9,11,12).
\end{aligned} \tag{6.2.1}$$

We have, for $i = 1, \ldots, 10$,

$$\Xi_i \in J^{\mathrm{cusp}}_{2,277}(\mathbb{Z}) \quad \text{and} \quad G_i := \mathrm{Grit}(\Xi_i) \in S_2(K(277),\mathbb{Z}).$$

Let f_{277} be the (a priori) meromorphic function on $\mathcal{H}_2$ defined by

$$\begin{aligned}
f_{277} := (&-14G_1^2 - 20G_8G_2 + 11G_9G_2 + 6G_2^2 - 30G_7G_{10} + 15G_9G_{10}\\
&+ 15G_{10}G_1 - 30G_{10}G_2 - 30G_{10}G_3 + 5G_4G_5 + 6G_4G_6 + 17G_4G_7\\
&- 3G_4G_8 - 5G_4G_9 - 5G_5G_6 + 20G_5G_7 - 5G_5G_8 - 10G_5G_9 - 3G_6^2\\
&+ 13G_6G_7 + 3G_6G_8 - 10G_6G_9 - 22G_7^2 + G_7G_8 + 15G_7G_9 + 6G_8^2\\
&- 4G_8G_9 - 2G_9^2 + 20G_1G_2 - 28G_3G_2 + 23G_4G_2 + 7G_6G_2\\
&- 31G_7G_2 + 15G_5G_2 + 45G_1G_3 - 10G_1G_5 - 2G_1G_4 - 13G_1G_6\\
&- 7G_1G_8 + 39G_1G_7 - 16G_1G_9 - 34G_3^2 + 8G_3G_4 + 20G_3G_5\\
&+ 22G_3G_6 + 10G_3G_8 + 21G_3G_9 - 56G_3G_7 - 3G_4^2)/\\
&(-G_4 + G_6 + 2G_7 + G_8 - G_9 + 2G_3 - 3G_2 - G_1).
\end{aligned} \tag{6.2.2}$$

A main result of Poor–Yuen [46, Theorem 7.1] is that f_{277} is actually *holomorphic*: in fact, $f_{277} \in S_2(K(277),\mathbb{Z})^+$ is a cuspidal, nonlift, paramodular form of weight 2 that is an eigenform for all Hecke operators and has integral Fourier coefficients whose greatest common divisor is 1. There are no nontrivial weight 2 paramodular cusp forms of level 1, so since

277 is prime, f_{277} is a newform. Equation (4.2.9) and Lemma 4.2.17 imply that the Euler factors $Q_p(f_{277}, t)$ are integral.

The first few eigenvalues for f_{277} were computed [46] as

$$a_p(f_{277}) = -2, -1, -1, 1, -2 \quad \text{for } p = 2, 3, 5, 7, 11 \tag{6.2.3}$$

and the first three Hecke polynomials, identifying f_{277} as type **(G)**, are:

$$\begin{aligned} Q_2(f_{277}, t) &= 1 + 2t + 4t^2 + 4t^3 + 4t^4, \\ Q_3(f_{277}, t) &= 1 + t + t^2 + 3t^3 + 9t^4, \\ Q_5(f_{277}, t) &= 1 + t - 2t^2 + 5t^3 + 25t^4. \end{aligned} \tag{6.2.4}$$

Remark 6.2.5. The form f_{277} can also be realized as the sum of a Borcherds product and a Gritsenko lift, giving a second, independent construction by Poor–Shurman–Yuen [44].

In a similar way, we construct a second form

$$f_{353} := Q(G_1, \ldots, G_{11}) \in S_2(K(353), \mathbb{Z})^+ \tag{6.2.6}$$

(plus eigenspace for the Fricke involution, as in (4.2.4)) a quotient of a quadratic polynomial by a linear polynomial of 11 Gritsenko lifts of theta blocks: see Poor–Yuen [46, Theorem 7.4] for the specific formula for Q and the forms G_i. This construction was contingent upon assuming the existence of some nonlift in $S_2(K(353))$; however, the dimension $\dim S_2(K(353)) = 12$ is now known [44] via the construction of a nonlift Borcherds product in $S_2(K(353))$.

The first two Euler factors, each showing that f_{353} is of type **(G)**, are

$$\begin{aligned} Q_2(f_{353}, t) &= 1 + t + 3t^2 + 2t^3 + 4t^4, \\ Q_3(f_{353}, t) &= 1 + 2t + 4t^2 + 6t^3 + 9t^4. \end{aligned} \tag{6.2.7}$$

Finally, we construct a form of level 587 as a Borcherds product. An antisymmetric nonlift Borcherds product $f_{587}^- \in S_2\left(K(587), \mathbb{Z}\right)^-$ was recently constructed by Gritsenko–Poor–Yuen [27]. The form f_{587}^- is necessarily an eigenform because $\dim S_2\left(K(587)\right)^- = 1$. The Fourier expansion is given by formally expanding

$$f_{587}^- = \operatorname{Borch}(\psi) = \xi^{587}\phi \exp(-\operatorname{Grit}(\psi)) \quad \text{for} \quad \psi = (\phi \,|\, V_2 - \Xi)/\phi, \tag{6.2.8}$$

where

$$\begin{aligned} \phi &= \mathrm{TB}_2(1,\ \ 1,2,2,\ \ 2,3,3,4,4,\ \ 5,5,6,6,7,8,\ \ 8,9,10,11,12,13,14) \in J^{\mathrm{cusp}}_{2,587}, \\ \Xi &= \mathrm{TB}_2(1,10,2,2,18,3,3,4,4,15,5,6,6,7,8,16,9,10,22,12,13,14) \in J^{\mathrm{cusp}}_{2,1174}. \end{aligned} \tag{6.2.9}$$

For the Borcherds product that appears in the formula for f_{587}^-, we have $\operatorname{Borch}(\psi) \in S_k(K(587))$ with $k = \frac{1}{2}c(0,0;\psi) = 2$ [27]. The first two Euler factors, verifying type **(G)**, are computed to be

$$\begin{aligned} Q_2(f_{587}^-, t) &= 1 + 3t + 5t^2 + 6t^3 + 4t^4, \\ Q_3(f_{587}^-, t) &= 1 + 4t + 9t^2 + 12t^3 + 9t^4. \end{aligned} \tag{6.2.10}$$

6.3. **Specialization.** To compute the action of the Hecke operators directly on a Fourier expansion of a Siegel paramodular form would require manipulations with series in three variables. To avoid this, we specialize our form. Possibilities for this specialization include restriction to Humbert surfaces (typically producing Hilbert modular forms), restriction to modular curves (producing classical modular forms), or evaluation at CM points (producing a numerical result, see Colman–Ghitza–Ryan [16]). Each of these methods has certain advantages and disadvantages—we choose to restrict to modular curves and work with one-variable q-series to avoid rigorous analysis of the upper bounds on the tails of convergent numerical series. The biggest advantage of our choice, however, is that Proposition 6.3.8 allows us to sum over only $O(p^2)$ cosets instead of $O(p^3)$ cosets, a significant savings; it is not clear whether such a speedup is available to a method that numerically evaluates at CM points.

Remark 6.3.1. Specialization of Siegel modular forms is not a new idea, but here we take a different approach. In previous work of Poor–Yuen [46], only three Euler factors were computed for f_{277} because the computation relied on multiplying initial expansions of multivariable Fourier series. Instead, below we will write the action of the Hecke operator $T(p)$ on a paramodular form f as a sum of slashes $f\,|_k\,T(p) = \sum_j f\,|_k\,M_j$, and the main innovation is to specialize each part of $f|M_j$ to a one variable q-series prior to any addition, multiplication, or division. Specialization was also used by Poor–Yuen [45] to compute upper bounds on dimensions and some Fourier coefficients by taking advantage of the known structure of the target space of elliptic modular forms, whereas here we only use the one variable nature of the target space.

Let $s \in \mathrm{M}_2^{\mathrm{sym}}(\mathbb{Q})_{>0}$ be a symmetric, positive definite matrix with rational coefficients. Let $\mathcal{H}_g$ be the Siegel upper half space of dimension g, so $\mathcal{H}_1$ is the upper half-plane. Define the holomorphic map

$$\begin{aligned} \phi_s \colon \mathcal{H}_1 &\to \mathcal{H}_2 \\ \tau &\mapsto s\tau. \end{aligned} \tag{6.3.2}$$

Lemma 6.3.3. *Let $R \subseteq \mathbb{C}$ be a subring. Let $s = \left(\begin{smallmatrix} a & b \\ b & c/N \end{smallmatrix}\right) \in \mathrm{M}_2^{\mathrm{sym}}(\mathbb{Q})_{>0}$ with $a, b, c \in \mathbb{Z}$. Then the pullback under ϕ_s defines a ring homomorphism*

$$\phi_s^* : M(K(N), R) \to M(\Gamma_0(\det(s)N), R) \tag{6.3.4}$$

from the graded ring of Siegel paramodular forms of level N with coefficients in R to the graded ring of classical modular forms of level $\det(s)N$ with coefficients in R. The map ϕ_s^* multiplies weights by 2 and maps cusp forms to cusp forms.

Proof. The proof follows from a straightforward modification of a result of Poor–Yuen [45, Proposition 5.4]. □

Let $f \in M_k(K(N), R)$ be a paramodular form with Fourier expansion (4.2.5), the Fourier expansion of the specialization $\phi_s^* f \in M_{2k}(\Gamma_0(\det(s)N), R)$ is

$$(\phi_s^* f)(\tau) = f(s\tau) = \sum_{n=0}^{\infty} \left(\sum_{T \colon \mathrm{Tr}(sT)=n} a(T; f) \right) q^n. \tag{6.3.5}$$

Furthermore, the specialization of f after slashing with a block upper-triangular matrix $\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right) \in \mathrm{GSp}_4^+(\mathbb{Q})$ with similitude $\mu = \det(AD)^{1/2}$ is given by

$$\begin{aligned} \phi_s^*(f\,|_k\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right))(\tau) &= (f\,|_k\left(\begin{smallmatrix} A & B \\ 0 & D \end{smallmatrix}\right))(s\tau) = \det(AD)^{k-3/2}\det(D)^{-k} f(AsD^{-1}\tau + BD^{-1}) \\ &= \det(A)^k \det(AD)^{-3/2} \sum_{n \in \mathbb{Q}_{\geq 0}} \Bigg(\sum_{T\colon \mathrm{Tr}(AsD^{-1}T)=n} e\left(\mathrm{Tr}(BD^{-1}T)\right)\, a(T;f) \Bigg) q^n. \end{aligned} \tag{6.3.6}$$

Let $s = \left(\begin{smallmatrix} a & b \\ b & c/N \end{smallmatrix}\right) \in \mathrm{M}_2^{\mathrm{sym}}(\mathbb{Q})_{>0}$ with $a, b, c \in \mathbb{Z}$. Using (4.2.8), the specialization of $f\,|_k\, T(p)$ may be written

$$\begin{aligned} \phi_s^*(f\,|_k\,T(p))(\tau) &= p^{2k-3} f(ps\tau) \\ &\quad + p^{k-3} \sum_{i \bmod p} f\Big(\left(\begin{smallmatrix} a/p & b \\ b & pc/N \end{smallmatrix}\right)\tau + \left(\begin{smallmatrix} i/p & 0 \\ 0 & 0 \end{smallmatrix}\right)\Big) \\ &\quad + p^{k-3} \sum_{i \bmod p} \Bigg(\sum_{j \bmod p} f\Big(\left(\begin{smallmatrix} pa & b+ia \\ b+ia & (c/N+2ib+i^2a)/p \end{smallmatrix}\right)\tau + \left(\begin{smallmatrix} 0 & 0 \\ 0 & j/p \end{smallmatrix}\right)\Big)\Bigg) \\ &\quad + p^{-3} \sum_{i,j,k \bmod p} f\Big(s\tau/p + \left(\begin{smallmatrix} i/p & j/p \\ j/p & k/p \end{smallmatrix}\right)\Big). \end{aligned} \tag{6.3.7}$$

Upon expanding in Puiseux q-series, there is cancellation among these sums of specializations. The following proposition shows that partial summation gives new specializations whose sum *over smaller index sets* equals the original sum for integral powers of q. For a Puiseux series $f \in \mathbb{C}[[q^{1/\infty}]]$ and $e \in \mathbb{Q}_{\geq 0}$, we denote by $\mathrm{coeff}_e f \in \mathbb{C}$ the coefficient of q^e in f.

Proposition 6.3.8. *Let $s = \left(\begin{smallmatrix} a & b \\ b & c/N \end{smallmatrix}\right) \in \mathrm{M}_2^{\mathrm{sym}}(\mathbb{Q})_{>0}$ with $a, b, c \in \mathbb{Z}$. Let p be prime, and let $f \in M_k(K(N))$. Then the following statements hold for all $e \in \mathbb{Z}_{\geq 0}$.*

(a) *If $p \nmid a$, then*

$$\mathrm{coeff}_e \sum_{i \bmod p} f\Big(\left(\begin{smallmatrix} a/p & b \\ b & pc/N \end{smallmatrix}\right)\tau + \left(\begin{smallmatrix} i/p & 0 \\ 0 & 0 \end{smallmatrix}\right)\Big) = p\,\mathrm{coeff}_e f\Big(\left(\begin{smallmatrix} a/p & b \\ b & pc/N \end{smallmatrix}\right)\tau\Big)$$

$$\mathrm{coeff}_e \sum_{i,j,k \bmod p} f\Big(s\tau/p + \left(\begin{smallmatrix} i/p & j/p \\ j/p & k/p \end{smallmatrix}\right)\Big) = p\,\mathrm{coeff}_e \sum_{j,k \bmod p} f\Big(s\tau/p + \left(\begin{smallmatrix} 0 & j/p \\ j/p & k/p \end{smallmatrix}\right)\Big).$$

(b) *If $p \nmid b$, then*

$$\mathrm{coeff}_e \sum_{i,j,k \bmod p} f\Big(s\tau/p + \left(\begin{smallmatrix} i/p & j/p \\ j/p & k/p \end{smallmatrix}\right)\Big) = p\,\mathrm{coeff}_e \sum_{i,k \bmod p} f\Big(s\tau/p + \left(\begin{smallmatrix} i/p & 0 \\ 0 & k/p \end{smallmatrix}\right)\Big).$$

(c) *If $p \nmid c$, then*

$$\mathrm{coeff}_e \sum_{i,j,k \bmod p} f\Big(s\tau/p + \left(\begin{smallmatrix} i/p & j/p \\ j/p & k/p \end{smallmatrix}\right)\Big) = p\,\mathrm{coeff}_e \sum_{i,j \bmod p} f\Big(s\tau/p + \left(\begin{smallmatrix} i/p & j/p \\ j/p & 0 \end{smallmatrix}\right)\Big).$$

(d) *For $i \in \mathbb{Z}$, if $p \nmid (c + 2ibN + i^2aN)$, then*

$$\mathrm{coeff}_e \sum_{j \bmod p} f\Big(\left(\begin{smallmatrix} pa & b+ia \\ b+ia & (c/N+2ib+i^2a)/p \end{smallmatrix}\right)\tau + \left(\begin{smallmatrix} 0 & 0 \\ 0 & j/p \end{smallmatrix}\right)\Big) = p\,\mathrm{coeff}_e f\Big(\left(\begin{smallmatrix} pa & b+ia \\ b+ia & (c/N+2ib+i^2a)/p \end{smallmatrix}\right)\tau\Big).$$

Proof. We prove (c); the other proofs are similar. Suppose $p \nmid c$. Let $e \in \mathbb{Z}_{\geq 0}$. Then the coefficient of q^e in the left-hand side is equal to

$$\sum_{\substack{i,j,k \bmod p \\ n,r,m:\, an+br+cm=pe}} e((in+jr+km)/p)a(T;f) \tag{6.3.9}$$

where $T = \left(\begin{smallmatrix} n & r/2 \\ r/2 & mN \end{smallmatrix}\right)$. If any of n, r, m is not a multiple of p, then summing over i, j, k modulo p in (6.3.9) would yield a contribution of zero. Hence we may restrict the sum to the terms where $p \mid n$, $p \mid r$, and $p \mid m$. But since $p \nmid c$ and given $an + br + cm = pe$, the conditions $p \mid n$ and $p \mid r$ imply $p \mid m$. Thus (6.3.9) becomes simply

$$\sum_{\substack{i,j,k \bmod p \\ n,r,m:\, an+br+cm=pe \\ p|n,\, p|r}} e((in+jr+0)/p)a(T;f) = p \sum_{\substack{i,j \bmod p \\ n,r,m:\, an+br+cm=pe \\ p|n,\, p|r}} e((in+jr)/p)a(T;f)$$

$$= p \sum_{\substack{i,j \bmod p \\ n,r,m:\, an+br+cm=pe}} e((in+jr)/p)a(T;f) = p \operatorname{coeff}_e \sum_{i,j \bmod p} f\left(s\tau/p + \left(\begin{smallmatrix} i/p & j/p \\ j/p & 0 \end{smallmatrix}\right)\right). \qquad \square$$

Remark 6.3.10. Proposition 6.3.8 provides a certain subtle speedup because the coefficients at integral powers are equal, even though the series themselves are not necessarily equal. Further simplifying the above sums to

$$p^3 \sum_{\substack{n,r,m:\, an+br+cm=pe \\ p|n,p|r,p|m}} a(T;f).$$

does not help: we want to leave the sums in terms of coefficients of specializations.

In a similar way, we can compute the specialization $\phi_s^*(f \mid_k T_1(p^2))$ and there are similar cancellations in the character sums as in Proposition 6.3.8.

6.4. **Algorithmic detail.** In this section, we provide three further bits of algorithmic detail.

First, we describe the choice of s. Suppose f has a nonzero coefficient $a(t_0; f)$ where t_0 has small determinant and small entries. If we choose s to be the adjoint of $2t_0$, then the restriction $\phi_s^*(f)$ likely begins with $a(t_0; f)q^{\det(s)}$. In particular if t_0 has minimal determinant, then this is forced. In practice, we can just check the initial expansion to see that

$$\phi_s^*(f)(\tau) = a(t_0; f)q^{\det(s)} + \text{higher powers of } q.$$

For each $T(p)$, we want to expand $\phi_s^*(f|T(p))$ to at least q^e where $e = \det(s)$ is the target exponent of q. For a polynomial combination of Gritsenko lifts and Borcherds products, the target exponent of each part $g(G\tau + H)$ would also be e. But for a rational function of Gritsenko lifts and Borcherds products, we have to be slightly more careful. If the denominator of this rational functional restricted to $(G\tau + H)$ has leading term q^μ, then we must expand both the numerator and denominator to a higher target term $q^{e+\mu}$. Therefore, we may end up evaluating the restriction of the denominator twice, with the initial execution used to get the leading exponent μ.

Second, we provide our algorithm for finding all T such that $\langle G, T\rangle \leq u$. Let G and H be two rational, symmetric 2×2 matrices with G positive definite. We explain how to effectively compute specializations of the form $f(G\tau + H)$, as in equation 6.3.7 or Proposition 6.3.8.

We adapt our index sets $\mathcal{S}$ to the type used in (6.1.5) for Borcherds products but they can be used in all the cases we need to program. For any $u, \delta \in \mathbb{R}$, let

$$\mathcal{S}(N, G, u, \delta) = \Big\{(n, r, m) \in \mathbb{Z}^3 : \operatorname{tr}\Big(\begin{pmatrix} n & r/2 \\ r/2 & mN \end{pmatrix} G\Big) \le u, m \ge 0, 4mnN - r^2 \ge \delta, \\ \text{if } m = 0 \text{ then } n \ge 0 \text{ and if } m = n = 0 \text{ then } r < 0\Big\}.$$

Proposition 6.4.1. *Let $G = \left(\begin{smallmatrix} \alpha & \beta \\ \beta & \gamma \end{smallmatrix}\right) \in \mathrm{M}_2(\mathbb{R})$ be positive definite. Let $u, \delta \in \mathbb{R}$. Let $\Delta = \det G = \alpha\gamma - \beta^2 > 0$. Let $X = 4\alpha umN - \alpha^2\delta - 4\Delta(mN)^2$. Then the elements $(n, r, m) \in \mathcal{S}(N, G, u, \delta)$ satisfy the following bounds.*

(a) *If $m \ge 1$, then*

$$1 \le m \le \frac{\alpha(u + \sqrt{u^2 - \delta\Delta})}{2\Delta N}, \\ \frac{-2\beta mN - \sqrt{X}}{\alpha} \le r \le \frac{-2\beta mN + \sqrt{X}}{\alpha}, \quad \text{and} \\ \frac{r^2 + \delta}{4mN} \le n \le \frac{u - \beta r - \gamma mN}{\alpha}.$$

(b) *If $m = 0$ and $n > 0$, then*

$$r^2 \le -\delta \quad \text{and} \quad 1 \le n \le \frac{u - \beta r}{\alpha}.$$

(c) *If $m = n = 0$, then*

$$r^2 \le -\delta \text{ and } r < 0.$$

Proof. The main two conditions that need to be satisfied are $\alpha n + \beta r + \gamma mN \le u$ and $4mnN - r^2 \ge \delta$. The case $m = 0$ is straightforward, so we only deal with the case $m \ge 1$ here. These two inequalities lead immediately to the third inequality as stated in the proposition. From this third inequality, we work with terms on the left and right of n; multiply through by $4mN\alpha$ and put the terms on one side:

$$\alpha r^2 + \alpha\delta - 4mNu + 4mN\beta r + 4\gamma(mN)^2 \le 0.$$

Solving this quadratic inequality for r yields the second inequality stated in the proposition. A condition for there to be a solution in r is that the inside X of the square root must be nonnegative. Solving the resulting quadratic inequality yields the first inequality in the proposition. □

We conclude with a final speedup. Suppose we wish to calculate the coefficient of q^e in $f(G\tau + H)$. If there are no $(n, r, m) \in \mathcal{S}(N, G, u, \delta)$ such that $\operatorname{tr}\Big(\begin{pmatrix} n & r/2 \\ r/2 & mN \end{pmatrix} G\Big) = e$, then we may skip the term involving G. This simple observation is especially useful for terms in the second summand in (6.3.7): for well chosen s, there are typically at most 2 choices of i for which such (n, r, m) exist. It often happens that, for these surviving i, Proposition 6.3.8(d) applies.

6.5. **Example of restricting f_{277}.** Now suppose that f is represented as a rational function in Gritsenko lifts G_i with coefficients in a commutative ring R by $f = Q(G_1, \dots, G_r)$. Both the slash by M and the specialization by ϕ_s^* may be applied directly to each Gritsenko lift, so that we obtain

$$\phi_s^*(f \mid M) = Q(\phi_s^*(G_1 \mid M), \dots, \phi_s^*(G_r \mid M)). \tag{6.5.1}$$

If the Fourier coefficients of f satisfy $a(T; f) \in R \subseteq \mathbb{C}$, then for the representative matrices M_j appearing in the coset decomposition (4.2.8) for the Hecke operator $T(p)$, the sum in (6.3.6) can be taken over $n \in \frac{1}{p}\mathbb{Z}_{\geq 0}$ and the coefficients of $\phi_s^*(f \mid M_j)$ belong to the ring $R[1/p, \zeta_p]$ where $\zeta_p = e(1/p)$ is a primitive pth root of unity. From specializing $f \mid T(p) = \sum_j f \mid M_j = a_p(f) f$, the eigenvalue $a_p(f)$ for $T(p)$ can be computed by performing field operations on Laurent–Puiseux series in q via

$$a_p(f) = \frac{1}{\phi_s^*(f)} \sum_j \phi_s^*(f \mid M_j) \in R[1/p, \zeta_p][[q^{1/p}]] \tag{6.5.2}$$

whenever the specializing curve ϕ_s is chosen so that $\phi_s^*(f)$ is not identically zero. In practice, we choose a target exponent e such that $\operatorname{coeff}_e \phi_s^* f \neq 0$ and then

$$a_p(f) = \frac{\operatorname{coeff}_e\left(\sum_j \phi_s^*(f \mid M_j)\right)}{\operatorname{coeff}_e(\phi_s^*(f))}. \tag{6.5.3}$$

Remark 6.5.4. One practical advantage of this technique of restricting to modular curves is that when more than one coefficient in the q-expansion of (6.5.2) is computed, it constitutes a double check on the value of $a_p(f)$.

Example 6.5.5. We consider the core example of the form f_{277} of level $N = 277$ constructed above (6.2.2). A Fourier coefficient of f_{277} whose matrix index has the smallest determinant is $a(t_0; f_{277}) = -3$, where $t_0 = \begin{pmatrix} 49 & -233/2 \\ -233/2 & 277 \end{pmatrix}$ and $\det(2t_0) = 3$. Accordingly we select $s = \begin{pmatrix} 554 & 233 \\ 233 & 98 \end{pmatrix}$, which is the adjoint of $2t_0$. Working over $R = \mathbb{Z}$, we find

$$\phi_s^*(f_{277}) = -3q^3 + 6q^6 + 6q^9 + 3q^{12} + 3q^{15} - 12q^{18} + 3q^{21} + O(q^{24}). \tag{6.5.6}$$

As a sanity check, we recognized $\phi_s^*(f_{277})$ using modular symbols as a classical modular form of weight 4 and level $3 \cdot 277$ to order $O(q^{400})$. We then compute

$$\phi_s^*(f_{277} \mid T_2) = 6q^3 - 12q^6 - 12q^9 - 6q^{12} - 6q^{15} + 24q^{18} - 6q^{21} + O(q^{24}) \tag{6.5.7}$$

so quite convincingly, $a_2(f_{277}) = -2$, in agreement with (6.2.3).

To compute the action of Hecke operators on the specialized expansion (6.5.2), we work (to a finite degree of q-adic precision) with coefficients over $\mathbb{C}$ or over $\mathbb{Z}/m\mathbb{Z}$ with m suitably large—we consider these two approaches in turn in the next two sections.

6.6. **Over floating point complex numbers.** We may also compute $a_p(f)$ via equation (6.5.2) over the complex numbers using interval arithmetic.

Example 6.6.1. We perform our Hecke computation with in-house C++ code. Continuing with $f = f_{277}$ as in Example 6.5.5, for $p = 2$ we work with 512 bits of precision: the upper size encountered was $3.40282 \cdot 10^{38}$ and the lower size was $2.9387 \cdot 10^{-39}$, giving

$$a_2(f) = \frac{\phi_s^*(f \mid T_2)}{\phi_s^*(f)} \equiv \frac{6q^3 + O(q^5)}{-3q^3 + O(q^4)} = -2 + O(q)$$

up to an error 10^{-75} under a second on a standard desktop CPU. The largest computation required for this f was $a_{43}(f) = 4$; with the same bit precision and maximum error smaller than 10^{-40}, it took less than 90 minutes.

Remark 6.6.2. Given the first few Dirichlet coefficients of an L-function in the Selberg class with specified conductor and Γ-factors, Farmer–Koutsoliotas–Lemurell [21] can (in principle) rigorously compute complex approximations to the next few Dirichlet coefficients using just the approximate functional equation. This method is practical for small examples—and it is especially useful when the L-function is of unknown, speculative, or otherwise complicated origin. Prolonging an initial L-series is a possible avenue for extending the range of examples of modularity proven in this article.

6.7. **Expansion over a finite field.** As an alternative to complex expansion, we may also work in a finite ring. To do so, we need the following archimedean information about the Hecke eigenvalue.

Proposition 6.7.1. *Let $f \in S_k(K(N))$ be an eigenform for the Hecke operators $T(p), T_1(p^2)$ with eigenvalues $a_p(f), a_{1,p^2}(f) \in \mathbb{C}$ where $p \nmid N$. Then*

$$|a_p(f)| \le p^{k-3}(1+p)(1+p^2); \quad |a_{1,p^2}(f)| \le p^{2k-6}(1+p)(1+p^2)p. \tag{6.7.2}$$

Proof. By an elementary estimate, there exists a $B > 0$ such that $|a(T; f)| \le B \det(T)^{k/2}$ for all T. Clearly $B = \sup_{T>0} |a(T; f)| \det(T)^{-k/2}$ is optimal. By (4.2.9), we have

$$\begin{aligned}
|a_p(f)|\,|a(T;f)| &= |a\,(T; f|T(p))| \\
&\le |a\,(pT; f)| + p^{k-2} \sum_{j \bmod p} |a(\tfrac{1}{p} T \left[\begin{smallmatrix} 1 & 0 \\ j & p \end{smallmatrix}\right]; f)| + p^{k-2} |a(\tfrac{1}{p} T \left[\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right]; f)| + p^{2k-3} |a(\tfrac{1}{p} T; f)| \\
&\le B p^k \det(T)^{k/2} + B p^{k-1} \det(T)^{k/2} + B p^{k-2} \det(T)^{k/2} + B p^{k-3} \det(T)^{k/2}.
\end{aligned}$$

From the equation $|a_p(f)|\,|a(T;f)| \det(T)^{-k/2} \le B\left(p^k + p^{k-1} + p^{k-2} + p^{k-3}\right)$, we obtain the desired result by taking the supremum over $T > 0$.

A similar argument shows the inequality for $a_{1,p^2}(f)$. □

If $a \in \mathbb{Z}$ and $|a| < C$, then we can recover $a \in \mathbb{Z}$ from its congruence class modulo m whenever $m > 2C$. For our purposes, we might as well work with a *prime* modulus m, and indeed, because of the needed pth roots of unity, we choose a large prime m such that $m \equiv 1 \pmod{p}$ and work in $R = \mathbb{Z}[\zeta_p]/\mathfrak{m}$ where $\mathfrak{m}$ is a fixed choice of split prime above m, and we compute the expansion (6.5.2) in $R[[q]]$ as

$$a_p(f) \equiv \frac{1}{\phi_s^*(f)} \sum_j \phi_s^*(f \mid M_j) \pmod{\mathfrak{m}}$$

and then lift the result to $\mathbb{Z} \subseteq \mathbb{Z}[\zeta_p]$. The computational benefit is that we may replace ζ_p by an integer and compute modulo m.

Example 6.7.3. Let $f_{587}^- \in S_2(K(587))^-$ be the Borcherds product defined in (6.2.8). We choose $t_0 = \begin{pmatrix} 4 & -137/2 \\ -137/2 & 1174 \end{pmatrix}$ and have $a(t_0, f) = -1$. We used $s = \begin{pmatrix} 2348 & 137 \\ 137 & 8 \end{pmatrix}$ and target exponent $e = \operatorname{tr}(st_0) = 15$. We used the finite field method in our computations, which required a choice of a prime modulus m and an integer γ such that $\gamma \not\equiv 1 \pmod{m}$ and $\gamma^p \equiv 1 \pmod{m}$. The modulus m must be chosen large enough so that $m > \lfloor 2C \rfloor$ where $C = p^2(1+1/p)(1+1/p^2)$ from Proposition 6.7.1. The code was written in C++ using FLINT for operations of polynomials in one variable modulo an integer, and the computation of the restriction method to compute $a_{41}(f_{587}^-)$ took less than 2 hours on a typical CPU. The computation of $a_{1,p^2}(f)$ for $p \leq 11$ took just a few minutes.

7. Verifying paramodularity

In this section, we carry out the Faltings–Serre method for our case of interest $\mathrm{G} = \mathrm{GSp}_4$ and $\ell = 2$, proving our main Theorem 1.2.1 as well as the other two advertised cases. We employ the conventions and notation of section 4, in particular for Galois representations and L-functions.

7.1. The case $N = 277$.

Let $X = X_{277}$ be the smooth projective curve over $\mathbb{Q}$ given by the equation

$$X\colon y^2 + (x^3 + x^2 + x + 1)y = -x^2 - x \tag{7.1.1}$$

with LMFDB label 277.a.277.1, or equivalently by

$$y^2 + y = x^5 - 2x^3 + 2x^2 - x. \tag{7.1.2}$$

Both models are minimal with discriminant $\Delta = 277$. Let $A = A_{277} = \operatorname{Jac} X_{277}$ be the Jacobian of X_{277}, a principally polarized abelian surface over $\mathbb{Q}$ of conductor 277. Let $f = f_{277} \in S_2(K(277))$ be the Siegel modular form of weight 2 constructed in (6.2.2).

Our main result (implying Theorem 1.2.1) is as follows.

Theorem 7.1.3. *For all primes p, we have $L_p(A_{277}, T) = Q_p(f_{277}, T)$. In particular, we have $L(A_{277}, s) = L(f_{277}, s, \mathrm{spin})$ and the abelian surface A_{277} is paramodular.*

To ease notation, we now dispense with subscripts. To prove this theorem, we use the strategy described in section 3.2, with the further practical improvements from section 3.3. Attached to A by (4.1.3) and to f by Theorem 4.3.4 and by the remarks afterward are 2-adic Galois representations

$$\rho_A, \rho_f\colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(\mathbb{Q}_2^{\mathrm{al}})$$

where $S = \{2, 277, \infty\}$ such that $\det \rho_A = \det \rho_f = \chi_2^2$ the square of the 2-adic cyclotomic character. Our first task is to verify equivalence of residual representations. We start with Lemma 4.3.8(a), which allows us to conclude that the residual representations $\overline{\rho}_A^{\mathrm{ss}}, \overline{\rho}_f^{\mathrm{ss}}\colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(\mathbb{F}_2)$ take values in $\mathbb{F}_2$.

Lemma 7.1.4. *The residual representations $\overline{\rho}_A, \overline{\rho}_f\colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(\mathbb{F}_2)$ are equivalent and have absolutely irreducible image $S_5(b)$.*

Proof. We apply Algorithm 2.2.3. The representation $\overline{\rho}_A$ is given by the action on $A[2]$; completing the square in (7.1.2) to obtain the model $y^2 = g(x) = 4x^5 - 8x^3 + 8x^2 - 4x + 1$ we obtain $\overline{\rho}_A$ via the action on the roots of $g(x)$, which we verify is isomorphic to $G = S_5(b)$

as the elements of order 3 have trace 1 by (5.1.8). As implied by the general theory, the field $\mathbb{Q}(A[2])$ is ramified only at $2, 277$.

For $\overline{\rho}_f$, we only have indirect access to the Galois representation. By (6.2.4), we have

$$\det(1 - \overline{\rho}_f(\mathrm{Frob}_3)T) = 1 + T + T^2 + T^3 + T^4 \in \mathbb{F}_2[T],$$

so $\operatorname{img} \overline{\rho}_f$ contains an element of order 5. Similarly Frob_5 has order divisible by 3, so $\operatorname{img} \overline{\rho}_f$ is isomorphic to one of A_5, S_5, A_6, S_6. Therefore the fixed field under $\ker \overline{\rho}_f$ is the splitting field of an irreducible, separable polynomial $g(x)$ of degree 5 or 6. Let $F := \mathbb{Q}[x]/(g(x))$; then F is unramified away from $2, 277$. But we know a bit more: by Lemma 4.3.10, the 277-valuation of the Artin conductor of $\overline{\rho}_f$ is at most 1, so $\mathrm{ord}_{277}(d_F) \leq 1$. A Hunter search, or looking up the possible fields in the database of Jones–Roberts [36], shows that there are no such degree 6 polynomials, and exactly two polynomials of degree 5, namely $x^5 - x^4 + 2x^2 - x + 1$ and $x^5 - x^4 + 4x^3 + 5x - 1$. Both polynomials have the same Galois closure, with Galois group S_5; we need to distinguish the representations afforded by the inclusion $S_5 \subseteq S_6$ and the fixed representation (5.1.1). We refer to (5.1.8): for the second one Frob_3 does not have order 5, so we must have a match with the representation afforded by the first one. □

With Lemma 7.1.4 in hand, we apply Lemma 4.3.8(b) to conclude that our 2-adic representations descend to $\rho_A, \rho_f \colon \mathrm{Gal}_{\mathbb{Q},S} \to \mathrm{GSp}_4(\mathbb{Z}_2)$. We now finish the proof of the theorem.

Proof of Theorem 7.1.3. We apply Algorithm 2.4.1. Step 1 was done in Lemma 7.1.4, and the residual representations have a common image

$$G := \operatorname{img} \overline{\rho} \leq \mathrm{GSp}_4(\mathbb{F}_2) = \mathrm{Sp}_4(\mathbb{F}_2)$$

with $G \simeq S_5(b)$. Let K be the fixed field under $\ker \overline{\rho}$, so $\mathrm{Gal}(K \,|\, \mathbb{Q}) \simeq G$ under $\overline{\rho}$.

Using Theorem 5.3.3, we now find all obstructing extension groups E, an exact core-free subgroup $D \leq E$, and a list of conjugacy classes of obstructing elements. We refer to the field diagram (5.3.2). The extension $K_0 = K^H$ has degree 10, explicitly it is given by adjoining a root of the polynomial

$$x^{10} + 3x^9 + x^8 - 10x^7 - 17x^6 - 7x^5 + 11x^4 + 18x^3 + 13x^2 + 5x + 1.$$

The possible obstructing extensions $\varphi \colon \mathrm{Gal}(L \,|\, \mathbb{Q}) \hookrightarrow E$ are obtained as the Galois closure of the quadratic extension $L_0 \supseteq K_0$, still unramified away from S so they may be constructed using class field theory: we find there are 4095 quadratic extensions $L_0 \supseteq K_0$ unramified away from S. To write down polynomials (not necessarily small) that represent these fields takes about 5 minutes; as we developed the algorithm, we found it convenient to optimize these polynomials (using polredabs), which took about 6 hours. In the course of the algorithm we consider 24062 obstructing pairs (L, φ).

For each such obstructing pair (L, φ), we compute a small prime $p \neq 2, 277$ such that the conjugacy class of Frob_p is obstructing, according to the stages of section 3.3. Computing obstructing primes by their L_0-cycle type as in Step 4′, we obtain the list of primes $\{3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 53\}$; going a bit further, considering obstructing primes by the pair of L_0, K_0-cycle type as in Step 4″, we manage only to remove the prime $p = 53$ from the list (but reduce the sizes of primes in many cases), so we refine the list of primes to those with $p \leq 43$. The total running time for this step was about 90 minutes on a standard CPU.

There are 8 pairs (L, φ) that require $p = 53$. The field L_0 generated by a root of

$$x^{20} + 121x^{18} + 7459x^{16} + 286418x^{14} + 7324711x^{12} + 126372663x^{10} + 1387797423x^8 + 7013797890x^6 - 30031807329x^4 - 582846604659x^2 - 1630793025157$$

has Galois closure L with $\mathrm{Gal}(L \mid \mathbb{Q}) \simeq E \leq \mathsf{sp}_4(\mathbb{F}_2) \rtimes G$ with $\#E = 2^{10}5!$. There are four outer automorphisms ξ, and with respect to one of these, we find that Frob_5 is an obstructing conjugacy class based on the L_0, K_0-cycle type pair $6^3 1^2, 6^1 3^1 1^1$ but Frob_{53} is the first obstructing prime based *only* on the L_0-cycle type $8^1 4^2 2^2$ (and this cycle type works for all four ξ).

We are now in Step 5 of the algorithm, and to conclude we will show that $\operatorname{tr} \rho_A(\mathrm{Frob}_p) = \operatorname{tr} \rho_f(\mathrm{Frob}_p)$ for all $p \leq 43$. The former traces can be done by counting points, the latter traces were computed using the method in Example 6.6.1, and we check that they are equal, completing the proof. (In fact, we went further than necessary and checked the equality of traces for all $p \leq 97$.) □

7.2. **The case $N = 353$.** We now turn to a case with residual image $S_3 \wr C_2$. Let $X = X_{353}$ be the genus 2 curve with LMFDB label 353.a.353.1 defined by

$$X \colon y^2 + (x^3 + x + 1)y = x^2$$

and $A = A_{353} = \operatorname{Jac} X$, a typical abelian surface of conductor 353. Let $f = f_{353} \in S_2(K(353))$ be the paramodular form constructed in (6.2.6).

Theorem 7.2.1. *For all primes p, we have $L_p(A_{353}, T) = Q_p(f_{353}, T)$. In particular, $L(A, s) = L(f_{353}, s, \mathrm{spin})$ and the abelian surface A_{353} is paramodular.*

Proof. The proof is similar to that of Theorem 7.1.3, but with some slightly different arguments. To supplement the data (6.2.7), we compute $a_p(f), a_{1,p^2}(f)$ for $p \leq 11$, and counting points yields equality of the additional Euler factors

$$\begin{aligned} L_5(A, T) = Q_5(f, T) &= 1 - T + 2T^2 - 5T^3 + 25T^4, \\ L_7(A, T) = Q_7(f, T) &= 1 - 6T^2 + 49T^4, \\ L_{11}(A, T) = Q_{11}(f, T) &= 1 - 2T + T^2 - 22T^3 + 121T^4. \end{aligned} \tag{7.2.2}$$

Our first task is to verify that the mod 2 representations $\overline{\rho}_A$ and $\overline{\rho}_f$ are equivalent and absolutely irreducible. For A, we find the 2-torsion field generated by the splitting field of the polynomial $x^6 + 2x^4 + 2x^3 + 5x^2 + 2x + 1$ and Galois group $S_3 \wr C_2$.

Let K be the fixed field of $\ker \overline{\rho}_f$ and $G := \mathrm{Gal}(K \mid \mathbb{Q})$. Since $L_3(A, T) \equiv 1 + T + T^3 + T^4 \pmod 2$ we see that G has an element of order 3 or 6 with trace 0. Since $L_{11}(A, T) \equiv 1 + T^2 + T^4$, we see G has an element of order 3 or 6 with trace 1. Squaring such elements preserves their trace, so G contains elements of order 3 with either trace. Thus $G \leq S_6$ has an element with cycle decomposition 3^1 and one with cycle decomposition 3^2. Listing all subgroups of S_6 with this property, we see that G must be isomorphic to one of the permutation groups

$$C_3^2, C_3 : S_3, C_3 \times S_3 \text{ (twice)}, C_3 : S_3 \cdot C_2, S_3^2 \text{ (twice)}, S_3 \wr C_2, A_6, S_6.$$

The subgroups in this list that are intransitive are $C_3^2, C_3 : S_3, C_3 \times S_3, S_3^2$. The groups $C_3^2, C_3 \times S_3$ have C_3 as a quotient, and by the Kronecker–Weber theorem there are no C_3-extensions unramified outside 2 and 353 since $353 \equiv 2 \pmod 3$. The groups $C_3 : S_3$ and S_3^2

have as quotient S_3, but there is a unique S_3 extension ramified only at 2 and 353 (verified by a class field calculation and the Jones–Roberts database [36]) defined by $x^3-x^2-6x+14$, and we compute that there are no cyclic cubic extensions of this field unramified away from primes dividing $2, 353$. This leaves the transitive groups $C_3 : S_3 \cdot C_2, S_3 \wr C_2, A_6, S_6$ arising as the normal closure of a degree 6 subfield K'. If $G = C_3 : S_3 \cdot C_2$, then as in the proof of Proposition 5.2.4, we have $\operatorname{ord}_{353} d_{K'} = 0, 1, 3$ but if $\operatorname{ord}_{353} d_{K'} = 3$ then G contains an element with cycle structure 2^3, a contradiction. Combined with Proposition 5.2.4 in the remaining cases, we have $\operatorname{ord}_{353} d_{K'} \leq 1$. Again by consulting the Jones–Roberts database [36], we find exactly two candidates, the extensions defined by $x^6 - 2x^5 + 2x^4 - x^2 + 1$ and $x^6 - 2x^5 - 3x^4 + 4x^3 + x^2 - 6x + 1$. In the first extension, Frob_3 has order 6 contradicting $Q_3(f, T) \equiv 1+T^4 \pmod 2$, so we have the latter, and G is isomorphic to $S_3 \wr C_2$. Finally, since the trace of $\overline{\rho}_f(\mathrm{Frob}_3)$ equals that of A, we see that the two residual images are isomorphic and absolutely irreducible (recall that there are two embeddings of $S_3 \wr C_2$ into $\mathrm{GSp}_4(\mathbb{F}_2)$ up to inner automorphisms, and they differ in the trace of order 3 and 6 elements).

Next, using Theorem 5.3.3 we compute the extension K_0 corresponding to the core-free subgroup C_2^2, defined by

$$x^{18} - 10x^{14} + 3x^{12} + 25x^{10} - 5x^8 - 19x^6 + 5x^2 + 1. \tag{7.2.3}$$

Using computational class field theory, we list all quadratic extensions $L_0 \supseteq K_0$ unramified away from primes above $2, 353$. We find that there are 65535 such extensions. For each extension, we find an obstructing element; after computing for just over 5 hours on a standard CPU (about 0.2 seconds per field) we find the list of primes

$$\{3, 5, 7, 11, 13, 19, 23, 29, 31, 37, 41, 43, 53, 97, 137\}. \tag{7.2.4}$$

(The prime $p = 181$ arose from 2 extensions L_0 and 4 maps φ each looking only at cycle types, but by identifying the precise conjugacy classes we find obstructing classes for $p = 5, 137$.)

To conclude, using the floating point algorithm we compute $\operatorname{tr} \rho_f(\mathrm{Frob}_p)$ for all primes $p \leq 109$ as well as the primes $p = 137, 139, 251$ (for robustness) in 29 hours on a standard CPU, and we see they agree with the traces obtained from point counts on X, completing the proof. □

Example 7.2.5. We pause to consider an extreme example where the refinement in section 3.3 provides a significant improvement. Consider the extension defined by adjoining a square root of the element

$$-430a^{16} + 302a^{14} + 3956a^{12} - 3904a^{10} - 6944a^8 + 5348a^6 + 3628a^4 - 1454a^2 - 510$$

where a is a root of (7.2.3), the defining polynomial for K_0.

There are 4 outer automorphisms giving rise to possible maps φ: but in fact, we will see below that only 2 of these maps extend $\overline{\rho}$, which is to say the other 2 do not preserve the residual representation. If we only consider cycle types that obstruct all 4 possible maps φ as in Step 4′, we have the types $8^4 2^2, 4^6 2^2 1^8, 4^2 2^{10} 1^8$. For one of these 4 extensions, the smallest prime p with this cycle type is $p = 251$. If we push further in this extension, and look at the L_0-cycle type and the order in K_0, we compute that $p = 101$ works. Going even further and using L_0, K_0-cycle type, we find that $p = 11$ works!

7.3. **The case $N = 587$.** We conclude with one final case. Let $X = X_{587}$ be the genus 2 curve with LMFDB label 587.a.587.1 defined by

$$X\colon y^2 + (x^3 + x + 1)y = -x^2 - x$$

and $A = A_{587} = \operatorname{Jac} X_{587}$, a typical abelian surface of conductor 587 and rank 1. Let $f = f_{587}^- \in S_2(K(587))$ be the paramodular form constructed using (6.2.9).

Theorem 7.3.1. *For all primes p we have $L_p(A_{587}, T) = Q_p(f_{587}^-, T)$, and A_{587} is paramodular.*

Proof. We first verify that the mod 2 representations $\overline{\rho}_A$ and $\overline{\rho}_f$ are equivalent and absolutely irreducible. For A, we find the 2-torsion field generated by the splitting field of the polynomial $x^6 - 2x^5 + 2x^4 - x^2 + 2x - 1$ with Galois group $G = S_6$. For f, we have

$$Q_3(f, T) = 1 + 4T + 9T^2 + 12T^3 + 9T^4 \equiv 1 + T^2 + T^4 \pmod 2$$

and

$$Q_{11}(f, T) = 1 + T - T^2 + 11T^3 + 121T^4 \equiv 1 + T + T^2 + T^3 + T^4 \pmod 2$$

by Poor–Yuen [45, Table 5] and Example 6.7.3. In particular, the residual image has order divisible by 3 and 5.

The subgroups of S_6 (up to isomorphisms) of order divisible by 15 are:

$$A_5, S_5, A_6, S_6.$$

In all cases, there exists a polynomial of degree 5 or 6 unramified outside $\{2, 587\}$ and we can choose them such that the discriminant valuation is at most 1 at 587 by Proposition 5.2.4. By [36] there are only two degree 5 polynomials with field discriminant having valuation 1 at 587, namely: $x^5 - x^3 - x - 2$ and $x^5 + 2x^3 - 8x^2 - 13x - 8$ and two degree 6 polynomials with field discriminant having valuation 1 at 587: $x^6 - 2x^5 + 2x^4 - x^2 + 2x - 1$ and $x^6 - 2x^5 + 3x^4 + 4x^3 - 2x^2 - 4x + 2$. For the degree 5 polynomials, the first field has Frob_3 of order 4 (then it would have even trace) while Frob_{11} has order 2 in the second field. Regarding the degree six ones, in the second extension Frob_{11} has order 2, but odd trace in A. We deduce that the residual representation of f_{587}^- correponds then to the same extension as A, and since both representations have the same trace at Frob_3, we deduce that they are indeed equivalent and absolutely irreducible.

By Theorem 5.3.3 we are led to compute all quadratic extensions of the degree 20 extension

$$x^{20} + x^{18} - 4x^{17} - 3x^{16} - 2x^{15} + 7x^{14} - 6x^{13} - 18x^{12} - 8x^{11} + 8x^{10} + \\ + 8x^9 - 18x^8 + 6x^7 + 7x^6 + 2x^5 - 3x^4 + 4x^3 + x^2 + 1. \tag{7.3.2}$$

We find that there are $2^{19} - 1 = 524287$ such extensions. Writing down minimal polynomials (not necessarily small) that represent these fields takes about 10 minutes; for convenience, we also computed optimized representatives, which took many CPU weeks.

Finding an obstructing element for each of them, we find the list of primes to verify:

$$\{3, 5, 7, 11, 13, 17, 19, 23, 29, 37, 41\}. \tag{7.3.3}$$

The total CPU time to compute this list of primes was about 2.5 hours (about 0.2 seconds per field). Finally, we computed the corresponding traces above and they match, completing the proof. □

Appendix: Reduction of G-covariant bilinear forms, by J.-P. Serre

Introduction. This note is intended as a complement to [54] where reductions of G-invariant bilinear forms modulo primes were studied. Indeed, in most applications to ℓ-adic representations the natural bilinear forms are not G-invariant; they are only covariant with respect to a character of the group G. The simplest example of this is the $\mathbb{Q}_\ell$-Tate module V_ℓ of an abelian variety A over a field F of characteristic $\neq \ell$: a polarization of A defines a nondegenerate alternating form B on V_ℓ, which is covariant under the action of the absolute Galois group $\Gamma_F = \mathrm{Gal}(F_s/F)$, namely:

$$B(gx, gy) = \chi_\ell(g)B(x, y) \quad \text{for every } g \in \Gamma_F, x, y \in V_\ell,$$

where χ_ℓ is the ℓ-cyclotomic character.

We shall see that the results of [54] extend to the covariant case, with practically the same proofs.

1. The setting. It is almost the same as that of [54]. Namely:

G is a group,

K is a field with a discrete valuation,

R is the ring of integers of K,

π is a uniformizer of K,

$k = R/\pi R$ is the residue field,

$\varepsilon\colon G \to R^\times$ is a homomorphism,

V is a finite dimension K-vector space on which G acts, in such a way that there exists an R-lattice of V which is G-stable ("bounded action"),

V_k is the k-vector space obtained by the semisimplification of the $k[G]$-module $L/\pi L$, where L is a G-stable lattice of V; up to isomorphism, it is independent from the choice of L,

B is a symmetric (resp. alternating) nondegenerate K-bilinear form on V, which is ε-covariant under the action of G, i.e.

$$B(gx, gy) = \varepsilon(g)B(x, y) \quad \text{for } g \in G, x, y \in V. \tag{1.1}$$

2. Statement of the theorems. The main theorem is the analogue of Theorem A of [54]. Namely:

Theorem 1. *There exists a nondegenerate symmetric (resp. alternating) k-bilinear form on V_k such that*

$$b(gx, gy) = \varepsilon(g)b(x, y) \quad \textit{for } g \in G, x, y \in V_k. \tag{1.2}$$

As in [54], the proof will use the following complement to a classical theorem of Brauer and Nesbitt:

Theorem 2. *Let E be a finite dimensional $k[G]$-module endowed with a nondegenerate symmetric (resp. alternating) k-bilinear form b having property (1.2). Then, the semisimplification E^{ss} of E has a k-bilinear form with the same properties as b.*

3. Proof of theorem 2. Use induction on $\dim E$. Assume $E \neq 0$ and choose a minimal nonzero G-submodule S of E. Let $H \subset E$ be the orthogonal subspace of S with respect to b. Since S is minimal, there are two possibilities:

a) $H \cap S = 0$, i.e. the restriction of b to S is nondegenerate. In that case, we have $E^{\mathrm{ss}} = S \oplus H^{\mathrm{ss}}$ and we apply the induction hypothesis to H.

b) $H \cap S = S$, i.e. S is totally isotropic for b. We have $E^{\mathrm{ss}} = (S \oplus E/H) \oplus (H/S)^{\mathrm{ss}}$.

The induction hypothesis applies to $(H/S)^{\mathrm{ss}}$. As for the first factor $S \oplus E/H$, one defines a bilinear form $b_1(x, y)$ on it by the following rule: if x, y both belong to S, or to E/H, then $b_1(x, y) = 0$; if $x \in S$ and $y \in E/H$, then $b_1(x, y) = b(x, y')$ where y' is any representative of y in E; if $x \in E/H$ and $y \in S$, then $b_1(x, y) = b_1(y, x)$ in the symmetric case and $b_1(x, y) = -b_1(y, x)$ in the alternating case. It is clear that the form b_1 has the required properties.

4. Proof of Theorem 1. The first step ([54, Theorem 5.2.1]) is to show the existence of a lattice L in V, which is G-stable, and almost self-dual, i.e. $\pi L' \subset L \subset L'$, where L' is the dual of L (note that formula (1.1) implies that the dual of a G-stable lattice is G-stable). This is done by choosing a G-stable lattice M, and defining L as the "lower middle" $m_-(M, M')$ of M and its dual M' :

$m_-(M, M')$ = smallest lattice containing $\pi^n M \cap \pi^{-n} M'$ for every $n \in \mathbb{Z}$.

It is proved in [54, Theorem 3.1.1] that $m_-(M, M')$ is an almost self-dual lattice.

The second step is to define a bilinear form b on the k-vector space $E = L/\pi L' \oplus L'/L$ by using the reduction mod π of B on $L/\pi L'$, and of πB on L'/L. It is clear that b is nondegenerate, ε-covariant, and symmetric (resp. alternating) if B is. By Theorem 2, the semisimplification E^{ss} of E has a bilinear form with the required properties. Since E^{ss} is isomorphic to V_k, this proves Theorem 1.

References

[1] Jeffrey D. Achter, *Detecting complex multiplication*, Computational aspects of algebraic curves, Lecture Notes Ser. Comput., vol. 13, World Sci. Publ., Hackensack, NJ, 2005, 38–50.

[2] Tobias Berger and Krzysztof Klosin (with an appendix by Cris Poor, Jerry Shurman, and David S. Yuen), *Deformations of Saito–Kurokawa type and the paramodular conjecture*, 2017, preprint, `arXiv:1710.10228`, accepted to Amer. J. Math.

[3] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), vol. 3–4, 235–265.

[4] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939.

[5] Tobias Berger, Lassina Dembélé, Ariel Pacetti, and Mehmet Haluk Şengün, *Theta lifts of Bianchi modular forms and applications to paramodularity*, J. Lond. Math. Soc. (2), **92** (2015), no. 2, 353–370.

[6] George Boxer, Frank Calegari, Toby Gee, and Vincent Pilloni, *Abelian surfaces over totally real fields are potentially modular*, 2018, `arXiv:1812.09269`.

[7] Armand Brumer and Kenneth Kramer, *Paramodular abelian varieties of odd conductor*, Trans. Amer. Math. Soc. **366** (2014), 2463–2516.

[8] Armand Brumer and Kenneth Kramer, *Certain abelian varieties bad at only one prime*, Algebra and Number Theory **12** (2018), 1027–1071.

[9] Armand Brumer and Kenneth Kramer, *Corrigendum to "Paramodular abelian varieties of odd conductor"*, Trans. Amer. Math. Soc., Published electronically May 1, 2019.

[10] Paramodularity code repository, `https://gitlab.fing.edu.uy/tornaria/modularity`.

[11] Andrew R. Booker, Jeroen Sijsling, Andrew V. Sutherland, John Voight, and Dan Yasaki, *Sato–Tate groups and modularity for atypical genus* 2 *curves*, preprint.
[12] Frank Calegari and David Geraghty, *Minimal modularity lifting for non-regular symplectic representations*, submmited, `http://www.math.uchicago.edu/~fcale/papers/Siegel.pdf`.
[13] Henri Carayol, *Formes modulaires et représentations galoisiennes à valeurs dans un anneau local complet*, p-adic monodromy and the Birch and Swinnerton-Dyer conjecture (Boston, MA, 1991), Contemp. Math., vol. 165, Amer. Math. Soc., Providence, RI, 1994, 213–237.
[14] Henri Cohen, *A course in computational algebraic number theory*, Springer-Verlag, Berlin, 1993.
[15] Henri Cohen, *Advanced topics in computational number theory*, Grad. Texts in Math., vol. 193, Springer-Verlag, 2000.
[16] Owen Colman, Alexandru Ghitza, and Nathan C. Ryan, *Analytic evaluation of Hecke eigenvalues for Siegel modular forms of degree two*, Proceedings of the thirteenth Algorithmic Number Theory Symposium (Madison, WI, 2018), eds. R. Scheidler and J. Sorenson, Open Book Series 2, MSP, Berkeley, CA, 2019, 207–220.
[17] Lassina Dembélé and Abhinav Kumar, *Examples of abelian surfaces with everywhere good reduction*, Math. Ann. **364** (2016), no. 3-4, 1365–1392.
[18] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti, *Proving modularity for a given elliptic curve over an imaginary quadratic field*, Math. Comp. **79** (2010), no. 270, 1145–1170.
[19] Tim Dokchitser and Vladimir Dokchitser, *Identifying Frobenius elements in Galois groups*, Algebra Number Theory **2013** (7), no. 6, 1325–1352.
[20] Martin Eichler and Don Zagier, *The theory of Jacobi forms*, Progress in Mathematics 55, Birkhäuser Verlag, Berlin 1985.
[21] David Farmer, Sally Koutsoliotas, and Stefan Lemurell, *L-functions with rational integer coefficients I: degree 4 and weight 0*, preprint.
[22] Jean-Marc Fontaine, *Il n'y a pas de variété abélienne sur* $\mathbb{Z}$, Invent. Math. **81** (1985), 515–538.
[23] Eberhard Freitag, *Siegelsche Modulfunktionen*, Grundlehren der mathematischen Wissenschaften, Band **254**, Berlin-Heidelberg-New York: Springer-Verlag, 1983.
[24] Fernando Q. Gouvêa, *Deformations of Galois representations*, Arithmetic algebraic geometry (Park City, UT, 1989), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, 233–406.
[25] Loïc Grenié, *Comparison of semi-simplifications of Galois representations*, J. Algebra **316** (2007), 608–618.
[26] Valery Gritsenko, *Arithmetical lifting and its applications*, Number theory (Paris 1992–1993), 103–126, London Math. Soc. Lecture Note Ser., 215, Cambridge Univ. Press, Cambridge, 1995.
[27] Valeri Gritsenko, Cris Poor, and David S. Yuen, *Antisymmetric paramodular forms of weights 2 and 3*, Int. Math. Res. Not., online publication February 2019.
[28] Valeri Gritsenko, Nils-Peter Skoruppa, and Don Zagier, *Theta blocks*, preprint.
[29] Alexandre Grothendieck, *Séminaire de Géométrie Algébrique du Bois Marie, 1967–69, Groupes de monodromie en géométrie algébrique (SGA 7)*, vol. 1, Lecture Notes in Mathematics, vol. 288, Berlin–New York, Springer-Verlag, 1972.
[30] David Harvey, *Counting points on hyperelliptic curves in average polynomial time*, Ann. of Math. (2) **179** (2014), no. 2, 783–803.
[31] David Harvey and Andrew V. Sutherland, *Computing Hasse-Witt matrices of hyperelliptic curves in average polynomial time, II*, Frobenius distributions: Lang-Trotter and Sato-Tate conjectures, Contemporary Math., vol. 663, Amer. Math. Soc., Providence, 2016, 127–147.
[32] Ben Howard, John Millson, Andrew Snowden and Ravi Vakil, *A description of the outer automorphism of* S_6*, and the invariants of six points in projective space*, J. Comb. Theory Ser. A, 115 (2008), no. 7, 1296-1303.
[33] Jennifer Johnson-Leung and Brooks Roberts, *Siegel modular forms of degree two attached to Hilbert modular forms*, J. Number Theory **132** (2012), no. 4, 543–564.
[34] Jennifer Johnson-Leung and Brooks Roberts, *Twisting of paramodular vectors*, Int. J. Number Theory **10** (2014), no. 4, 1043–1065.
[35] Jennifer Johnson-Leung and Brooks Roberts, *Twisting of Siegel paramodular forms*, Int. J. Number Theory **13** (2017), no. 7, 1755–1854.

[36] John Jones and David P. Roberts, *A database of number fields*, LMS J. Comput. Math. **17** (2014), no. 1, 595–618.
[37] Andrei Jorza, *p-adic Families and Galois Representations for* GSp(4) *and* GL(2), Math. Research Letters **19** (2012), no. 05, 987–996.
[38] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. I*, Invent. Math. **178** (2009), no. 3, 485–504.
[39] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture. II*, Invent. Math. **178** (2009), no. 3, 505–586.
[40] Gérard Laumon, *Fonctions zetas des variétés de Siegel de dimension trois*, Astérisque **302** (2005), 1–66.
[41] Ron Livné, *Cubic exponential sums and Galois representations*, Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985), Contemp. Math., vol. 67, Amer. Math. Soc., Providence, RI, 1987, 247–261.
[42] Chung Pang Mok, *Galois representations attached to automorphic forms on* GL_2 *over CM fields*, Compos. Math. **150** (2014), no. 4, 523–567.
[43] Vincent Pilloni, *Modularité, formes de Siegel et surfaces abéliennes*, J. Reine Angew. Math. **666** (2012), 35–82.
[44] Cris Poor, Jerry Shurman, and David S. Yuen, *Nonlift weight two paramodular eigenform constructions*, preprint, 2018, `arXiv:1805.04137`.
[45] Cris Poor and David S. Yuen, *Computations of spaces of Siegel modular cusp forms*, J. Math. Soc. Japan **59** (2007), no. 1, 185–222.
[46] Cris Poor and David S. Yuen, *Paramodular cusp forms*, Math. Comp. **84** (2015), no. 293, 1401–1438.
[47] Kenneth A. Ribet, *Endomorphisms of semi-stable abelian varieties over number fields*, Annals of Math. (2) **1975** (101), 555–562.
[48] Kenneth A. Ribet, *Abelian varieties over* $\mathbb{Q}$ *and modular forms*, Algebra and topology 1992 (Taejŏn), Korea Adv. Inst. Sci. Tech., Taejŏn, 1992, 53–79. Reprinted in: Modular curves and abelian varieties, Progr. Math., vol. 224, Birkhäuser, Basel, 2004, 241–261.
[49] Brooks Roberts and Ralf Schmidt, *On modular forms for the paramodular groups*, Automorphic forms and zeta functions, World Sci. Publ., Hackensack, NJ, (2006), 334–364.
[50] Brooks Roberts and Ralf Schmidt, *Local newforms for* GSp(4), Lecture notes in math., vol. 1918, Springer, Berlin, 2007.
[51] Ralf Schmidt, *Packet structure and paramodular forms*, Trans. Amer. Math. Soc. **370** (2018), 3085–3112.
[52] Matthias Schütt, *On the modularity of three Calabi–Yau threefolds with bad reduction at 11*, Canad. Math. Bull. **49** (2006), 296–312.
[53] Jean-Pierre Serre, *Oeuvres/Collected papers IV (1985-1998)*, Springer Collected Works in Math., Springer, Heidelberg, 2000, no. 135, 27–32.
[54] Jean-Pierre Serre, *On the mod p reduction of orthogonal representations*, Lie Groups, Geometry, and Representation Theory, Progress in Math., vol. 326, eds. Victor G. Kac and Vladimir L. Popov, Birkhäuser Basel, Switzerland, 2018, 527–540.
[55] Viggo Stoltenberg-Hansen and John V. Tucker, Computable rings and fields, *Handbook of computability theory*, ed. Edward R. Griffor, North-Holland, Amsterdam, 1999, 336–447.
[56] Richard Taylor, *Galois representations associated to Siegel modular forms of low weight*, Duke Math. J. **63** (1991), no. 2, 281–332.
[57] Richard Taylor and Teruyoshi Yoshida, *Compatibility of local and global Langlands correspondences*, J. Amer. Math. Soc. **20** (2007), 467–493.
[58] Richard Taylor and Andrew Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. (2), **141** (1995), no. 3, 553–572.
[59] Rainier Weissauer, *Four dimensional Galois representations*, Formes automorphes. II. Le cas du groupe GSp(4), Astérisque **302** (2005), 67–150.
[60] Andrew Wiles, *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. (2) **141** (1995), no. 3, 443–551.

[61] Hiroyuki Yoshida, *Siegel's modular forms and the arithmetic of quadratic forms*, Invent. Math. **60** (1980), 193–248.
[62] Hiroyuki Yoshida, *On generalization of the Shimura-Taniyama conjecture I and II*, Siegel Modular Forms and Abelian Varieties, Proceedings of the 4th Spring Conference on Modular Forms and Related Topics, 2007, 1–26.

Department of Mathematics, Fordham University, Bronx, NY 10458
Email address: brumer@fordham.edu

FAMAF-CIEM, Universidad Nacional de Córdoba. C.P:5000, Córdoba, Argentina.
Email address: apacetti@famaf.unc.edu.ar

Department of Mathematics, Fordham University, Bronx, NY 10458
Email address: poor@fordham.edu

Universidad de la República, Montevideo, Uruguay
Email address: tornaria@cmat.edu.uy

Department of Mathematics, Dartmouth College, 6188 Kemeny Hall, Hanover, NH 03755, USA
Email address: jvoight@gmail.com
URL: http://www.math.dartmouth.edu/~jvoight/

Department of Mathematics, University of Hawaii, Honolulu, HI 96822 USA
Email address: yuen@math.hawaii.edu

Collège de France, 3 rue d'Ulm, Paris
Email address: jpserre691gmail.com