Computing nonsurjective primes associated to Galois representations of genus 2 curves

Barinder S. Banwait, Armand Brumer, Hyun Jong Kim, Zev Klagsbrun, Jacob Mayle, Padmavathi Srinivasan, and Isabel Vogt

Abstract. For a genus 2 curve C over $\mathbb{Q}$ whose Jacobian A admits only trivial geometric endomorphisms, Serre's open image theorem for abelian surfaces asserts that there are only finitely many primes ℓ for which the Galois action on ℓ-torsion points of A is not maximal. Building on work of Dieulefait, we give a practical algorithm to compute this finite set. The key inputs are Mitchell's classification of maximal subgroups of $\mathrm{PSp}_4(\mathbb{F}_\ell)$, sampling of the characteristic polynomials of Frobenius, and the Khare–Wintenberger modularity theorem. The algorithm has been submitted for integration into Sage, executed on all of the genus 2 curves with trivial endomorphism ring in the LMFDB, and the results incorporated into the homepage of each such curve.

1. Introduction

Let $C/\mathbb{Q}$ be a smooth, projective, geometrically integral curve (referred to hereafter as a nice curve) of genus 2, and let A be its Jacobian. We assume throughout that A admits no nontrivial geometric endomorphisms; that is, we assume that $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}$, and we refer to any such abelian variety as typical[1]. We also say that a nice curve is typical if its Jacobian is typical. Let $G_{\mathbb{Q}} \coloneqq \mathrm{Gal}\left(\overline{\mathbb{Q}}/\mathbb{Q}\right)$, let ℓ be a prime, and let $A[\ell] \coloneqq A(\overline{\mathbb{Q}})[\ell]$ denote the ℓ-torsion points of $A(\overline{\mathbb{Q}})$. Let

$$\rho_{A,\ell} : G_{\mathbb{Q}} \to \mathrm{Aut}\left(A[\ell]\right)$$

denote the Galois representation on $A[\ell]$. By fixing a basis for $A[\ell]$, and observing that $A[\ell]$ admits a nondegenerate Galois-equivariant alternating bilinear form, namely the Weil pairing, we may identify the codomain of $\rho_{A,\ell}$ with the general symplectic group $\mathrm{GSp}_4(\mathbb{F}_\ell)$.

In a letter to Vignéras [**Ser00**, Corollaire au Théorème 3], Serre proved an open image theorem for typical abelian varieties of dimensions 2 or 6, or of odd dimensions, generalizing his celebrated open image theorem for elliptic curves [**Ser72**]. More precisely, the set of nonsurjective primes ℓ, namely those for which $\rho_{A,\ell}(G_{\mathbb{Q}})$ is a proper subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$, is finite.

1991 *Mathematics Subject Classification.* 11F80 (primary), 11G10, 11Y16 (secondary).

[1] Abelian varieties with extra endomorphisms define a thin set (in the sense of Serre) in the moduli space $\mathcal{A}_g$ of principally polarized abelian varieties of dimension g and as such are not the typically arising case.

In the elliptic curve case, Serre subsequently provided a conditional upper bound, in terms of the conductor of E, on this finite set [**Ser81**, Théorème 22]; this bound has since been made unconditional [**Coj05, Kra95**]. There are also algorithms to compute the finite set of nonsurjective primes [**Zyw22**], and practical implementations in Sage [**CL12**].

Serre's open image theorem for typical abelian surfaces was made explicit by Dieulefait [**Die02**] who described an algorithm that returns a finite set of primes *containing* the set of nonsurjective primes. In a different direction, Lombardo [**Lom16**, Theorem 1.3] provided an upper bound for the largest nonsurjective prime involving the stable Faltings height of A.

In this paper we develop two algorithms that together provide the exact determination of the nonsurjective primes for C, yielding the main result of our paper as follows.

THEOREM 1.1. *Let $C/\mathbb{Q}$ be a typical genus 2 curve whose Jacobian A has conductor N.*

(1) *Algorithm 3.1 produces a finite list* $\mathsf{PossiblyNonsurjectivePrimes}(C)$ *that provably contains all nonsurjective primes.*

(2) *Given $B > 0$, Algorithm 4.1 produces a sublist* $\mathsf{LikelyNonsurjectivePrimes}(C; B)$ *of* $\mathsf{PossiblyNonsurjectivePrimes}(C)$ *that contains all the nonsurjective primes. If B is sufficiently large, then the elements of* $\mathsf{LikelyNonsurjectivePrimes}(C; B)$ *are precisely the nonsurjective primes of A.*

The two common ingredients in Algorithms 3.1 and 4.1 are Mitchell's 1914 classification of maximal subgroups of $\mathrm{PSp}_4(\mathbb{F}_\ell)$ [**Mit14**] and sampling of characteristic polynomials of Frobenius elements. Indeed, $\rho_{A,\ell}$ is nonsurjective precisely when its image is contained in one of the proper maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. The (integral) characteristic polynomial of Frobenius at a good prime p is computationally accessible since it is determined by counting points on C over $\mathbb{F}_{p^r}$ for $r \leq 2$. The reduction of this polynomial modulo ℓ gives the characteristic polynomial of the action of the Frobenius element on $A[\ell]$. By the Chebotarev density theorem, the images of the Frobenius elements for varying primes p equidistribute over the conjugacy classes of $\rho_{A,\ell}(G_\mathbb{Q})$ and hence let us explore the image.

Algorithm 3.1 makes use of the fact that if the image of $\rho_{A,\ell}$ is nonsurjective, then the characteristic polynomials of Frobenius at auxiliary primes p will be constrained modulo ℓ. Using this idea, Dieulefait worked out the constraints imposed by each type of maximal subgroup for $\rho_{A,\ell}(G_\mathbb{Q})$ to be contained in that subgroup. Our Algorithm 3.1 combines Dieulefait's conditions, with some modest improvements, to produce a finite list $\mathsf{PossiblyNonsurjectivePrimes}(C)$.

Algorithm 4.1 then weeds out the extraneous surjective primes from the list $\mathsf{PossiblyNonsurjectivePrimes}(C)$. Given ℓ, we need to generate enough different elements in the image to rule out containment in any proper maximal subgroup. The key input is a purely group-theoretic condition (Proposition 4.2) that guarantees that a subgroup is all of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ if it contains particular types of elements. This algorithm is probabilistic and depends on the choice of a parameter B which, if sufficiently large, provably establishes nonsurjectivity. The parameter B is a cut-off for the number of Frobenius elements (referred to as *Frobenius witnesses*) that we use to sample the conjugacy classes of $\rho_{A,\ell}(G_\mathbb{Q})$.

As an illustration of the interplay between theory and practice, analyzing the "worst case" run time of each step in Algorithm 3.1 yields a new *theoretical* bound, conditional on the Generalized Riemann Hypothesis (GRH), on the product of all nonsurjective primes in terms of the conductor.

Theorem 1.2. *Let $C/\mathbb{Q}$ be a typical genus 2 curve with conductor N. Assuming the Generalized Riemann Hypothesis (GRH), we have, for any $\epsilon > 0$,*

$$\prod_{\ell \text{ nonsurjective}} \ell \ll \exp(N^{1/2+\epsilon}),$$

where the implied constant is absolute and effectively computable.

While we believe this bound to be far from asymptotically optimal, it is the first bound in the literature expressed in terms of the (effectively computable) conductor.

Naturally one wants to find the sufficiently large value of B in Theorem 1.1(2), which the next result gives, conditional on GRH.

Theorem 1.3. *Let $C/\mathbb{Q}$ be a typical genus 2 curve, and let q be the largest nonsurjective prime for C. Then, assuming GRH, the set* $\mathsf{LikelyNonsurjectivePrimes}(C;B)$ *is precisely the set of nonsurjective primes of C provided that*

$$B \geq \left(4\left[(2q^{11}-1)\log \operatorname{rad}(2qN_A) + 22q^{11}\log(2q)\right] + 5q^{11} + 5\right)^2. \tag{1}$$

The proof of Theorem 1.3 involves an explicit Chebotarev bound due to Bach and Sorenson [**BS96**] that assumes GRH. An unconditional version of Theorem 1.3 can be given using an unconditional Chebotarev result (for instance [**KW22**]), though the bound for B will be exponential in q. In addition, if we assume both GRH and the Artin Holomorphy Conjecture (AHC), then a version of Theorem 1.3 holds with the improved asymptotic bound $B \gg q^{11}\log^2(qN_A)$, but without an explicit constant, see Remark 19.

Unfortunately, the bound from Theorem 1.3 is prohibitively large to use in practice. By way of illustration, consider the typical genus 2 curve of smallest conductor, which has a model

$$y^2 + (x^3+1)y = x^2 + x,$$

and label `249.a.249.1` in the *L-functions and modular forms database* (LMFDB) [**LMF22**]. The output of Algorithm 3.1 is the set $\{2,3,5,7,83\}$. Applying Algorithm 4.1 with $B = 100$ rules out the prime 83, so in particular 7 is a bound on the largest nonsurjective prime for C. Noting that the expression on the right hand side of Equation 1 grows with q, we can apply Theorem 1.3 with $q = 7$ to obtain the value $B = 3.578 \times 10^{23}$ for which $\mathsf{LikelyNonsurjectivePrimes}(C;B)$ coincides with the set of nonsurjective primes associated with C. With this value of B, our implementation of the algorithm was still running after 24 hours, after which we terminated it. Even if the version of Theorem 1.3 that relies on AHC could be made explicit, the value of $q^{11}\log^2(qN_A)$ in this example is on the order of 10^{11}, which would still be a daunting prospect.

To execute the combined algorithm on all typical genus 2 curves in the LMFDB - which at the time of writing constitutes 63,107 curves - we have decided to take a fixed value of $B = 1000$ in Algorithm 4.1. The combined algorithm then takes about 4 hours on MIT's Lovelace computer, a machine with 2 AMD EPYC 7713 2GHz processors, each with 64 cores, and a total of 2TB of memory. The result of this computation of nonsurjective primes for these curves is available to view on the homepage of each curve in the LMFDB. In addition, the combined algorithm has been run on a much larger set of 1,743,737 curves provided to us by Andrew Sutherland. See Section 6 for the results of this computation. The largest Frobenius witness required for the smaller LMFDB dataset was 89, and for Sutherland's larger dataset was 863, so we chose $B = 1000$ to have our implementation work for both datasets.

Remark 1. It would be interesting to know if there is a uniform upper bound on the largest prime ℓ that could occur as a nonsurjective prime for the Jacobian of a typical genus 2 curve defined over $\mathbb{Q}$, analogous to the conjectural bound of 37 for the largest nonsurjective prime for elliptic curves defined over $\mathbb{Q}$ (see e.g. [**BPR13**, Introduction]). Such a bound (if it exists) must be at least 31, as shown by example (12) in Section 6.

Algorithm 4.1 samples the characteristic polynomial of Frobenius $P_p(t)$ for each prime p of good reduction for the curve up to a particular bound and applies Tests 4.4 and 4.5 to $P_p(t)$. Assuming that $\rho_{A,\ell}$ is surjective, we expect that the outcome of these tests should be independent for sufficiently large primes. More precisely,

Theorem 1.4. *Let $C/\mathbb{Q}$ be a typical genus 2 curve with Jacobian A and suppose ℓ is an odd prime such that $\rho_{A,\ell}$ is surjective. There is an effective bound B_0 such that for any $B > B_0$, if we sample the characteristic polynomials $P_p(t)$ of Frobenius for n primes $p \in [B, 2B]$ chosen uniformly and independently at random, the probability that none of these pass Tests 4.4 or 4.5 is less than $3 \cdot \left(\frac{9}{10}\right)^n$.*

Remark 2. In fact, for each prime ℓ satisfying the conditions of Theorem 1.4, there is an explicit constant $c_\ell \leq \frac{9}{10}$ tending to $\frac{3}{4}$ as $\ell \to \infty$ which may be computed using Corollary 5.3 such that the bound $3 \cdot \left(\frac{9}{10}\right)^n$ in Theorem 1.4 can be replaced by $3 \cdot c_\ell^n$. While Theorem 1.4 allows us to consider these probabilities in theory, in practice the bound B_0 also arises from applying the Effective Chebotarev density theorem, so is therefore at least as large as as the bound from Theorem 1.3, and is therefore similarly infeasible.

The combined algorithm to probabilistically determine the nonsurjective primes of a typical genus 2 curve over $\mathbb{Q}$ has been implemented in Sage [**The20**], and it will appear in a future release of this software[2]. Until then, the implementation is available at the following repository:

`https://github.com/ivogt161/abeliansurfaces`

The `README.md` file contains detailed instructions on its use. This repository also contains other scripts in both Sage and Magma [**BCP97**] useful for verifying some of the results of this work; any filenames used in the sequel will refer to the above repository.

Outline of this paper. In Section 2, we begin by reviewing the properties of the characteristic polynomials of Frobenius with a view towards computational aspects. We also recall the classification of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. In Section 3, we explain Algorithm 3.1 and establish Theorem 1.1(1); that is, for each of the maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ listed in Section 2.4, we generate a list of primes that provably contains all primes ℓ for which the mod ℓ image of Galois is contained in this maximal subgroup. Theorem 1.2 is proved in subsection 3.3. In

[2] see `https://github.com/sagemath/sage/issues/30837` for the ticket tracking this integration.

Section 4, we first prove a group-theoretic criterion (Proposition 4.2) for a subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ to equal $\mathrm{GSp}_4(\mathbb{F}_\ell)$. Then, for each ℓ in the finite list from Section 3, we ascertain whether the characteristic polynomials of the Frobenius elements sampled satisfy the group-theoretic criterion; Theorem 1.1(2) and Theorem 1.3 also follow from this study. In Section 5 we prove Theorem 1.4 concerning the probability of output error, assuming that Frobenius elements are uniformly distributed in $\rho_{A,\ell}(G_\mathbb{Q})$. Finally, in Section 6, we close with remarks concerning the execution of the algorithm on the large dataset of genus 2 curves mentioned above, and highlight some interesting examples that arose therein.

ACKNOWLEDGEMENTS. This work was started at a workshop held remotely 'at' the Institute for Computational and Experimental Research in Mathematics (ICERM) in Providence, RI, in May 2020, and was supported by a grant from the Simons Foundation (546235) for the collaboration 'Arithmetic Geometry, Number Theory, and Computation'. It has also been supported by the National Science Foundation under Grant No. DMS-1929284 while the authors were in residence at ICERM during a Collaborate@ICERM project held in May 2022. I.V.'s work was partially supported by NSF grants DMS-1902743 and DMS-2200655.

We are grateful to Noam Elkies for providing interesting examples of genus 2 curves in the literature, Davide Lombardo for helpful discussions related to computing geometric endomorphism rings, and to Andrew Sutherland for providing a dataset of Hecke characteristic polynomials that were used for executing our algorithm on all typical genus 2 curves in the LMFDB, as well as making available the larger dataset of approximately 2 million curves that we ran our algorithm on.

2. Preliminaries

2.1. Notation. Let A be an abelian variety of dimension g defined over $\mathbb{Q}$. Associated to A is a positive integer $N = N_A$ called the conductor (see e.g. [**BK94**, Section 2]). We write N_{sq} for the largest integer such that $N_{\mathrm{sq}}^2 \mid N$.

Let ℓ be a prime. The ℓ-adic Tate module $T_\ell A \simeq \varprojlim A[\ell^n]$ of A is a free $\mathbb{Z}_\ell$-module of rank $2g$. For each prime p, we write $\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ for an absolute Frobenius element associated to p. By a good prime p for an abelian variety A, we mean a prime p for which A has good reduction, or equivalently $p \nmid N_A$. If p is a good prime for A, then the trace a_p of the action of Frob_p on $T_\ell A$ is an integer. See Section 2.2 for a discussion of the characteristic polynomial of Frobenius.

An abelian variety A with geometric endomorphism ring $\mathbb{Z}$ is called typical. A typical genus 2 curve is a nice curve whose Jacobian is a typical abelian surface.

Let V be a 4-dimensional vector space over $\mathbb{F}_\ell$ endowed with a nondegenerate skew-symmetric bilinear form $\langle \cdot, \cdot \rangle$. A subspace $W \subseteq V$ is called isotropic (for $\langle \cdot, \cdot \rangle$) if $\langle w_1, w_2 \rangle = 0$ for all $w_1, w_2 \in W$. A subspace $W \subseteq V$ is called nondegenerate (for $\langle \cdot, \cdot \rangle$) if $\langle \cdot, \cdot \rangle$ restricts to a nondegenerate form on W. The general symplectic group of $(V, \langle \cdot, \cdot \rangle)$ is the subgroup of $\mathrm{GL}(V)$ defined by

$$\mathrm{GSp}(V, \langle \cdot, \cdot \rangle) := \{ M : \exists \ \mathrm{mult}(M) \in \mathbb{F}_\ell^\times : \langle Mv, Mw \rangle = \mathrm{mult}(M) \langle v, w \rangle \ \forall \ v, w \in V \}.$$

The map $M \mapsto \mathrm{mult}(M)$ is a surjective homomorphism from $\mathrm{GSp}(V, \langle \cdot, \cdot \rangle)$ to $\mathbb{F}_\ell^\times$ called the similitude character; its kernel is the symplectic group, denoted $\mathrm{Sp}(V, \langle \cdot, \cdot \rangle)$. Usually the bilinear form is understood from context, and we drop $\langle \cdot, \cdot \rangle$ from the notation.

By a subquotient W of a Galois module U, we mean a Galois module W that admits a surjection $U' \twoheadrightarrow W$ from a subrepresentation U' of U.

Since we are chiefly concerned with the sets $\mathsf{LikelyNonsurjectivePrimes}(C; B)$ and $\mathsf{PossiblyNonsurjectivePrimes}(C)$ for a fixed curve C, we will henceforth, for ease of notation, drop the C from the notation for these sets.

2.2. Integral characteristic polynomial of Frobenius. The theoretical result underlying the whole approach is the following.

Theorem 2.1 (Weil, see [**ST68**, Theorem 3]). *Let A be an abelian variety of dimension g defined over $\mathbb{Q}$ and let p be a prime of good reduction for A. There exists a monic integral polynomial $P_p(t) \in \mathbb{Z}[t]$ of degree $2g$ with constant coefficient p^g such that for any $\ell \neq p$, the polynomial $P_p(t)$ is the characteristic polynomial of the action of Frob_p on $T_\ell A$. Every root of $P_p(t)$ has complex absolute value $p^{1/2}$.*

The polynomials $P_p(t)$ are computationally accessible by counting points on C over $\mathbb{F}_{p^r}$, $r = 1, 2$. See [**Poo17**, Chapter 7] for more details. In fact, $P_p(t)$ can be accessed via the `frobenius_polynomial` command in Sage. In particular, we denote the trace of Frobenius by a_p. By the Grothendieck-Lefschetz trace formula, if $A = \mathrm{Jac}\, C$, p is a prime of good reduction for C, and $\lambda_1, \ldots, \lambda_{2g}$ are the roots of $P_p(t)$, then $\#C(\mathbb{F}_{p^r}) = p^r + 1 - \sum_{i=1}^{2g} \lambda_i^r$.

2.3. The Weil pairing and consequences on the characteristic polynomial of Frobenius. The nondegenerate Weil pairing gives an isomorphism of Galois modules:

$$T_\ell A \simeq (T_\ell A)^\vee \otimes_{\mathbb{Z}_\ell} \mathbb{Z}_\ell(1). \tag{2}$$

The Galois character acting on $\mathbb{Z}_\ell(1)$ is the ℓ-adic cyclotomic character, which we denote by cyc_ℓ. The integral characteristic polynomial for the action of Frob_p on $\mathbb{Z}_\ell(1)$ is simply $t - p$. The integral characteristic polynomial for the action of Frob_p on $(T_\ell A)^\vee$ is the reversed polynomial

$$P_p^\vee(t) = P_p(1/t) \cdot t^{2g}/p^g$$

whose roots are the inverses of the roots of $P_p(t)$.

We now record a few easily verifiable consequences of the nondegeneracy of the Weil pairing when $\dim(A) = 2$.

Lemma 2.2.

(i) *The roots of $P_p(t)$ come in pairs that multiply out to p. In particular, $P_p(t)$ has no root with multiplicity* 3.
(ii) *$P_p(t) = t^4 - a_p t^3 + b_p t^2 - p a_p t + p^2$ for some $a_p, b_p \in \mathbb{Z}$.*
(iii) *If the trace of an element of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is $0 \mod \ell$, then its characteristic polynomial is reducible modulo ℓ. In particular, this applies to $P_p(t)$ when $a_p \equiv 0 \bmod \ell$.*
(iv) *If $A[\ell]$ is a reducible $G_\mathbb{Q}$-module, then $P_p(t)$ is reducible modulo ℓ.*

Proof. Parts (i) and (ii) are immediate from the fact that the non-degenerate Weil pairing allows us to pair up the four roots of $P_p(t)$ into two pairs that each multiply out to p.

For part (iii), suppose that $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ has $\mathrm{tr}(M) = 0$. Then the characteristic polynomial $P_M(t)$ of M is of the form $t^4 + bt^2 + c^2$. When the discriminant of P_M is 0 modulo ℓ, the polynomial P_M has repeated roots and is hence reducible.

So assume that the discriminant of P_M is nonzero modulo ℓ. When $\ell \neq 2$, the result follows from [**Car56**, Theorem 1]. When $\ell = 2$, a direct computation shows that the characteristic polynomial of a trace 0 element of $\mathrm{GSp}_4(\mathbb{F}_2)$ is either $(t+1)^4$ or $(t^2+t+1)^2$, which are both reducible.

Part (iv) is immediate from Theorem 2.1 since $P_p(t) \mod \ell$ by definition is the characteristic polynomial for the action of $\mathrm{Frob}\, p$ on $A[\ell]$. □

2.4. Maximal subgroups of $\mathbf{GSp_4}(\mathbb{F}_\ell)$. Mitchell [**Mit14**] classified the maximal subgroups of $\mathrm{PSp}_4(\mathbb{F}_\ell)$ in 1914. This can be used to deduce the following classification of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with surjective similitude character.

LEMMA 2.3 (Mitchell). *Let V be a 4-dimensional $\mathbb{F}_\ell$-vector space endowed with a nondegenerate skew-symmetric bilinear form ω. Then any proper subgroup G of $\mathrm{GSp}(V,\omega)$ with surjective similitude character is contained in one of the following types of maximal subgroups.*

(1) ***Reducible maximal subgroups***
   (a) *Stabilizer of a 1-dimensional isotropic subspace for ω.*
   (b) *Stabilizer of a 2-dimensional isotropic subspace for ω.*

(2) ***Irreducible subgroups governed by a quadratic character***
   Normalizer G_ℓ of the group M_ℓ that preserves each summand in a direct sum decomposition $V_1 \oplus V_2$ of V into two 2-dimensional subspaces, where V_1 and V_2 are jointly defined over $\mathbb{F}_\ell$ and either:
   (a) *both nondegenerate for ω; or*
   (b) *both isotropic for ω.*
   Moreover, M_ℓ is an index 2 subgroup of G_ℓ.

(3) ***Stabilizer of a twisted cubic***
   $\mathrm{GL}(W)$ *acting on* $\mathrm{Sym}^3 W \simeq V$*, where W is a dimension 2 $\mathbb{F}_\ell$-vector space.*

(4) ***Exceptional subgroups*** *See Table 7 for explicit generators for the groups described below.*
   (a) *When $\ell \equiv \pm 3 \bmod 8$: group with image G_{1920} in $\mathrm{PGSp}(V,\omega)$ of order 1920.*
   (b) *When $\ell \equiv \pm 5 \bmod 12$ and $\ell \neq 7$: group with image G_{720} in $\mathrm{PGSp}(V,\omega)$ of order 720.*
   (c) *When $\ell = 7$: group with image G_{5040} in $\mathrm{PGSp}(V,\omega)$ of order 5040.*

See Lemma 2.5 for a detailed description of the groups G_ℓ and M_ℓ in case (2) above.

REMARK 3. We have chosen to label the maximal subgroups in the classification using invariant subspaces for the symplectic pairing ω on V, following the more modern account due to Aschbacher (see [**Lom16**, Section 3.1]; for a more comprehensive treatment see [**KL90**]). For the convenience of the reader, we record the correspondence between Mitchell's original labels and ours below.

Mitchell's label	**Label in Lemma 2.3**
Group having an invariant point and plane	1a
Group having an invariant parabolic congruence	1b
Group having an invariant hyperbolic or elliptic congruence	2a
Group having an invariant quadric	2b

TABLE 1. Dictionary between maximal subgroup labels in [**Die02**]/[**Mit14**] and Lemma 2.3

Remark 4. The maximal subgroups in (1) are the analogues of the Borel subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. The maximal subgroups in (2) when the two subspaces V_1, V_2 in the direct sum decomposition are individually defined over $\mathbb{F}_\ell$ are the analogues of normalizers of the split Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$. When the two subspaces V_1, V_2 are not individually defined over $\mathbb{F}_\ell$ instead, the maximal subgroups in (2) are analogues of the normalizers of the non-split Cartan subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

Remark 5. We briefly explain why the action of $\mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathrm{Sym}^3(\mathbb{F}_\ell^2)$ preserves a nondegenerate symplectic form. It suffices to show that the restriction to $\mathrm{SL}_2(\mathbb{F}_\ell)$ fixes a vector in $\bigwedge^2 \mathrm{Sym}^3(\mathbb{F}_\ell^2)$. If V has basis $\{x, y\}$, then an invariant vector is $x^3 \wedge y^3 - 3x^2y \wedge xy^2$.

Remark 6. One can extract explicit generators of the exceptional maximal subgroups from Mitchell's original work[3]. Indeed [**Mit14**, the proof of Theorem 8, page 390] gives four explicit matrices that generate a G_{1920} (which is unique up to conjugacy in $\mathrm{PGSp}_4(\mathbb{F}_\ell)$). Mitchell's description of the other exceptional groups is in terms of certain projective linear transformations called skew perspectivities attached to a direct sum decomposition $V = V_1 \oplus V_2$ into 2-dimensional subspaces. A skew perspectivity of order n with axes V_1 and V_2 is the projective linear transformation that scales V_1 by a primitive nth root of unity and fixes V_2. This proof also gives the axes of the skew perspectivities of order 2 and 3 that generate the remaining exceptional groups [**Mit14**, pages 390-391]. Table 7 lists generators of (one representative of the conjugacy class of) each of the exceptional maximal subgroup extracted from Mitchell's descriptions.

In the file `exceptional.m` publicly available with our code, we verify that Magma's list of conjugacy classes of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ agree with those described in Lemma 2.3 for $3 \le \ell \le 47$.

Remark 7. The classification of exceptional maximal subgroups of $\mathrm{PSp}_4(\mathbb{F}_\ell)$ is more subtle than that of $\mathrm{PGSp}_4(\mathbb{F}_\ell)$, because of the constraint on the similitude character of matrices in $\mathrm{PSp}_4(\mathbb{F}_\ell)$. While the similitude character is not well-defined on $\mathrm{PGSp}_4(\mathbb{F}_\ell)$ (multiplication by a scalar $c \in \mathbb{F}_\ell^\times$ scales the similitude character by c^2) it is well-defined modulo squares. The group $\mathrm{PSp}_4(\mathbb{F}_\ell)$ is the kernel of this natural map:

$$1 \to \mathrm{PSp}_4(\mathbb{F}_\ell) \to \mathrm{PGSp}_4(\mathbb{F}_\ell) \xrightarrow{\text{mult}} \mathbb{F}_\ell^\times/(\mathbb{F}_\ell^\times)^2 \simeq \{\pm 1\} \to 1.$$

An exceptional subgroup of $\mathrm{PGSp}_4(\mathbb{F}_\ell)$ gives rise to an exceptional subgroup of $\mathrm{PSp}_4(\mathbb{F}_\ell)$ of either the same size or half the size depending on the image of mult restricted to that subgroup, which in turn depends on the congruence class of ℓ. For this reason, the maximal exceptional subgroups of $\mathrm{PSp}_4(\mathbb{F}_\ell)$ in Mitchell's original classification (also recalled in Dieulefait [**Die02**, Section 2.1]) can have order 1920 *or* 960 and 720 *or* 360 depending on the congruence class of ℓ, and 2520 (for $\ell = 7$). Such an exceptional subgroup gives rise to a *maximal* exceptional subgroup of $\mathrm{PGSp}_4(\mathbb{F}_\ell)$ only when mult is surjective (i.e., its intersection with $\mathrm{PSp}_4(\mathbb{F}_\ell)$ has index two), which explains the restricted congruence classes of ℓ for which they arise.

We now record a lemma that directly follows from the structure of maximal subgroups described above. This lemma will be used in Section 4 to devise a

[3] Mitchell's notation for $\mathrm{PGSp}_4(\mathbb{F}_\ell)$ is $A_\nu(\ell)$ and for $\mathrm{PSp}_4(\mathbb{F}_\ell)$ is $A_1(\ell)$.

criterion for a subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ to be the entire group. For an element T in $\mathrm{GSp}_4(\mathbb{F}_\ell)$, let $\mathrm{tr}(T)$, $\mathrm{mid}(T)$, $\mathrm{mult}(T)$ denote the trace of T, the middle coefficient of the characteristic polynomial of T, and the similitude character applied to T respectively[4]. For a scalar λ, we have

$$\mathrm{tr}(\lambda T) = \lambda\,\mathrm{tr}(T), \quad \mathrm{mid}(\lambda T) = \lambda^2\,\mathrm{mid}(T), \quad \mathrm{mult}(\lambda T) = \lambda^2\,\mathrm{mult}(T).$$

Hence the quantities $\mathrm{tr}(T)^2/\,\mathrm{mult}(T)$ and $\mathrm{mid}(T)/\,\mathrm{mult}(T)$ are well-defined on $\mathrm{PGSp}_4(\mathbb{F}_\ell)$. For $\ell > 2$ and $* \in \{720, 1920, 5040\}$, define

(3)

$$C_{\ell,*} := \left\{ \left(\frac{\mathrm{tr}(T)^2}{\mathrm{mult}(T)}, \frac{\mathrm{mid}(T)}{\mathrm{mult}(T)} \right) \;\middle|\; T \in \text{ exceptional subgroup of projective order } * \right\}$$

Lemma 2.4.

(1) *In cases 2a and 2b of Lemma 2.3:*
   (a) *every element in $G_\ell \smallsetminus M_\ell$ has trace* 0*, and,*
   (b) *the group M_ℓ stabilizes a non-trivial linear subspace of $\overline{\mathbb{F}}_\ell^4$.*

(2) *Every element that is contained in a maximal subgroup corresponding to the stabilizer of a twisted cubic has a reducible characteristic polynomial.*

(3) *For $* \in \{1920, 720\}$, the set $C_{\ell,*}$ defined in* (3) *equals the reduction modulo ℓ of the elements of the set C_* below.*

$$C_{1920} = \{(0,-2),(0,-1),(0,0),(0,1),(0,2),(1,1),(2,1),(2,2),(4,2),(4,3),(8,4),(16,6)\}$$

$$C_{720} = \{(0,1),(0,0),(4,3),(1,1),(16,6),(0,2),(1,0),(3,2),(0,-2)\}$$

We also have

$$C_{7,5040} = \{(0,0),(0,1),(0,2),(0,5),(0,6),(1,0),(1,1),(2,6),(3,2),(4,3),(5,3),(6,3)\}.$$

Proof.

(1) In cases 2a and 2b of Lemma 2.3, since any element of the normalizer G_ℓ that is not in M_ℓ switches elements in the two subspaces V_1 and V_2 (i.e. maps elements in the subspace V_1 in the decomposition $V_1 \oplus V_2$ to elements in V_2 and vice-versa), it follows that any element in $G_\ell \smallsetminus M_\ell$ has trace zero.

(2) The conjugacy class of maximal subgroups corresponding to the stabilizer of a twisted cubic comes from the embedding $\mathrm{GL}_2(\mathbb{F}_\ell) \xrightarrow{\iota} \mathrm{GSp}_4(\mathbb{F}_\ell)$ induced by the natural action of $\mathrm{GL}_2(\mathbb{F}_\ell)$ on the space of monomials of degree 3 in 2 variables. If M is a matrix in $\mathrm{GL}_2(\mathbb{F}_\ell)$ with eigenvalues λ, μ (possibly repeated), then the eigenvalues of $\iota(M)$ are $\lambda^3, \mu^3, \lambda^2\mu, \lambda\mu^2$ and hence the characteristic polynomial of $\iota(M)$ factors as $(T^2 - (\lambda^3 + \mu^3)T + \lambda^3\mu^3)(T^2 - (\lambda^2\mu + \lambda\mu^2)T + \lambda^3\mu^3)$ over $\mathbb{F}_\ell$ which is reducible over $\mathbb{F}_\ell$.

(3) This follows from the description of the maximal subgroups given in Table 7. Each case (except G_{5040} that only occurs for $\ell = 7$) depends on a choice of a root of a quadratic polynomial. In the associated file `exceptional_statistics.sage`, we generate the corresponding finite subgroups over the appropriate quadratic number field to compute C_*. It follows that the corresponding values for the subgroup G_* in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ can be obtained by reducing these values modulo ℓ. Since the group G_{5040} only appears for $\ell = 7$, we directly compute the set $C_{7,5040}$. □

[4] Explicitly, the characteristic polynomial of T is therefore $t^4 - \mathrm{tr}(T)t^3 + \mathrm{mid}(T)t^2 - \mathrm{mult}(T)\,\mathrm{tr}(T)t + \mathrm{mult}(T)^2$.

Remark 8. The condition in Lemma 2.4(3) is the analogue of the condition [**Ser72**, Proposition 19 (iii)] to rule out exceptional maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

We end this subsection by including the following lemma, to further highlight the similarities between the above classification of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ and the more familiar classification of maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$. This lemma is not used elsewhere in the article and is thus for expositional purposes only.

Lemma 2.5.

(1) *The subgroup M_ℓ in the case* (2a) *when the two nondegenerate subspaces V_1 and V_2* ***are*** *individually defined over $\mathbb{F}_\ell$ is isomorphic to*

$$\{(m_1, m_2) \in \mathrm{GL}_2(\mathbb{F}_\ell)^2 \mid \det(m_1) = \det(m_2)\}.$$

In particular, the order of M_ℓ is $\ell^2(\ell-1)(\ell^2-1)^2$.

(2) *The subgroup M_ℓ in the case* (2b) *when the two isotropic subspaces V_1 and V_2* ***are*** *individually defined over $\mathbb{F}_\ell$ is isomorphic to*

$$\{(m_1, m_2) \in \mathrm{GL}_2(\mathbb{F}_\ell)^2 \mid m_1^T m_2 = \lambda I, \text{ for some } \lambda \in \mathbb{F}_\ell^*\}.$$

In particular, the order of M_ℓ is $\ell(\ell-1)^2(\ell^2-1)$.

(3) *The subgroup M_ℓ in the case* (2a) *when the two nondegenerate subspaces V_1 and V_2* ***are not*** *individually defined over $\mathbb{F}_\ell$ is isomorphic to*

$$\{m \in \mathrm{GL}_2(\mathbb{F}_{\ell^2}) \mid \det(m) \in \mathbb{F}_\ell^*\}.$$

In particular, the order of M_ℓ is $\ell^2(\ell-1)(\ell^4-1)$.

(4) *The subgroup M_ℓ in the case* (2b) *when the two isotropic subspaces V_1 and V_2* ***are not*** *individually defined over $\mathbb{F}_\ell$ is isomorphic to* $\mathrm{GU}_2(\mathbb{F}_{\ell^2})$, *i.e.,*

$$\{m \in \mathrm{GL}_2(\mathbb{F}_{\ell^2}) \mid m^T \iota(m) = \lambda I, \text{ for some } \lambda \in \mathbb{F}_\ell^*\},$$

where ι denotes the natural extension of the Galois automorphism of $\mathbb{F}_{\ell^2}/\mathbb{F}_\ell$ to $\mathrm{GL}_2(\mathbb{F}_{\ell^2})$. *In particular, the order of M_ℓ is $\ell(\ell^2-1)^2$.*

Proof. Given a direct sum decomposition $V_1 \oplus V_2$ of a vector space V over $\mathbb{F}_q$, we get a natural embedding of $\mathrm{Aut}(V_1) \times \mathrm{Aut}(V_2)$ ($\cong \mathrm{GL}_2(\mathbb{F}_q)^2$) into $\mathrm{Aut}(V)$ ($\cong \mathrm{GL}_4(\mathbb{F}_q)$), whose image consists of automorphisms that preserve this direct sum decomposition. We will henceforth refer to elements of $\mathrm{Aut}(V_1) \times \mathrm{Aut}(V_2)$ as elements of $\mathrm{Aut}(V)$ using this embedding. To understand the subgroup M_ℓ of $\mathrm{GSp}_4(\mathbb{F}_q)$ in cases (1) and (2) where the two subspaces in the direct sum decomposition are individually defined over $\mathbb{F}_q$, we need to further impose the condition that the automorphisms in the image of the map $\mathrm{Aut}(V_1) \times \mathrm{Aut}(V_2) \to \mathrm{Aut}(V)$ preserve the symplectic form ω on V up to a scalar.

In (1), without any loss of generality, the two nondegenerate subspaces V_1 and V_2 can be chosen to be orthogonal complements under the nondegenerate pairing ω, and so by Witt's theorem, in a suitable basis for $V_1 \oplus V_2$ obtained by concatenating a basis of V_1 and a basis of V_2, the nondegenerate symplectic pairing ω has the following block-diagonal shape:

$$J := \begin{bmatrix} 0 & 1 & & \\ -1 & 0 & & \\ & & 0 & 1 \\ & & -1 & 0 \end{bmatrix}.$$

The condition that an element $(m_1, m_2) \in \mathrm{Aut}(V_1) \oplus \mathrm{Aut}(V_2)$ preserves the symplectic pairing up to a similitude factor of λ is the condition $(m_1, m_2)^T J (m_1, m_2) = \lambda J$, which boils down to $\det(m_1) = \lambda = \det(m_2)$.

Similarly, in (2), without any loss of generality, by Witt's theorem, in a suitable basis for $V_1 \oplus V_2$ obtained by concatenating a basis of the isotropic subspace V_1 and a basis of the isotropic subspace V_2, the nondegenerate symplectic pairing ω has the following block-diagonal shape.

$$J := \begin{bmatrix} & & 0 & 1 \\ & & 1 & 0 \\ 0 & -1 & & \\ -1 & 0 & & \end{bmatrix}.$$

The condition that an element $(m_1, m_2) \in \mathrm{Aut}(V_1) \oplus \mathrm{Aut}(V_2)$ preserves the symplectic pairing up to a similitude factor of λ is the condition $(m_1, m_2)^T J (m_1, m_2) = \lambda J$, which again boils down to $m_1^T m_2 = \lambda I$.

If we have a subspace W defined over $\mathbb{F}_{q^2}$ but not defined over $\mathbb{F}_q$, and we let $\overline{W}$ denote the conjugate subspace and further assume that $W \oplus \overline{W}$ gives a direct sum decomposition of V, then we get a natural embedding of $\mathrm{Aut}(W)$ ($\cong \mathrm{GL}_2(\mathbb{F}_{q^2})$) into $\mathrm{Aut}(V)$ ($\cong \mathrm{GL}_4(\mathbb{F}_q)$) whose image consists of automorphisms that commute with the natural involution of $V \otimes \mathbb{F}_{q^2}$ induced by the Galois automorphism of $\mathbb{F}_{q^2}$ over $\mathbb{F}_q$. The proofs of cases (3) and (4) are analogous to the cases (1) and (2) respectively, by using the direct sum decomposition $W \oplus \overline{W}$ and letting $m_2 = \iota(m_1)$. The condition that $\det(m_1) = \det(m_2)$ in (1) becomes the condition $\det(m_1) = \det(m_2) = \det \overline{m_1} = \overline{\det(m_1)}$, or equivalently, that $\det(m_1) \in \mathbb{F}_q$ in (3). Similarly, the condition that $m_1^T m_2 = \lambda I$ in (2) becomes the condition that $m_1^T \iota(m_1) = \lambda I$ in (4). □

2.5. Image of inertia and (tame) fundamental characters.

Dieulefait [**Die02**] used Mitchell's work described in the previous subsection to classify the maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ that could occur as the image of $\rho_{A,\ell}$. This was achieved via an application of a fundamental result of Serre and Raynaud that strongly constrains the action of inertia at ℓ, and which we now recall.

Fix a prime $\ell > 3$ that does not divide the conductor N of A. Let I_ℓ be an inertia subgroup at ℓ. Let $\psi_n \colon I_\ell \to \mathbb{F}_{\ell^n}^\times$ denote a (tame) fundamental character of level n. The n Galois-conjugate fundamental characters $\psi_{n,1}, \ldots, \psi_{n,n}$ of level n are given by $\psi_{n,i} := \psi_n^{\ell^i}$. Recall that the fundamental character of level 1 is simply the mod ℓ cyclotomic character cyc_ℓ, and that the product of all fundamental characters of a given level is the cyclotomic character.

THEOREM 2.6 (Serre [**Ser72**], Raynaud [**Ray74**], cf. Theorem 2.1 in [**Die02**]). *Let ℓ be a semistable prime for A. Let $V/\mathbb{F}_\ell$ be an n-dimensional Jordan–Hölder factor of the I_ℓ-module $A[\ell]$. Then V admits a 1-dimensional $\mathbb{F}_{\ell^n}$-vector space structure such that $\rho_{A,\ell}|_{I_\ell}$ acts on V via the character*

$$\psi_{n,1}^{d_1} \cdots \psi_{n,n}^{d_n}$$

with each d_i equal to either 0 *or* 1.

On the other hand, the following fundamental result of Grothendieck constrains the action of inertia at semistable primes $p \neq \ell$.

Theorem 2.7 (Grothendieck [**GRR72**, Exposé IX, Prop 3.5]). *Let A be an abelian variety over a number field K. Then A has semistable reduction at $\mathfrak{p}$ not above ℓ if and only if the action of $I_{\mathfrak{p}} \subset G_K$ on $T_\ell A$ is 2-step unipotent (i.e. $(\rho_{A,\ell}(g) - I)^2 = 0$ for all $g \in I_{\mathfrak{p}}$).*

Combining these two results allows one fine control of the determinant of a subquotient of $A[\ell]$; this will be used in Section 3.

Corollary 2.8. *Let $A/\mathbb{Q}$ be an abelian surface, and let X_ℓ be a Jordan–Hölder factor of the $\overline{\mathbb{F}}_\ell[G_\mathbb{Q}]$-module $A[\ell] \otimes \overline{\mathbb{F}}_\ell$. If ℓ is a semistable prime, then*

$$\det X_\ell \simeq \epsilon \cdot \mathrm{cyc}_\ell^x$$

for some character $\epsilon : G_\mathbb{Q} \to \overline{\mathbb{F}}_\ell$ that is unramified at ℓ and some $0 \leq x \leq \dim X_\ell$. Moreover, $\epsilon^{120} = 1$.

Proof. The first part follows immediately from Theorem 2.6. For the fact that $\epsilon^{120} = 1$, we will show that ϵ^{120} is unramified everywhere; the result will then follow from the fact that there are no nontrivial unramified characters of $G_\mathbb{Q}$. Since ϵ is unramifed at ℓ, so too is ϵ^{120}, so it suffices to show that ϵ^{120} is unramified at primes $p \neq \ell$. From [**LV14a**, Theorem 7.2] we know that every abelian surface attains semistable reduction over an extension $K/\mathbb{Q}$ with $[K : \mathbb{Q}]$ dividing 120; therefore by Theorem 2.7 we have that the action of $I_{\mathfrak{p}} \subset G_K$ on $T_\ell A$ is 2-step unipotent for any prime $\mathfrak{p} \mid p$ of K. Hence the action of the 120th power of any element of I_p is unipotent, and thus has trivial determinant. □

We can now state Dieulefait's classification of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ that can occur as the image $\rho_{A,\ell}(G_\mathbb{Q})$ for a semistable prime $\ell > 7$.

Proposition 2.9 ([**Die02**]). *Let A be the Jacobian of a genus 2 curve defined over $\mathbb{Q}$ with Weil pairing ω on $A[\ell]$. If $\ell > 7$ is a semistable prime, then $\rho_{A,\ell}(G_\mathbb{Q})$ is either all of $\mathrm{GSp}(A[\ell], \omega)$ or it is contained in one of the maximal subgroups of Types (1) or (2) in Lemma 2.3.*

See also [**Lom16**, Proposition 3.15] for an expanded exposition of why the image of $G_\mathbb{Q}$ cannot be contained in maximal subgroup of Type (3) for a semistable prime $\ell > 7$.

Remark 9. However, if ℓ is a prime of additive reduction, or if $\ell \leq 7$, then the image of $G_\mathbb{Q}$ may also be contained in any of the four types of maximal subgroups described in Lemma 2.3. Nevertheless, by [**LV22**, Theorem 6.6], for any prime $\ell > 24$, we have that the exponent of the projective image is bounded $\exp(\mathbb{P}\rho_{A,\ell}) \geq (\ell - 1)/12$. Since $\exp(G_{1920}) = 2\exp(S_6) = 120$ and $\exp(G_{720}) = \exp(S_5) = 60$, the exceptional maximal subgroups cannot occur as $\rho_{A,\ell}(G_\mathbb{Q})$ for $\ell > 1441$.

2.6. A consequence of the Chebotarev density theorem. Let $K/\mathbb{Q}$ be a finite Galois extension with Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ and absolute discriminant d_K. Let $S \subseteq G$ be a nonempty subset that is closed under conjugation. By the Chebotarev density theorem, we know that

$$\lim_{x \to \infty} \frac{|\{p \leq x : p \text{ is unramified in } K \text{ and } \mathrm{Frob}_p \in S\}|}{|\{p \leq x\}|} = \frac{|S|}{|G|}. \tag{4}$$

Let p be the least prime such that p is unramified in K and $\mathrm{Frob}_p \in S$. There are effective versions of the Chebotarev density theorem that give bounds on p. The best known unconditional bounds are polynomials in d_K [**LMO79, AK19, KW22**]. Under GRH, the best known bounds are polynomials in $\log d_K$. In particular Bach and Sorenson [**BS96**] showed that under GRH,

$$p \le (4 \log d_K + 2.5[K:\mathbb{Q}] + 5)^2. \tag{5}$$

The present goal is to give an effective version of the Chebotarev density theorem in the context of abelian surfaces. We will use a corollary of (5) that is noted in [**MW21**] which allows for the avoidance of a prescribed set of primes by taking a quadratic extension of K. We do this because we will take $K = \mathbb{Q}(A[\ell])$, and p being unramified in K is not sufficient to imply that p is a prime of good reduction for A. Lastly, we will use that by [**Ser81**, Proposition 6], if $K/\mathbb{Q}$ is finite Galois, then

$$\log d_K \le ([K:\mathbb{Q}] - 1) \log \operatorname{rad}(d_K) + [K:\mathbb{Q}] \log([K:\mathbb{Q}]), \tag{6}$$

where $\operatorname{rad} n = \prod_{p|n} p$ denotes the radical of an integer n.

Lemma 2.10. *Let $A/\mathbb{Q}$ be a typical principally polarized abelian surface with conductor N_A. Let q be a prime. Let $S \subseteq \rho_{A,q}(G_\mathbb{Q})$ be a nonempty subset that is closed under conjugation. Let p be the least prime of good reduction for A such that $p \ne q$ and $\rho_{A,q}(\mathrm{Frob}_p) \in S$. Assuming GRH, we have*

$$p \le \left(4\left[(2q^{11} - 1) \log \operatorname{rad}(2qN_A) + 22q^{11} \log(2q)\right] + 5q^{11} + 5\right)^2.$$

Proof. Let $K = \mathbb{Q}(A[q])$. Then the image of $\rho_{A,q}$ is $\mathrm{Gal}(K/\mathbb{Q})$, the extension $K/\mathbb{Q}$ is Galois and

$$[K:\mathbb{Q}] \le |\mathrm{GSp}_4(\mathbb{F}_q)| = q^4(q^4-1)(q^2-1)(q-1) \le q^{11}.$$

As $\operatorname{rad}(d_K)$ is the product of primes that ramify in $\mathbb{Q}(A[q])$, the criterion of Néron-Ogg-Shafarevich for abelian varieties [**ST68**, Theorem 1] implies that $\operatorname{rad}(d_K)$ divides $\operatorname{rad}(qN_A)$. Let $\tilde{K} := K(\sqrt{m})$ where $m := \operatorname{rad}(2N_A)$. Note that the primes that ramify in $\tilde{K}$ are precisely 2, q, and the primes of bad reduction for A. Thus $\operatorname{rad}(d_{\tilde{K}}) = \operatorname{rad}(2qN_A)$. Moreover $[\tilde{K}:\mathbb{Q}] \le 2q^{11}$ and by (6),

$$\log(d_{\tilde{K}}) \le (2q^{11} - 1) \log \operatorname{rad}(2qN_A) + 22q^{11} \log(2q).$$

Applying [**MW21**, Corollary 6] to the field $\tilde{K}$, we get that (under GRH) there exists a prime p satisfying the claimed bound, that does not divide m, and for which $\rho_{A,q}(\mathrm{Frob}_p) \in S$. □

3. Finding a finite set containing all nonsurjective primes

In this section we describe Algorithm 3.1 referenced in Theorem 1.1(1), which is a reformulation of the algorithm of Dieulefait [**Die02**] with some modest improvements. This algorithm produces a finite list PossiblyNonsurjectivePrimes that provably includes all nonsurjective primes ℓ. We also prove Theorem 1.2.

Since our goal is to produce a finite list (from which we will later remove extraneous primes) it is harmless to include the finitely many bad primes as well as $2, 3, 5, 7$. Using Proposition 2.9, it suffices to find conditions on $\ell > 7$ for which $\rho_{A,\ell}(G_\mathbb{Q})$ could be contained in one of the maximal subgroups of type (1) and (2) in Lemma 2.3. We first find primes ℓ for which $\rho_{A,\ell}$ has (geometrically) reducible image (and hence is contained in a maximal subgroup in case (1) of Lemma 2.3 or in a subgroup M_ℓ in case (2)). To treat the geometrically irreducible cases, we then make use of the observation from Lemma 2.4 1a that every element outside of an index 2 subgroup has trace 0.

Algorithm 3.1. *Given a typical genus 2 curve $C/\mathbb{Q}$ with conductor N and Jacobian A, compute a finite list* PossiblyNonsurjectivePrimes *of primes as follows.*

(1) *Initialize* PossiblyNonsurjectivePrimes $= [2, 3, 5, 7]$.
(2) *Add to* PossiblyNonsurjectivePrimes *all primes dividing N.*
(3) *Add to* PossiblyNonsurjectivePrimes *the good primes ℓ for which $\rho_{A,\ell} \otimes \overline{\mathbb{F}}_\ell$ could be reducible via Algorithms 3.3, 3.6, and 3.10.*
(4) *Add to* PossiblyNonsurjectivePrimes *the good primes ℓ for which $\rho_{A,\ell} \otimes \overline{\mathbb{F}}_\ell$ could be irreducible but nonsurjective via Algorithm 3.13.*
(5) *Return* PossiblyNonsurjectivePrimes.

At a very high-level, each of the subalgorithms of Algorithm 3.1 makes use of a set of auxiliary good primes p. We compute the integral characteristic polynomial of Frobenius $P_p(t)$ and use it to constrain those $\ell \neq p$ for which the image could have a particular shape.

Remark 10. Even though robust methods to compute the conductor N of a genus 2 curve are not implemented at the time of writing, the odd-part N_{odd} of N can be computed via `genus2red` function of PARI and the `genus2reduction` module of SageMath, both based on an algorithm of Liu [**Liu94**]. Moreover, [**BK94**, Theorem 6.2] bounds the 2-exponent of N above by 20 and hence N can be bounded above by $2^{20}N_{\text{odd}}$. While these algorithms can be run only with the bound $2^{20}N_{\text{odd}}$, doing so substantially increases the run-time of the limiting Algorithm 3.10.

We now explain each of these steps in detail.

3.1. Good primes that are not geometrically irreducible. In this section we describe the conditions that ℓ must satisfy for the base-extension $\overline{A[\ell]} := A[\ell] \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell$ to be reducible. In this case, the representation $\overline{A[\ell]}$ is an extension

$$0 \to X_\ell \to \overline{A[\ell]} \to Y_\ell \to 0 \tag{7}$$

of a (quotient) representation Y_ℓ by a (sub) representation X_ℓ. Recall that N_{sq} denotes the largest square divisor of N.

Lemma 3.2. *Let ℓ be a prime of good reduction for A and suppose that $\overline{A[\ell]}$ sits in the sequence* (7). *Let $p \neq \ell$ be a good prime for A and let f denote the order of p in $(\mathbb{Z}/N_{\text{sq}}\mathbb{Z})^\times$. Then there exists $0 \leq x \leq \dim X_\ell$ (respectively, $0 \leq y \leq \dim Y_\ell$) such that the value of $\det X_\ell$ (respectively, $\det Y_\ell$) evaluated at $\text{Frob}_p^{\gcd(f,120)}$ is $p^{\gcd(f,120)x}$ (respectively, $p^{\gcd(f,120)y}$).*

Proof. Since ℓ is a good prime and X_ℓ is composed of Jordan–Hölder factors of $\overline{A[\ell]}$, Corollary 2.8 constrains its determinant. We have $\det X_\ell = \epsilon \operatorname{cyc}_\ell^x$ for some character $\epsilon\colon G_{\mathbb{Q}} \to \overline{\mathbb{F}}_\ell$ unramified at ℓ, and $0 \leq x \leq \dim X_\ell$, and $\epsilon^{120} = 1$. Hence the value of $\det X_\ell$ evaluated at Frob_p^{120} is $\operatorname{cyc}_\ell(\text{Frob}_p)^{120x} = p^{120x}$.

In fact, we can do slightly better. Since $\det \overline{A[\ell]} \simeq \operatorname{cyc}_\ell^2$, we have $\det Y_\ell \simeq \epsilon^{-1} \operatorname{cyc}_\ell^{2-x}$. Since the conductor is multiplicative in extensions, we conclude that $\operatorname{cond}(\epsilon)^2 \mid N$. By class field theory, the character ϵ factors through $(\mathbb{Z}/\operatorname{cond}(\epsilon)\mathbb{Z})^\times$, and hence through $(\mathbb{Z}/N_{\text{sq}}\mathbb{Z})^\times$, sending Frob_p to $p \bmod N_{\text{sq}}$. Since $p^f \equiv 1 \bmod$

N_{sq}, we have that $\epsilon(\text{Frob}_p)^{\gcd(f,120)} = 1$, and the value of $\det X_\ell$ evaluated at $\text{Frob}_p^{\gcd(f,120)}$ is $p^{\gcd(f,120)x}$. Exchanging X_ℓ and Y_ℓ, we deduce the result for Y_ℓ. □

This is often enough information to find all ℓ for which $\overline{A[\ell]}$ has a nontrivial subquotient. Namely, by Theorem 2.1, every root of $P_p(t)$ has complex absolute value $p^{1/2}$. Thus the $\gcd(f,120)$-th power of each root has complex absolute value $p^{\gcd(f,120)/2}$, and hence is never *integrally* equal to 1 or $p^{\gcd(f,120)}$. Since Lemma 3.2 guarantees that this equality must hold modulo ℓ for any good prime ℓ for which $\overline{A[\ell]}$ is reducible with a 1-dimensional subquotient, we always get a nontrivial condition on ℓ. Some care must be taken to rule out ℓ for which $\overline{A[\ell]}$ only has 2-dimensional subquotient(s).

3.1.1. *Odd-dimensional subquotient (cf.* [**Die02**, Section 3.1]*).* Let p be a good prime. Given a polynomial $P(t)$ and an integer f, write $P^{(f)}(t)$ for the polynomial whose roots are the fth powers of roots of $P(t)$. Universal formulas for such polynomials in terms of the coefficients of $P(t)$ are easy to compute, and are implemented in our code in the case where P is a degree 4 polynomial whose roots multiply in pairs to p^α, and $f \mid 120$.

Algorithm 3.3 (cf. [**Die02**, Section 3.1]). *Given a typical genus 2 Jacobian $A/\mathbb{Q}$ of conductor N, let f denote the order of p in $(\mathbb{Z}/N_{\text{sq}}\mathbb{Z})^\times$ and write $f' =$* $\gcd(f,120)$. *Compute an integer M_{odd} as follows.*

(1) *Choose a nonempty finite set $\mathcal{T}$ of auxiliary good primes $p \nmid N$.*
(2) *For each p, compute*

$$R_p := P_p^{(f')}(1).$$

(3) *Let $M_{odd} = \gcd_{p\in\mathcal{T}}(pR_p)$ over all auxiliary primes.*

Return the list of prime divisors ℓ of M_{odd}.

Remark 11. Algorithm 3.3 offers a modest improvement on [**Die02**, Section 3.1]), where the exponent f is used (without taking the gcd with 120.)

Proposition 3.4. *Any good prime ℓ for which $\overline{A[\ell]}$ has an odd-dimensional subrepresentation is returned by Algorithm 3.3.*

Proof. Since $\overline{A[\ell]}$ is 4-dimensional and has an odd-dimensional subrepresentation, it has a 1-dimensional subquotient. For any $p \in \mathcal{T}$, Lemma 3.2 shows that the value of $\det X_\ell$ evaluated at $\text{Frob}_p^{f'}$ is either $p^{f'}$ or 1. Thus, the action of $\text{Frob}_p^{f'}$ on $\overline{A[\ell]}$ has an eigenvalue that is equal to $p^{f'}$ or 1 in $\overline{\mathbb{F}}_\ell$, and so $P_p^{(f')}(t)$ has a root that is equal to 1 or $p^{f'}$ in $\overline{\mathbb{F}}_\ell$. Since the roots of $P^{(f')}(t)$ multiply in pairs to $p^{f'}$, we have $P_p^{(f')}(p^{f'}) = p^{2f'}P_p^{(f')}(1)$. Hence ℓ divides $p \cdot P_p^{(f')}(1) = pR_p$. □

Using Theorem 2.1, we can give a theoretical bound on the “worst case” of this step of the algorithm using only one auxiliary prime p. Of course, taking the greatest common divisor over multiple auxiliary primes will likely remove extraneous factors, and in practice this step of the algorithm runs substantially faster than other steps.

Proposition 3.5. *Algorithm 3.3 terminates. More precisely, if p is good, then*

$$0 \neq |M_{odd}| \ll p^{241},$$

where the implied constant is absolute.

PROOF. This follows from the fact that the coefficient of t^i in $P_p^{(f')}(t)$ has magnitude on the order of $p^{(2-i/2)f'}$ and $f' \leq 120$. □

3.1.2. *Two-dimensional subquotients.* We now assume that $\overline{A[\ell]}$ is reducible, but does not have any odd-dimensional subquotients. In particular, it has an irreducible subrepresentation X_ℓ of dimension 2, with irreducible quotient Y_ℓ of dimension 2. If $\overline{A[\ell]}$ is reducible but indecomposable, then X_ℓ is the unique subrepresentation of $\overline{A[\ell]}$ and $Y_\ell^\vee \otimes \mathrm{cyc}_\ell$ is the unique subrepresentation of $\overline{A[\ell]}^\vee \otimes \mathrm{cyc}_\ell$. The isomorphism $T_\ell A \simeq (T_\ell A)^\vee \otimes \mathrm{cyc}_\ell$ from (2) yields an isomorphism $\overline{A[\ell]} \simeq (\overline{A[\ell]})^\vee \otimes \mathrm{cyc}_\ell$ and hence $X_\ell \simeq Y_\ell^\vee \otimes \mathrm{cyc}_\ell$. Otherwise, $\overline{A[\ell]} \simeq X_\ell \oplus Y_\ell$ and so the nondegeneracy of the Weil pairing gives

$$X_\ell \oplus Y_\ell \simeq (X_\ell^\vee \otimes \mathrm{cyc}_\ell) \oplus (Y_\ell^\vee \otimes \mathrm{cyc}_\ell)\,.$$

Therefore either:

(a) $X_\ell \simeq Y_\ell^\vee \otimes \mathrm{cyc}_\ell$ and $Y_\ell \simeq X_\ell^\vee \otimes \mathrm{cyc}_\ell$, or
(b) $X_\ell \simeq X_\ell^\vee \otimes \mathrm{cyc}_\ell$ and $Y_\ell \simeq Y_\ell^\vee \otimes \mathrm{cyc}_\ell$ and $\overline{A[\ell]} \simeq X_\ell \oplus Y_\ell$.

We call the first case related 2-dimensional subquotients and the second case self-dual 2-dimensional subrepresentations. We will see that the ideas of Lemma 3.2 easily extend to treat the related subquotient case; we will use the validity of Serre's conjecture to treat the self-dual case. In the case that $\overline{A[\ell]}$ is decomposable, the above two cases correspond respectively to the index 2 subgroup M_ℓ in cases (2a) (the isotropic case) and (2b) (the nondegenerate case) of Lemma 2.3.

3.1.3. *Related two-dimensional subquotients (cf.* [**Die02**, Section 3.2]*).* Let p be a good prime. Let $P_p(t) := t^4 - at^3 + bt^2 - pat + p^2$ be the characteristic polynomial of Frob_p acting on $\overline{A[\ell]}$. Suppose that α and β are the eigenvalues of Frob_p acting on the subrepresentation X_ℓ. Then, since $X_\ell \simeq Y_\ell^\vee \otimes \mathrm{cyc}_\ell$, the eigenvalues of the action of Frob_p on Y_ℓ are p/α and p/β. The action of Frob_p on $\det X_\ell$ is therefore by a product of two of the roots of $P_p(t)$ that do not multiply to p. Note that there are four such pairs of roots of $P_p(t)$ that do not multiply to p. Let $Q_p(t)$ be the quartic polynomial whose roots are the products of pairs of roots of $P_p(t)$ that do not multiply to p. By design, the roots of $Q_p(t)$ have complex absolute value p, but are not equal to p. (It is elementary to work out that

$$Q_p(t) = t^4 - (b-2p)t^3 + p(a^2 - 2b + 2p)t^2 - p^2(b-2p)t + p^4$$

and is a quartic whose roots multiply in pairs to p^2.)

ALGORITHM 3.6 (cf. [**Die02**, Section 3.2]). *Given a typical genus* 2 *Jacobian $A/\mathbb{Q}$ of conductor N, let f denote the order of p in $(\mathbb{Z}/N_{\mathrm{sq}}\mathbb{Z})^\times$ and write $f' =$* $\gcd(f, 120)$. *Compute an integer $M_{related}$ as follows.*

(1) *Choose a finite set $\mathcal{T}$ of auxiliary good primes $p \nmid N$;*
(2) *For each p, compute the product*

$$R_p := Q_p^{(f')}(1) Q_p^{(f')}(p^{f'})$$

(3) *Let $M_{related} = \gcd_{p\in\mathcal{T}}(pR_p)$.*

Return the list of prime divisors ℓ of $M_{related}$.

REMARK 12. Algorithm 3.6 offers a modest improvement on the procedure described in [**Die02**, Section 3.2]) by taking the gcd of f with 120.

Proposition 3.7. *Any good prime ℓ for which $\overline{A[\ell]}$ has related two-dimensional subquotients is returned by Algorithm 3.6.*

Proof. Proceed similarly as in the proof of Proposition 3.4 — in particular, ℓ divides $Q_p^{(f')}(1)$, $Q_p^{(f')}(p^{f'})$, or $Q_p^{(f')}(p^{2f'})$ and hence ℓ divides pR_p since $Q_p^{(f')}(p^{2f'}) = p^{4f'}Q_p^{(f')}(1)$. □

A theoretical "worst case" analysis yields the following.

Proposition 3.8. *Algorithm 3.6 terminates. More precisely, if q is the smallest surjective prime for A, then a good prime p for which R_p is nonzero is bounded by a function of q. Assuming GRH,*

$$p \ll q^{22}\log^2(qN),$$

where the implied constants are absolute and effectively computable. Moreover, for such a prime p,

$$|M_{related}| \ll p^{961} \ll q^{21142}\log^{1922}(qN),$$

where the implied constants are absolute.

Proof. By Serre's open image theorem for genus 2 curves, such a prime q exists. Since there exists an element of $\mathrm{GSp}_4(\mathbb{F}_q)$ with irreducible characteristic polynomial, by Lemma 2.10 there exists a prime p (bounded as claimed) such that R_p is nonzero modulo q. Finally,

$$M_{\mathrm{related}} \le pR_p = pQ^{(f')}(1)Q^{(f')}(p^{f'}) \ll p^{8f'+1} \ll p^{961},$$

since the coefficient of t^i in $Q^{(f')}(t)$ has magnitude on the order of $p^{(4-i)f'}$ and $f' \le 120$. □

3.1.4. *Self-dual two-dimensional subrepresentations (cf.* [**Die02**, Section 3.3]*).* In this case, both subrepresentations X_ℓ and Y_ℓ are absolutely irreducible 2-dimensional Galois representations with determinant the cyclotomic character cyc_ℓ. It follows that the representations are odd (i.e., the determinant of complex conjugation is -1.) Therefore, by the Khare–Wintenberger theorem (formerly Serre's conjecture on the modularity of mod-ℓ Galois representations) [**Kha06, KW09a, KW09b**], both X_ℓ and Y_ℓ are modular; that is, for $i = 1, 2$, there exist newforms $f_i \in S_{k_i}^{\mathrm{new}}(\Gamma_1(N_i), \epsilon_i)$ such that

$$X_\ell \cong \overline{\rho}_{f_1,\ell} \text{ and } Y_\ell \cong \overline{\rho}_{f_2,\ell}.$$

Furthermore, by the multiplicativity of Artin conductors, we obtain the divisibility $N_1N_2 \mid N$.

Lemma 3.9. *Both f_1 and f_2 have weight two and trivial Nebentypus; that is, $k_1 = k_2 = 2$, and $\epsilon_1 = \epsilon_2 = 1$.*

Proof. From Theorem 2.6, we have that $X_\ell|_{I_\ell}$ and $Y_\ell|_{I_\ell}$ must each be conjugate to either of the following subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$:

$$\begin{pmatrix} 1 & * \\ 0 & \mathrm{cyc}_\ell \end{pmatrix} \text{ or } \begin{pmatrix} \psi_2 & 0 \\ 0 & \psi_2^\ell \end{pmatrix}.$$

The assertion of weight 2 now follows from [**Ser87**, Proposition 3]. (Alternatively, one may use Proposition 4 of *loc. cit.*, observing that X_ℓ and Y_ℓ are finite and flat as group schemes over $\mathbb{Z}_\ell$ because ℓ is a prime of good reduction.)

From Section 1 of *loc. cit.*, the Nebentypus ϵ_i of f_i satisfies, for all $p \nmid \ell N$,

$$\det X_\ell(\mathrm{Frob}_p) = p \cdot \epsilon_i(p),$$

where this equality is viewed inside $\overline{\mathbb{F}}_\ell^\times$. The triviality of ϵ_i follows. □

We therefore have newforms $f_i \in \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(N_i))$ such that

$$\overline{A[\ell]} \simeq \overline{\rho}_{f_1,\ell} \oplus \overline{\rho}_{f_2,\ell}. \tag{8}$$

We may assume without loss of generality that $N_1 \leq \sqrt{N}$. Let $p \nmid N$ be an auxiliary prime. We obtain from equation (8) that the integral characteristic polynomial of Frobenius factors:

$$P_p(t) \equiv (t^2 - a_p(f_1)t + p)(t^2 - a_p(f_2)t + p) \mod \ell;$$

here we use the standard property that, for f a normalised eigenform with trivial Nebentypus, $\rho_{f,\ell}(\mathrm{Frob}_p)$ satisfies the polynomial equation $t^2 - a_p(f)t + p$ for $p \neq \ell$. In particular, we have

$$\mathrm{Res}(P_p(t), t^2 - a_p(f_1)t + p) \equiv 0 \mod \ell.$$

This serves as the basis of the algorithm to find all primes ℓ in this case.

Algorithm 3.10 ([**Die02**, Section 3.3]). *Given a typical genus* 2 *Jacobian* $A/\mathbb{Q}$ *of conductor* N*, compute an integer* $M_{\textit{self-dual}}$ *as follows.*

(1) *Compute the set* S *of divisors* d *of* N *with* $d \leq \sqrt{N}$.
(2) *For each* $d \in S$:
 (a) *choose a finite set* $\mathcal{T}$ *of auxiliary primes* $p \nmid N$;
 (b) *for each auxiliary prime* p*, compute the* Hecke L-polynomial

$$Q_d(t) \coloneqq \prod_f (t^2 - a_p(f)t + p),$$

 where the product is taken over the finitely many newforms in $\mathcal{S}_2^{new}(\Gamma_0(d))$;
 (c) *compute the resultant*

$$R_p(d) \coloneqq \mathrm{Res}(P_p(t), Q_d(t));$$

 (d) *Take the greatest common divisor*

$$M(d) \coloneqq \gcd_{p \in \mathcal{T}}(pR_p(d)).$$

(3) *Let* $M_{\textit{self-dual}} \coloneqq \prod_{d \in S} M(d)$.

Return the list of prime divisors ℓ *of* $M_{\textit{self-dual}}$.

Proposition 3.11. *Any good prime* ℓ *for which* $\overline{A[\ell]}$ *has self-dual* 2*-dimensional subrepresentations is returned by Algorithm 3.10.*

Proof. As explained before Algorithm 3.10, there exists $N_1 \in S$ and a newform $f_1 \in \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(N_1))$ such that $\mathrm{Res}(P_p(t), t^2 - a_p f_1 t + p) \equiv 0 \bmod \ell$ for every $p \in \mathcal{T} \smallsetminus \{\ell\}$. In particular, $pR_p(N_1) \equiv 0 \bmod \ell$, so ℓ divides $M(N_1)$ and $M_{\text{self-dual}}$. □

We can again do a "worst case" theoretical analysis of this algorithm to conclude the following. As this indicates, this is by far the limiting step of the algorithm.

Proposition 3.12. *Algorithm 3.10 terminates. More precisely, if q is the smallest surjective prime for A, then a good prime p for which $R_p(d)$ is nonzero is bounded by a function of q. Assuming GRH, $p \ll q^{22}\log^2(qN)$, where the implied constant is absolute and effectively computable. Moreover, for such a prime p, we have*

$$|R_p(d)| \ll (2p^{1/2})^{8\dim \mathcal{S}_2^{new}(\Gamma_0(d))} \ll (4p)^{(d+1)/3},$$

and so all together

$$|M_{self\text{-}dual}| \ll (4p)^{N^{1/2+\epsilon}},$$

where the implied constants are absolute.

Proof. As in Proposition 3.8, we use Serre's open image theorem and the Effective Chebotarev Theorem. If $R_p(d)$ is zero integrally, then in particular $R_p(d) \equiv 0 \bmod q$ and $P_p(t) \bmod q$ has a factor in common with a quadratic polynomial is therefore reducible modulo q. Since $\mathrm{GSp}_4(\mathbb{F}_q)$ contains elements that do not have reducible characteristic polynomial, Lemma 2.10 implies that such elements are the image of Frob_p for p bounded as claimed.

The resultant $R_p(d)$ is the product of the pairwise differences of the roots of $P_p(t)$ and $Q_d(t)$, which all have complex absolute value $p^{1/2}$. Hence the pairwise differences have absolute value at most $2p^{1/2}$. Moreover $\dim \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d)) \leq (d+1)/12$ by [**Mar05**, Theorem 2]. Since there are $8\dim \mathcal{S}_2^{\mathrm{new}}(\Gamma_0(d))$ such terms multiplied to give $R_p(d)$, the bound for $R_p(d)$ follows. Since $M_{\text{self-dual}} = \prod_{\substack{d|N \\ d\leq\sqrt{N}}} pR_p(d)$, it suffices to bound

$$\sum_{\substack{d|N \\ d\leq\sqrt{N}}} \frac{d+4}{3} \leq \sum_{\substack{d|N \\ d\leq\sqrt{N}}} \frac{\sqrt{N}+4}{3} \leq \sigma_0(N)\frac{\sqrt{N}+4}{3}.$$

Since $\sigma_0(N) \ll N^{\epsilon}$ by [**Apo76**, (31) on page 296], we obtain the claimed bound. □

Remark 13. The polynomial $Q_d(t)$ in step (2) of Algorithm 3.10 is closely related to the characteristic polynomial $H_d(z)$ of the Hecke operator T_p acting on the space $S_2(\Gamma_0(d))$, which may be computed via modular symbols computations. One may recover $Q_d(t)$ from $H_d(z)$ by first homogenizing H with an auxiliary variable t (say) to obtain $H_d(z,t)$, and setting $z = p + t^2$ (an observation we made in conjunction with Joseph Wetherell).

Remark 14. In our computations of nonsurjective primes for the database of typical genus 2 curves with conductor at most 2^{20} (including those in the LMFDB), we only needed to use polynomials $Q_d(t)$ for level up to 2^{10} (since step (1) of the Algorithm has a $\sqrt{N}$ term). We are grateful to Andrew Sutherland for providing us with a precomputed dataset of the characteristic polynomials of the Hecke operators for these levels, resulting from the creation of an extensive database of modular forms going well beyond what was previously available [**BBB$^+$21**].

Remark 15. Our Sage implementation uses two auxiliary primes in Step 2(b) of the above algorithm. Increasing the number of such primes yields smaller supersets at the expense of longer runtime.

3.2. Good primes that are geometrically irreducible. Let ϕ be any quadratic Dirichlet character $\phi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$. Our goal in this subsection is to find all good primes ℓ governed by ϕ, by which we mean that

$$\mathrm{tr}(\rho_{A,\ell}(\mathrm{Frob}_p)) \equiv a_p \equiv 0 \bmod \ell$$

whenever $\phi(p) = -1$. (Recall that $-a_p$ is the coefficient of t^3 in $P_p(t)$).

We will consider the set of all quadratic Dirichlet character $\phi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$. Using the structure theorem for finite abelian groups and the fact that ϕ factors through $(\mathbb{Z}/N\mathbb{Z})^\times/(\mathbb{Z}/N\mathbb{Z})^{\times 2}$, this set has the structure of an $\mathbb{F}_2$-vector space of dimension

$$d(N) \coloneqq \omega(N) + \begin{cases} 0 & : \ v_2(N) = 0 \\ -1 & : \ v_2(N) = 1 \\ 0 & : \ v_2(N) = 2 \\ 1 & : \ v_2(N) \geq 3, \end{cases}$$

where $\omega(m)$ denotes the number of prime factors of m and $v_2(m)$ is the 2-adic valuation of m. In particular, $d(N) \leq \omega(N) + 1$.

Algorithm 3.13 ([**Die02**, Sections 3.4-3.5]). *Given a typical genus 2 Jacobian $A/\mathbb{Q}$ of conductor N, compute an integer M_{quad} as follows.*

(1) *Compute the set S of quadratic Dirichlet characters $\phi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$.*
(2) *For each $\phi \in S$:*
  (a) *Choose a nonempty finite set $\mathcal{T}$ of "auxiliary" primes $p \nmid N$ for which $a_p \neq 0$ and $\phi(p) = -1$.*
  (b) *Take the greatest common divisor*

$$M_\phi \coloneqq \gcd_{p \in \mathcal{T}}(p a_p),$$

  over all auxiliary primes p.
(3) *Let $M_{quad} \coloneqq \prod_{\phi \in S} M_\phi$.*

Return the list of prime divisors ℓ of M_{quad}.

Proposition 3.14. *Any good prime ℓ for which ℓ is governed by a quadratic character is returned by Algorithm 3.13.*

Proof. Suppose that ℓ is governed by the quadratic character $\phi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$. Then for every good prime $p \neq \ell$ for which $\phi(p) = -1$, the prime ℓ must divide the integral trace a_p of Frobenius. Hence ℓ divides M_ϕ and M_{quad}. □

Proposition 3.15. *Algorithm 3.13 terminates. More precisely, if q is the smallest surjective prime for A, then a good prime p for which $\phi(p) = -1$ and a_p is nonzero is bounded by a function of q. Assuming GRH, $p \ll 2^{2d(N)} q^{22} \log^2(qN)$, where the implied constant is absolute and effectively computable. Moreover, we have*

$$\prod_{\phi \in S} \prod_{\substack{\ell \text{ governed} \\ \text{by } \phi}} \ell \ll \left(2^{3d(N)} q^{33} \log^3(qN)\right)^{2 - 2^{1-d(N)}} \ll 2^{6\omega(N)} q^{66} \log^6(qN),$$

where the implied constant is absolute and effectively computable.

Proof. We imitate the proof of [**LV14b**, Lemma 21] in our setting. Let V be the d-dimensional $\mathbb{F}_2$-vector space of quadratic Dirichlet characters of modulus N (equivalently, quadratic Galois characters unramified outside of N). Let $\rho_V\colon G_K \to$

$V^\vee$ denote the representation sending Frob_p to the linear functional $\phi \mapsto \phi(p)$. Since the character for $\mathrm{PGSp}_4(\mathbb{F}_q)/\mathrm{PSp}_4(\mathbb{F}_q)$ is the abelianization of $\mathbb{P}\rho_{A,q}$, we conclude in the same way as [**LV14b**, Proof of Lemma 21] that for any $\alpha \in V^\vee$, there exists an $X_\alpha \in \mathrm{GSp}_4(\mathbb{F}_q)$ with $\mathrm{tr}(X_\alpha) \neq 0$ such that (α, X_α) is in the image of $\rho_V \times \rho_{A,\ell}$.

Apply the effective Chebotarev density theorem to the Galois extension corresponding to $\rho_V \times \rho_{A,q}$. This has degree at most $2^{d(N)}|\mathrm{GSp}_4(\mathbb{F}_q)|$ and is unramified outside of qN. Therefore, assuming GRH and combining (5) and (6), there exists a prime

$$p_\alpha \ll 2^{2d(N)} q^{22} \log^2(qN)$$

for which $(\alpha, X_\alpha) = (\rho_V(\mathrm{Frob}_{p_\alpha}), \rho_{A,q}(\mathrm{Frob}_{p_\alpha}))$. Let ϕ be a character not in the kernel of α. Any exceptional prime ℓ governed by ϕ must divide $p_\alpha a_{p_\alpha}$, which is nonzero because it is nonzero modulo q. This proves that the algorithm terminates, since every ϕ is not in the kernel of precisely half of all $\alpha \in V^\vee$. We now bound the size of the product of all ℓ governed by a character in S. If ℓ is governed by ϕ, then ℓ divides the quantity

$$p|a_p| \leq p^{3/2} \ll 2^{3d(N)} q^{33} \log^3(qN).$$

Taking the product over all nonzero α in V (of which there are $2^{d(N)} - 1$), each ℓ will show up half the time, so we obtain:

$$\left(\prod_{\substack{\ell \text{ governed} \\ \text{by } \phi \in S}} \ell \right)^{2^{d(N)-1}} \ll \left(2^{3d(N)} q^{33} \log^3(qN)\right)^{2^{d(N)}-1},$$

which implies the result by taking the $(2^{d(N)-1})$th root of both sides. □

Putting all of these pieces together, we obtain the following.

Proof of Theorem 1.1(1). If $\rho_{A,\ell}$ is nonsurjective, $\ell > 7$, and $\ell \nmid N$, then Proposition 2.9 implies that $\rho_{A,\ell}(G_\mathbb{Q})$ must be in one of the maximal subgroups of Type (1) or (2) listed in Lemma 2.3. If it is contained in one of the reducible subgroups, i.e. the subgroups of Type (1), then $\rho_{A,\ell}(G_\mathbb{Q})$ (and, hence, $\rho_{A,\ell}(G_\mathbb{Q}) \otimes \overline{\mathbb{F}}_\ell$) is reducible, and so ℓ is added to PossiblyNonsurjectivePrimes in Step (3) by Propositions 3.4, 3.7, and 3.11. If $\rho_{A,\ell}(G_\mathbb{Q})$ is contained in one of the index 2 subgroups M_ℓ of an irreducible subgroup of Type (2) listed in Lemma 2.3, then again ℓ is added to PossiblyNonsurjectivePrimes in Step (3), since $M_\ell \otimes \overline{\mathbb{F}}_\ell$ is always reducible by Lemma 2.4(1b).

Hence we may assume that $\rho_{A,\ell}(G_\mathbb{Q})$ is contained in one of the irreducible maximal subgroups G_ℓ of Type (2) listed in Lemma 2.3, but not in the index 2 subgroup M_ℓ. The normalizer character

$$G_\mathbb{Q} \xrightarrow{\rho_{A,\ell}} G_\ell \to G_\ell/M_\ell = \{\pm 1\}$$

is nontrivial and unramified outside of N, and so it corresponds to a quadratic Dirichlet character $\phi\colon (\mathbb{Z}/N\mathbb{Z})^\times \to \{\pm 1\}$. Lemma 2.4(1a) shows that $\mathrm{tr}(g) = 0$ in $\mathbb{F}_\ell$ for any $g \in G_\ell \smallsetminus M_\ell$. Consequently, ℓ is governed by ϕ (in the language of Section 3.2), so ℓ is added to PossiblyNonsurjectivePrimes in Step (4) by Proposition 3.14. □

3.3. Bounds on Serre's open image theorem.

In this section we combine the theoretical worst case bounds in the Algorithms 3.3, 3.6, 3.10, and 3.13 to give a bound on the smallest surjective good prime q, and the product of all nonsurjective primes, thereby establishing Theorem 1.2.

Corollary 3.16. *Let $A/\mathbb{Q}$ be a typical genus 2 Jacobian of conductor N. Assuming GRH, we have*

$$\prod_{\ell \textit{ nonsurjective}} \ell \ll \exp(N^{1/2+\epsilon}),$$

where the implied constant is absolute and effectively computable.

Proof. Let q be the smallest surjective good prime for A, which is finite by Serre's open image theorem. Multiplying the bounds in Propositions 3.5, 3.8, 3.12, and 3.15 by the conductor N, the product of all nonsurjective primes is bounded by a function of q and N of the following shape

$$\prod_{\ell \text{ nonsurjective}} \ell \ll q^{N^{1/2+\epsilon}}. \tag{9}$$

On the other hand, since q is the smallest surjective prime by definition, the product of all primes less than q divides the product of all nonsurjective primes. Using [**Ser81**, Lemme 11], we have

$$\exp(q) \ll \prod_{\ell<q} \ell \leq \prod_{\ell \text{ nonsurjective}} \ell \ll q^{N^{1/2+\epsilon}}.$$

Combining the first and last terms, we have $q \ll N^{1/2+\epsilon}\log(q)$, whence $q \ll N^{1/2+\epsilon}$. Plugging this back into (9) yields a bound of $(N^{1/2+\epsilon})^{N^{1/2+\epsilon}}$. By taking logarithms and using that $\log N \ll N^{\epsilon}$, one sees that $(N^{1/2+\epsilon})^{N^{1/2+\epsilon}} \ll \exp(N^{1/2+\epsilon})$, and the claimed bound follows. □

4. Testing surjectivity of $\rho_{A,\ell}$

In this section we establish Theorem 1.1(2). The goal is to weed out any extraneous nonsurjective primes in the output PossiblyNonsurjectivePrimes of Algorithm 3.1 to produce a smaller list LikelyNonsurjectivePrimes(B) containing all nonsurjective primes (depending on a chosen bound B) by testing the characteristic polynomials of Frobenius elements up to the bound B. If B is sufficiently large (quantified in Section 5), the list LikelyNonsurjectivePrimes(B) is provably the list of nonsurjective primes.

Algorithm 4.1. *Given $B > 0$ and the output* PossiblyNonsurjectivePrimes *of Algorithm 3.1 for the typical genus 2 curve with equation $y^2 + h(x)y = f(x)$, output a sublist* LikelyNonsurjectivePrimes(B) *of* PossiblyNonsurjectivePrimes *as follows.*

(1) *Initialize* LikelyNonsurjectivePrimes(B) *as* PossiblyNonsurjectivePrimes.
(2) *Remove 2 from* LikelyNonsurjectivePrimes(B) *if the size of the Galois group of the splitting field of $4f + h^2$ is 720.*
(3) *For each good prime $p < B$, while* LikelyNonsurjectivePrimes(B) *is nonempty:*
    (a) *Compute the integral characteristic polynomial $P_p(t)$ of* Frob_p.
    (b) *For each prime ℓ in* LikelyNonsurjectivePrimes(B), *run Tests 4.4*(i), (ii), *and* (iii) *on $P_p(t)$ to rule out $\rho_{A,\ell}(G_{\mathbb{Q}})$ being contained in one of the exceptional maximal subgroups.*

(c) *For each prime ℓ in* $\mathsf{LikelyNonsurjectivePrimes}(B)$*, run Tests 4.5*(i) *and* (ii) *on $P_p(t)$ to rule out $\rho_{A,\ell}(G_{\mathbb{Q}})$ being contained in one of the nonexceptional maximal subgroups.*

(d) *If there exists $\ell \in$* $\mathsf{LikelyNonsurjectivePrimes}(B)$ *for which each of the 5 tests Tests 4.4*(i)–(iii) *and Tests 4.5*(i)–(ii) *have succeeded at least once, remove ℓ.*

(4) *Return* $\mathsf{LikelyNonsurjectivePrimes}(B)$*.*

Remark 16. In our implementation of Step 3 of this algorithm, we have chosen to only use primes p of good reduction for the curve as auxiliary primes, which is a stronger condition than being a good prime for the Jacobian A. More precisely, the primes that are good for the Jacobian but bad for the curve are precisely the prime factors of the discriminant $4f + h^2$ of a minimal equation for the curve that do not divide the conductor N_A of the Jacobian. At such a prime, the reduction of the curve consists of two elliptic curves E_1 and E_2 intersecting transversally at a single point. Since there are many auxiliary primes $p < B$ to choose from, excluding bad primes for the curve is not a serious restriction, but allows us to access the characteristic polynomial of Frobenius directly by counting points on the reduction of the curve. This is not strictly necessary: one could use the characteristic polynomials of Frobenius for the elliptic curves E_1 and E_2, which can be computed using the `genus2reduction` module of SageMath.

We briefly summarize the contents of this section. In Section 4.1, we first prove a purely group-theoretic criterion for a subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ to equal the whole group. Then in Section 4.2, we explain Test 4.4 and Test 4.5, whose validity follows immediately from Lemma 2.4(3) and Proposition 4.2 respectively. The main idea of these tests is to use auxiliary good primes $p \neq \ell$ to generate characteristic polynomials in the image of $\rho_{A,\ell}$. If we find enough types of characteristic polynomials to rule out each proper maximal subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ (cf. Proposition 4.2), then we can conclude that $\rho_{A,\ell}$ is surjective. In Section 4.3, we prove Theorems 1.1(2) and 1.3 that justify this algorithm.

4.1. A group-theoretic criterion.

We now use the classification of maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ described in Section 2.4 to deduce a group-theoretic criterion for a subgroup G of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ to be the whole group. This is analogous to [**Ser72**, Proposition 19 (i)-(ii)].

Proposition 4.2. *Fix a prime $\ell \neq 2$ and a subgroup $G \subseteq \mathrm{GSp}_4(\mathbb{F}_\ell)$ with surjective similitude character. Assume that G is not contained in one of the exceptional maximal subgroups described in Lemma 2.3*(4)*. Then $G = \mathrm{GSp}_4(\mathbb{F}_\ell)$ if and only if there exists matrices $X, Y \in G$ such that*

(a) *the characteristic polynomial of X is irreducible; and*

(b) $\mathrm{trace}\, Y \neq 0$ *and the characteristic polynomial of Y has a linear factor with multiplicity one.*

Proof. The ‘only if’ direction follows from Proposition 5.1 below, where we show that a *nonzero* proportion of elements of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ satisfy the conditions in (a) and (b).

Now assume that the group G has elements X and Y as in the statement of the proposition. We have to show that $G = \mathrm{GSp}_4(\mathbb{F}_\ell)$. By assumption, G is not a subgroup of a maximal subgroup of type (4). For each of the remaining types of maximal subgroups in Lemma 2.3, we will use one of the elements X or Y to rule out G being contained in a subgroup of that type.

(a) By Lemma 2.2 (iv), every element of a subgroup of type (1) has a reducible characteristic polynomial. The same is true for elements of type (3) by Lemma 2.4 (2). This is violated by the element X, so G cannot be contained in a subgroup of type (1) or type (3).

(b) Recall the notation used in the description of a type (2) maximal subgroups in Lemma 2.3. By Lemma 2.4 1a, every element in $G_\ell \smallsetminus M_\ell$ has trace 0. By Lemma 2.2 (iii), an element with irreducible characteristic polynomial automatically has nonzero trace. Hence both X and Y have nonzero traces, and so cannot be contained in $G_\ell \smallsetminus M_\ell$. We now consider two cases
   (i) If the two subspaces are individually defined over $\mathbb{F}_\ell$, then every element in M_ℓ preserves a two-dimensional subspace and hence has a reducible characteristic polynomial. This is violated by the element X.
   (ii) If the two subspaces are permuted by $G_{\mathbb{F}_\ell}$, then the action of M_ℓ on the corresponding subspaces V and V' are conjugate. Therefore, every $\mathbb{F}_\ell$-rational eigenvalue for the action of Frob_p on V, also appears as an eigenvalue for the action on V', with the same multiplicity. This is violated by the element Y.

   Hence G cannot be contained in a maximal subgroup of type (2).

Since any subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ that is not contained in a proper maximal subgroup of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ must equal $\mathrm{GSp}_4(\mathbb{F}_\ell)$, we are done. □

REMARK 17. [**AdRK13**, Corollary 2.2] gives a very similar criterion for a subgroup G of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ to contain $\mathrm{Sp}_4(\mathbb{F}_\ell)$, namely that it contains a transvection, and also an element with irreducible characteristic polynomial (and hence automatically nonzero trace).

4.2. Surjectivity tests.

4.2.1. *Surjectivity test for $\ell = 2$.*

PROPOSITION 4.3. *Let A be the Jacobian of the hyperelliptic curve $y^2 + h(x)y = f(x)$ defined over $\mathbb{Q}$. Then $\rho_{A,2}$ is surjective if and only if the size of the Galois group of the splitting field of $4f + h^2$ is 720.*

PROOF. This follows from the fact that $\mathrm{GSp}_4(\mathbb{F}_2) \cong S_6$ which is a group of size 720, and that the representation $\rho_{A,2}$ is the permutation action of the Galois group on the six roots of $4f + h^2$. □

4.2.2. *Surjectivity tests for $\ell \neq 2$.*

The tests to rule out the exceptional maximal subgroups rely on the existence of the finite lists C_{1920} and C_{720} (independent of ℓ), and $C_{7,5040}$ given in Lemma 2.4(3).

TEST 4.4 (Tests for ruling out exceptional maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for $\ell \neq 2$).
Given a polynomial $P_p(t) = t^4 - a_p t + b_p t^2 - pa_p t + p^2$ and $\ell \geq 2$,

(i) $P_p(t)$ passes Test 4.4 (i) if $\ell \equiv \pm 1 \bmod 8$ or $(a_p^2/p, b_p/p) \bmod \ell$ lies outside of $C_{1920} \bmod \ell$.
(ii) $P_p(t)$ passes Test 4.4 (ii) if $\ell \equiv \pm 1 \bmod 12$ or $(a_p^2/p, b_p/p) \bmod \ell$ lies outside of $C_{720} \bmod \ell$.
(iii) $P_p(t)$ passes Test 4.4 (iii) if $\ell \neq 7$ or $(a_p^2/p, b_p/p) \bmod \ell$ lies outside of $C_{7,5040}$.

Test 4.5 (Tests for ruling out non-exceptional maximal subgroups for $\ell \neq 2$). Given a polynomial $P_p(t) = t^4 - a_p t + b_p t^2 - pa_p t + p^2$ and $\ell \geq 2$,

(i) $P_p(t)$ passes Test 4.5 (i) if $P_p(t)$ modulo ℓ is irreducible.

(ii) $P_p(t)$ passes Test 4.5 (ii) if $P_p(t)$ modulo ℓ has a linear factor of multiplicity 1 and has nonzero trace.

For any one of the five tests above, say that the test succeeds if a given polynomial $P_p(t)$ passes the corresponding test.

Remark 18. We call an auxiliary prime p a witness for a given prime ℓ if the polynomial $P_p(t)$ passes one of our tests for ℓ. The verbose output of our code prints witnesses for each of our tests for each prime ℓ in PossiblyNonsurjectivePrimes but not in LikelyNonsurjectivePrimes(B).

4.3. Justification for surjectivity tests. Considering Tests 4.4 and 4.5, we define

$$\begin{aligned}
C_\alpha &= \{M \in \mathrm{GSp}_4(\mathbb{F}_\ell) : P_M(t) \text{ is irreducible}\}\\
C_\beta &= \{M \in \mathrm{GSp}_4(\mathbb{F}_\ell) : \mathrm{tr}(M) \neq 0 \text{ and } P_M(t) \text{ has a linear factor of multiplicity } 1\}\\
C_{\gamma_1} &= \left\{M \in \mathrm{GSp}_4(\mathbb{F}_\ell) : \left(\frac{\mathrm{tr}(M)^2}{\mathrm{mult}(M)}, \frac{\mathrm{mid}(M)}{\mathrm{mult}(M)}\right) \notin C_{\ell,1920} \text{ or } \ell \equiv \pm 1 \bmod 8\right\}\\
C_{\gamma_2} &= \left\{M \in \mathrm{GSp}_4(\mathbb{F}_\ell) : \left(\frac{\mathrm{tr}(M)^2}{\mathrm{mult}(M)}, \frac{\mathrm{mid}(M)}{\mathrm{mult}(M)}\right) \notin C_{\ell,720} \text{ or } \ell \equiv \pm 1 \bmod 12\right\}\\
C_{\gamma_3} &= \left\{M \in \mathrm{GSp}_4(\mathbb{F}_\ell) : \left(\frac{\mathrm{tr}(M)^2}{\mathrm{mult}(M)}, \frac{\mathrm{mid}(M)}{\mathrm{mult}(M)}\right) \notin C_{\ell,5040} \text{ or } \ell \neq 7\right\}\\
C_\gamma &= C_{\gamma_1} \cap C_{\gamma_2} \cap C_{\gamma_3}.
\end{aligned}$$

Proof of Theorem 1.1(2) and Theorem 1.3. Let $B > 0$. Since the list LikelyNonsurjectivePrimes(B) is a sublist of PossiblyNonsurjectivePrimes, which contains all nonsurjective primes by Theorem 1.1(1), any prime which is not in the list PossiblyNonsurjectivePrimes is surjective. Let $\ell \in$ PossiblyNonsurjectivePrimes and **not** in LikelyNonsurjectivePrimes(B). If $\ell = 2$, then by Proposition 4.3, $\rho_{A,2}$ is surjective. If $\ell > 2$, this means that we found primes $p_1, p_2, p_3, p_4, p_5 \leq B$ each distinct from ℓ and of good reduction for A for which $\rho_{A,\ell}(\mathrm{Frob}_{p_1}) \in C_\alpha$, $\rho_{A,\ell}(\mathrm{Frob}_{p_2}) \in C_\beta$, $\rho_{A,\ell}(\mathrm{Frob}_{p_3}) \in C_{\gamma_1}$, $\rho_{A,\ell}(\mathrm{Frob}_{p_4}) \in C_{\gamma_2}$, and $\rho_{A,\ell}(\mathrm{Frob}_{p_4}) \in C_{\gamma_3}$. Note that by (2), the similitude factor $\mathrm{mult}(\rho_{A,\ell}(\mathrm{Frob}_p))$ is p. Therefore, by Lemma 2.4(3), it follows that $\rho_{A,\ell}(G_\mathbb{Q})$ is not contained in an exceptional maximal subgroup. The surjectivity of $\rho_{A,\ell}$ now follows from Proposition 4.2.

Finally, we will show that if B is sufficiently large (as quantified by Theorem 1.3), then any prime ℓ in LikelyNonsurjectivePrimes is nonsurjective. Since the sets C_α, C_β, C_{γ_1}, C_{γ_2} and C_{γ_3} are nonempty by Proposition 5.1 below and closed under conjugation, it follows from Lemma 2.10 that there exist primes $p_1, p_2, p_3, p_4, p_5 \leq B$ as above. □

Remark 19. If we assume both GRH and AHC, Ram Murty and Kumar Murty [**MM97**, p. 52] noted (see also [**FJ20**, Theorem 2.3]) that the bound (5) can be replaced with $p \ll \frac{(\log d_K)^2}{|S|}$. Proposition 5.1, which follows, shows that the sets C_α, C_β, and C_γ have size at least $\frac{|\mathrm{GSp}_4(\mathbb{F}_\ell)|}{10}$. This can be used to prove the ineffective version of Theorem 1.3 which relies on AHC noted in the introduction in a manner similar to the proof of Theorem 1.3.

5. The probability of success

In this section we prove Theorem 1.4, by studying the respective probabilities α_ℓ, β_ℓ, and γ_ℓ that a matrix chosen uniformly at random from $\mathrm{GSp}_4(\mathbb{F}_\ell)$ is contained in each of C_α, C_β, and C_γ defined in Section 4.3.

Proposition 5.1. *Let M be a matrix chosen uniformly at random from $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with ℓ odd. Then*

(i) *The probability that $M \in C_\alpha$ is given by*

$$\alpha_\ell = \frac{1}{4} - \frac{1}{2(\ell^2+1)}.$$

(ii) *The probability that $M \in C_\beta$ is given by*

$$\beta_\ell = \frac{3}{8} - \frac{3}{4(\ell-1)} + \frac{1}{2(\ell-1)^2}.$$

(iii) *The probability that $M \in C_\gamma$ is*

$$\gamma_\ell \geq 1 - \frac{3\ell}{\ell^2+1}.$$

[**Shi82**] characterizes all conjugacy classes of elements of $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for ℓ odd, grouping them into 26 different types. For each type γ, Shinoda further computes the number $N(\gamma)$ of conjugacy classes of type γ and the size $|C_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma)|$ of the centralizer, which is the size $|C_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(M)|$ of the centralizer of M in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ for any M in a conjugacy class of type γ. The size $|C(\gamma)|$ of any conjugacy class of type γ can then easily be computed as $|\mathcal{C}(\gamma)| = \frac{|\mathrm{GSp}_4(\mathbb{F}_\ell)|}{|C_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma)|}$ and the probability that a uniformly chosen $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ has conjugacy type γ is then given by

$$\frac{N(\gamma)|\mathcal{C}(\gamma)|}{|\mathrm{GSp}_4(\mathbb{F}_\ell)|} = \frac{N(\gamma)}{|C_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma)|}. \tag{10}$$

To prove Proposition 5.1, we will need to examine a handful of types of conjugacy classes of $\mathrm{GSp}_4(\mathbb{F}_\ell)$. There is only a single conjugacy type γ whose characteristic polynomials are irreducible. This type is denoted K_0 in [**Shi82**] where it is shown there that $N(K_0) = \frac{(\ell-1)(\ell^2-1)}{4}$ and $|C_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(K_0)| = (\ell-1)(\ell^2+1)$.

While there is only one way for a polynomial to be irreducible, there are several ways for a quartic polynomial to have a root of odd order. However, only some of these can occur if $f(t)$ is the characteristic polynomial of a matrix $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ and we only need to concern ourselves with the following three possibilities:

(a) $f(t)$ splits completely over $\mathbb{F}_\ell$;
(b) $f(t)$ has two roots over $\mathbb{F}_\ell$, both of which occur with multiplicity one; and
(c) $f(t)$ has two simple roots and one double root over $\mathbb{F}_\ell$.

Cases (a) and (b) correspond to the conjugacy types H_0 and J_0 in [**Shi82**] respectively. There are two types of conjugacy classes for which $f(t)$ has two simple roots and one double root, which are denoted by E_0 and E_1 in [**Shi82**].

Data for the relevant conjugacy class types is given by Table 2, including the probability that a uniform random $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ has conjugacy type γ via (10).

Type γ in [**Shi82**]	$N(\gamma)$	$\lvert C_{\mathrm{GSp}_4(\mathbb{F}_\ell)}(\gamma)\rvert$	Associated Probability
K_0 (Irreducible)	$\frac{(\ell-1)(\ell^2-1)}{4}$	$(\ell^2+1)(\ell-1)$	$\frac{1}{4}-\frac{1}{2(\ell^2+1)}$
H_0 (Split)	$\frac{(\ell-1)(\ell-3)^2}{8}$	$(\ell-1)^3$	$\frac{1}{8}-\frac{1}{2(\ell-1)}+\frac{1}{2(\ell-1)^2}$
J_0 (Two Simple Roots)	$\frac{(\ell-1)^3}{4}$	$(\ell+1)(\ell-1)^2$	$\frac{1}{4}-\frac{1}{2(\ell+1)}$
E_0 (One Double Root)	$\frac{(\ell-1)(\ell-3)}{2}$	$\ell(\ell-1)^2(\ell^2-1)$	$\frac{1}{2\ell(\ell^2-1)}-\frac{1}{\ell(\ell-1)(\ell^2-1)}$
E_1 (One Double Root)	$\frac{(\ell-1)(\ell-3)}{2}$	$\ell(\ell-1)^2$	$\frac{1}{2\ell}-\frac{1}{\ell(\ell-1)}$

TABLE 2. Number of conjugacy classes and centralizer sizes for each conjugacy class type in [**Shi82**].

PROOF OF PROPOSITION 5.1. Part (i) is simply the entry in Table 2 in the last column corresponding to the "K_0 (Irreducible)" type.

We now establish part (ii). As indicated in the discussion above Table 2, the only conjugacy classes of matrices in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ whose characteristic polynomials have some linear factors of odd multiplicity are those of the types H_0, J_0, E_0, E_1. However, for part (ii) since we are only interested in matrices M also having nonzero trace, it is insufficient to simply sum over the rightmost entries in the bottom four rows of Table 2. From [**Shi82**, Table 2], we see that the elements of E_0 and E_1 have trace $\frac{c(a+1)^2}{a}$ for some $c, a \in \mathbb{F}_\ell^\times$ with $a \neq \pm 1$. In particular, it follows that elements of types E_0 and E_1 have nonzero traces. The elements of type J_0 have trace $\frac{(c+a)(c+a^\ell)}{c}$ where $c \in \mathbb{F}_\ell^\times$ and $a \in \mathbb{F}_{\ell^2} \smallsetminus \mathbb{F}_\ell$. Therefore, the elements of type J_0 also have nonzero trace.

It remains to analyze which conjugacy classes of Type H_0 have nonzero trace. Following [**Shi82**], the $\frac{(\ell-1)(\ell-3)^2}{8}$ conjugacy classes of type H_0 correspond to quadruples of distinct elements in $a_1, a_2, b_1, b_2 \in \mathbb{F}_\ell^\times$ satisfying $a_1 b_1 = a_2 b_2$ modulo the action of swapping any of a_1 with b_1, a_2 with b_2, or a_1, b_1 with a_2, b_2. The eigenvalues of any matrix in the conjugacy class are a_1, a_2, b_1, and b_2. Consequently the matrix has trace zero only if either $a_2 = -a_1$ and $b_2 = -b_1$ or $b_1 = -a_2$ and $b_2 = -a_1$. This accounts for $\frac{(\ell-1)(\ell-3)}{4}$ of the $\frac{(\ell-1)(\ell-3)^2}{8}$ conjugacy classes of type H_0, leaving $\frac{(\ell-1)(\ell-3)(\ell-5)}{8}$ conjugacy classes with non-zero trace. As a result, the probability that a matrix $M \in \mathrm{GSp}_4(\mathbb{F}_\ell)$ chosen uniformly at random has non-zero trace and totally split characteristic polynomial is

$$\frac{(\ell-1)(\ell-3)(\ell-5)}{8(\ell-1)^3} = \frac{1}{8} - \frac{3}{4(\ell-1)} + \frac{1}{(\ell-1)^2}. \tag{11}$$

To obtain part (ii), we add (11) to the entries in the rightmost column of the final three rows of Table 2, getting

$$\left(\frac{1}{8} - \frac{3}{4(\ell-1)} + \frac{1}{(\ell-1)^2}\right) + \left(\frac{1}{4} - \frac{1}{2(\ell+1)}\right) + \left(\frac{1}{2\ell(\ell^2-1)} - \frac{1}{\ell(\ell-1)(\ell^2-1)}\right) + \left(\frac{1}{2\ell} - \frac{1}{\ell(\ell-1)}\right) = \frac{3}{8} - \frac{3}{4(\ell-1)} + \frac{1}{2(\ell-1)^2}.$$

To prove (iii), note that for any pair (u, v), the cardinality of the set

$$\{t^4 - at^3 + bt^2 - amt + m^2 : a, b \in \mathbb{F}_\ell, m \in \mathbb{F}_\ell^\times \text{ and } (\tfrac{a^2}{m}, \tfrac{b}{m}) = (u, v)\}$$

is at most $\ell - 1$. By [**Cha97**, Theorem 3.5], the number of matrices in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ with a given characteristic polynomial is at most $(\ell+3)^8$. Assuming $\ell \neq 7$, by combining these observations, and noting that $|C_{\ell,720} \cup C_{\ell,1920}| \leq 14$, we obtain the bound

$$\gamma_\ell \geq 1 - \frac{14(\ell-1)(\ell+3)^8}{|\,\mathrm{GSp}_4(\mathbb{F}_\ell)|}.$$

For $\ell > 17$, this implies the claimed bound. For $3 \leq \ell \leq 17$, we directly check the claim using Magma. □

Lemma 5.2. *Let $C/\mathbb{Q}$ be a typical genus 2 curve with Jacobian A and suppose ℓ is an odd prime such that $\rho_{A,\ell}$ is surjective. For any $\epsilon > 0$, there exists an effective constant B_0 (with $B_0 > \ell N_A$) such that for any $B > B_0$ and each $\delta \in \{\alpha, \beta, \gamma\}$, we have*

$$\left| \frac{|\{p \textit{ prime} : B \leq p \leq 2B \textit{ and } \rho_{A,\ell}(\mathrm{Frob}_p) \in C_\delta\}|}{|\{p \textit{ prime} : B \leq p \leq 2B\}|} - \delta_\ell \right| < \epsilon.$$

Proof. Let $G = \mathrm{Gal}(\mathbb{Q}(A[\ell])/\mathbb{Q})$ and $S \subseteq G$ be any subset that is closed under conjugation. By taking B to be sufficiently large, we have that $B > \ell N_A$ and can make

$$\left| \frac{|\{p \text{ prime} : B \leq p \leq 2B \text{ and } \mathrm{Frob}_p \in S\}|}{|\{p \text{ prime} : B \leq p \leq 2B\}|} - \frac{|S|}{|G|} \right|$$

arbitrarily small by (4). Moreover, the previous statement can be made effective by using an effective version of the Chebotarev density theorem; in particular, the value B_0 must be larger than the bound B from Equation (1). The result then follows because each of the sets C_α, C_β, and C_γ is closed under conjugation. □

For positive integers n and $B > \ell N_A$, let $P(B,n)$ be the probability that n primes $p_1, \dots, p_n$ (possibly non-distinct) chosen uniformly at random in the interval $[B, 2B]$ have the property that

$$\rho_{A,\ell}(\mathrm{Frob}_{p_i}) \notin C_\alpha \text{ for each } i \quad \text{or} \quad \rho_{A,\ell}(\mathrm{Frob}_{p_i}) \notin C_\beta \text{ for each } i$$
$$\text{or} \quad \rho_{A,\ell}(\mathrm{Frob}_{p_i}) \notin C_\gamma \text{ for each } i.$$

Corollary 5.3. *Suppose C and ℓ are as in Lemma 5.2 and let n be a positive integer. For any $\epsilon > 0$, there exists an effective constant B_0 (with $B_0 > \ell N_A$) such that for all $B > B_0$, we have*

$$P(B,n) < (1-\alpha_\ell)^n + (1-\beta_\ell)^n + (1-\gamma_\ell)^n + \epsilon.$$

Proof. For $\delta \in \{\alpha, \beta, \gamma\}$, let X_δ be the event that none of the $\rho_{A,\ell}(\mathrm{Frob}_{p_i})$ are contained in C_δ. We then have

$$P(X_\alpha \cup X_\beta \cup X_\gamma) \leq P(X_\alpha) + P(X_\beta) + P(X_\gamma)$$

The result then follows by Lemma 5.2, which shows that there exists a B_0 such that the probabilities of X_α, X_β, and X_γ can be made arbitrarily close to $(1-\alpha_\ell)^n$, $(1-\beta_\ell)^n$, and $(1-\gamma_\ell)^n$ respectively. □

Proof of Theorem 1.4. The claim made by Theorem 1.4 is that $P(B,n) < 3 \cdot \left(\frac{9}{10}\right)^n$ for B sufficiently large. By Proposition 5.1, we have $1 - \alpha_\ell \leq \frac{4}{5}$, $1 - \beta_\ell \leq \frac{7}{8}$, and $1 - \gamma_\ell \leq \frac{9}{10}$ for all ℓ odd. The result then follows from Corollary 5.3 because $\left(\frac{4}{5}\right)^n + \left(\frac{7}{8}\right)^n + \left(\frac{9}{10}\right)^n < 3 \cdot \left(\frac{9}{10}\right)^n$. □

6. Results of computation and interesting examples

We report on the results of running our algorithm on a dataset of 1,743,737 typical genus 2 curves with conductor bounded by 2^{20} which are part of a new dataset of approximately 5 million curves currently being prepared for addition into the LMFDB. Running our algorithm on all of these curves in parallel took about 35 hours on MIT's Lovelace computer (see the Introduction for the hardware specification of this machine). Instructions for obtaining the entire results file may be found in the `README.md` file of the repository.

We first show in Table 3 how many of these curves were nonsurjective at particular primes, indicating also if this can be explained by the existence of a rational torsion point of that prime order. We found 31 as the largest nonsurjective prime, which occurred for the curve

$$y^2 + (x+1)y = x^5 + 23x^4 - 48x^3 + 85x^2 - 69x + 45 \tag{12}$$

of conductor $7^2 \cdot 31^2$ and discriminant $7^2 \cdot 31^9$ (the prime 2 was also nonsurjective here). The Jacobian of this curve does not admit a nontrivial rational 31-torsion point, so unlike many other instances of nonsurjective primes we observed, this one cannot be explained by the presence of rational torsion. One could ask if it might be explained by the existence of a $\mathbb{Q}$-rational 31-isogeny (as suggested by Algorithm 3.1, since 31 is returned by Algorithm 3.6). This seems to be the case - see forthcoming work of van Bommel, Chidambaram, Costa, and Kieffer [**vBCCK22**] where the isogeny class of this curve (among others) is computed.

nonsurj. prime	# w/ torsion	# w/o torsion	Example curve
2	1,060,966	437,201	464.a.464.1
3	76,265	95,108	277.a.277.2
5	11,365	10,044	16108.b.64432.1
7	1,857	2,056	295.a.295.2
11	162	203	4288.b.548864.1
13	106	261	439587.d.439587.1
17	22	51	1996.b.510976.1
19	10	20	1468.6012928
23	2	8	6784.1821066133504
29	1	5	79056.59014987776
31	0	1	47089.1295541485872879

TABLE 3. Nonsurjective primes in the dataset, and whether they are explained by torsion, with examples from the LMFDB dataset if available, else a string of the form "conductor.discrimnant".

We also observed (see Table 4) that the vast majority of curves had less than 3 nonsurjective primes.

It is interesting to compare Tables 3 and 4 to the analogous tables for non-CM elliptic curves over $\mathbb{Q}$ (3,816,674 curves), which are Tables 5 and 6 respectively (we omit example curves here since they can be readily searched for in the LMFDB).

# nonsurj. primes	# curves	Example curve	Nonsurj. primes of example
0	199,183	743.a.743.1	–
1	1,394,671	1923.a.1923.1	5(torsion)
2	148,606	976.a.999424.1	2, 29(torsion)
3	1,277	15876.a.15876.1	2, 3, 5

Table 4. Frequency count of nonsurjective primes in the dataset, with examples from the LMFDB dataset.

nonsurj. prime	# w/ torsion	# w/o torsion
2	1,332,490	5,726
3	57,930	213,654
5	1,545	19,211
7	80	4,100
11	0	156
13	0	736
17	0	40
37	0	96

Table 5. Nonsurjective primes for non-CM elliptic curves over $\mathbb{Q}$ in the LMFDB, and whether they are explained by torsion.

# nonsurj. primes	# curves
0	2,233,530
1	1,530,524
2	52,620

Table 6. Frequency count of nonsurjective primes for non-CM elliptic curves over $\mathbb{Q}$ in the LMFDB.

We observe a similar pattern regarding the majority of curves nonsurjective at 2 being explained by torsion, though in the elliptic curve case a much larger proportion are explained by 2-torsion than for genus 2 curves. This switches for the nonsurjective prime 3 in both cases, although again for elliptic curves, the discrepancy is much starker. The zeroes in the torsion column for Table 5 are explained by Mazur's torsion theorem. The number of nonsurjective primes between genus 1 and genus 2 is qualitatively different: the majority of elliptic curves do not have any nonsurjective primes, while the vast majority of genus 2 curves have precisely one nonsurjective prime. It is also curious that the elliptic curve dataset does not contain a curve with 3 nonsurjective primes.

We conclude with a few examples that illustrate where Algorithm 3.1 fails when the abelian surface has extra (geometric) endomorphisms.

Example 6.1. The Jacobian A of the genus 2 curve 3125.a.3125.1 on the LMFDB given by $y^2 + y = x^5$ has $\mathrm{End}(A_{\mathbb{Q}}) = \mathbb{Z}$ but $\mathrm{End}(A_{\overline{\mathbb{Q}}}) = \mathbb{Z}[\zeta_5]$. Let ϕ be the Dirichlet character of modulus 5 defined by the Legendre symbol

$$\phi\colon (\mathbb{Z}/5\mathbb{Z})^\times \to \{\pm 1\}, \qquad 2 \mapsto -1.$$

In this case, Algorithm 3.13 fails to find an auxilliary prime $p < 1000$ for which $a_p \neq 0$ and $\phi(p) = -1$. This is consistent with the endomorphism calculation, since the trace of $\rho_{A,\ell}(\mathrm{Frob}_p)$ is 0 for all primes p that do not split completely in $\mathbb{Q}(\zeta_5)$ and any inert prime in $\mathbb{Q}(\sqrt{5})$ automatically does not split completely in $\mathbb{Q}(\zeta_5)$.

Example 6.2. The modular curve $X_1(13)$ (169.a.169.1) has genus 2 and its Jacobian $J_1(13)$ has CM by $\mathbb{Z}[\zeta_3]$ over $\mathbb{Q}$. As in [**MT74**, Claim 2, page 45], for any prime ℓ that splits as $\pi\overline{\pi}$ in $\mathbb{Q}(\zeta_3)$, the representation $J_1(13)[\ell]$ splits as a direct sum $V_\pi \oplus V_{\overline{\pi}}$ of two 2-dimensional subrepresentations that are dual to each other. (A similar statement holds for $J_1(13)[\ell] \otimes_{\mathbb{F}_\ell} \overline{\mathbb{F}}_\ell$, and so this representation is never absolutely irreducible.) As expected, Algorithm 3.6 fails to find an auxiliary prime $p < 1000$ for which R_p is nonzero.

Example 6.3. The first (ordered by conductor) curve whose Jacobian J admits real multiplication over $\overline{\mathbb{Q}}$ is the curve 529.a.529.1; indeed, this Jacobian is isogenous to the Jacobian of the modular curve $X_0(23)$. Since there is a single Galois orbit of newforms - call it f - of level $\Gamma_0(23)$ and weight 2, we have that J is isogenous to the abelian variety A_f associated to f, and thus we expect the integer $M_{\text{self-dual}}$ output by Algorithm 3.10 to be zero for any auxiliary prime, which is indeed the case.

References

[AdRK13] Sara Arias-de Reyna and Christian Kappen, *Abelian varieties over number fields, tame ramification and big Galois image*, Math. Res. Lett. **20** (2013), no. 1, 1–17. MR 3126717

[AK19] Jeoung-Hwan Ahn and Soun-Hi Kwon, *An explicit upper bound for the least prime ideal in the Chebotarev density theorem*, Ann. Inst. Fourier (Grenoble) **69** (2019), no. 3, 1411–1458. MR 3986919

[Apo76] Tom M. Apostol, *Introduction to analytic number theory*, Undergraduate Texts in Mathematics, Springer-Verlag, New York-Heidelberg, 1976. MR 0434929

[BBB+21] Alex J. Best, Jonathan Bober, Andrew R. Booker, Edgar Costa, John E. Cremona, Maarten Derickx, Min Lee, David Lowry-Duda, David Roe, Andrew V. Sutherland, and John Voight, *Computing classical modular forms*, Arithmetic Geometry, Number Theory, and Computation (Cham) (Jennifer S. Balakrishnan, Noam Elkies, Brendan Hassett, Bjorn Poonen, Andrew V. Sutherland, and John Voight, eds.), Springer International Publishing, 2021, pp. 131–213.

[BCP97] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system (v2.27-9). I. The user language*, J. Symbolic Comput. **24** (1997), no. 3-4, 235–265, Computational algebra and number theory (London, 1993).

[BK94] Armand Brumer and Kenneth Kramer, *The conductor of an abelian variety*, Compositio Mathematica **92** (1994), no. 2, 227–248 (en). MR 1283229

[BPR13] Yuri Bilu, Pierre Parent, and Marusia Rebolledo, *Rational points on $X_0^+(p^r)$*, Ann. Inst. Fourier (Grenoble) **63** (2013), no. 3, 957–984.

[BS96] Eric Bach and Jonathan Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. **65** (1996), no. 216, 1717–1735. MR 1355006

[Car56] Leonard Carlitz, *Note on a quartic congruence*, Amer. Math. Monthly **63** (1956), 569–571. MR 81298

[Cha97] Nick Chavdarov, *The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy*, Duke Math. J. **87** (1997), no. 1, 151–180. MR 1440067

[CL12] John Cremona and Eric Larson, *Galois representations for elliptic curves over number fields*, 2012, SageMath.

[Coj05] Alina Carmen Cojocaru, *On the surjectivity of the Galois representations associated to non-CM elliptic curves*, Canad. Math. Bull. **48** (2005), no. 1, 16–31, With an appendix by Ernst Kani. MR 2118760

[Die02] Luis V. Dieulefait, *Explicit determination of the images of the Galois representations attached to abelian surfaces with* $\mathrm{End}(A) = \mathbb{Z}$, Experiment. Math. **11** (2002), no. 4, 503–512 (2003). MR 1969642

[FJ20] Daniel Fiorilli and Florent Jouve, *Distribution of Frobenius elements in families of Galois extensions*, 2020.

[GRR72] Alexander Grothendieck, Michel Raynaud, and Dock Sang Rim, *Groupes de monodromie en géométrie algébrique. I*, Lecture Notes in Mathematics, Vol. 288, Springer-Verlag, 1972, Séminaire de Géométrie Algébrique du Bois-Marie 1967–1969 (SGA 7 I).

[Kha06] Chandrashekhar Khare, *Serre's modularity conjecture: The level one case*, Duke Math. J. **134** (2006), no. 3, 557–589.

[KL90] Peter Kleidman and Martin Liebeck, *The subgroup structure of the finite classical groups*, London Mathematical Society Lecture Note Series, vol. 129, Cambridge University Press, Cambridge, 1990. MR 1057341

[Kra95] Alain Kraus, *Une remarque sur les points de torsion des courbes elliptiques*, C. R. Acad. Sci. Paris Sér. I Math. **321** (1995), no. 9, 1143–1146. MR 1360773

[KW09a] Chandrashekhar Khare and Jean-Pierre Wintenberger, *Serre's modularity conjecture (I)*, Invent. Math. **178** (2009), no. 3, 485–504.

[KW09b] ———, *Serre's modularity conjecture (II)*, Invent. Math. **178** (2009), no. 3, 505–586.

[KW22] Habiba Kadiri and Peng-Jie Wong, *Primes in the Chebotarev density theorem for all number fields (with an Appendix by Andrew Fiori)*, J. Number Theory **241** (2022), 700–737. MR 4472459

[Liu94] Qing Liu, *Conducteur et discriminant minimal de courbes de genre* 2, Compositio Mathematica **94** (1994), no. 1, 51–79.

[LMF22] The LMFDB Collaboration, *The L-functions and modular forms database*, `http://www.lmfdb.org`, 2022, [Online; accessed 12 December 2022].

[LMO79] Jeffrey C. Lagarias, Hugh L. Montgomery, and Andrew M. Odlyzko, *A bound for the least prime ideal in the Chebotarev density theorem*, Invent. Math. **54** (1979), no. 3, 271–296. MR 553223

[Lom16] Davide Lombardo, *Explicit surjectivity of Galois representations for abelian surfaces and* GL_2*-varieties*, Journal of Algebra **460** (2016), 26–59.

[LV14a] Eric Larson and Dmitry Vaintrob, *Determinants of subquotients of Galois representations associated with abelian varieties*, Journal of the Institute of Mathematics of Jussieu **13** (2014), no. 3, 517–559.

[LV14b] ———, *On the surjectivity of Galois representations associated to elliptic curves over number fields*, Bull. Lond. Math. Soc. **46** (2014), no. 1, 197–209. MR 3161774

[LV22] Davide Lombardo and Matteo Verzobio, *On the local-global principle for isogenies of abelian surfaces*, 2022, arXiv:2206.15240.

[Mar05] Greg Martin, *Dimensions of the spaces of cusp forms and newforms on* $\Gamma_0(N)$ *and* $\Gamma_1(N)$, Journal of Number Theory **112** (2005), no. 2, 298–331.

[Mit14] Howard H. Mitchell, *The subgroups of the quaternary abelian linear group*, Trans. Amer. Math. Soc. **15** (1914), no. 4, 379–396. MR 1500986

[MM97] M. Ram Murty and V. Kumar Murty, *Non-vanishing of L-functions and applications*, Modern Birkhäuser Classics, Birkhäuser/Springer Basel AG, Basel, 1997, [2011 reprint of the 1997 original] [MR1482805]. MR 3025442

[MT74] Barry Mazur and John Tate, *Points of order* 13 *on elliptic curves*, Invent. Math. **22** (1973/74), 41–49. MR 347826

[MW21] Jacob Mayle and Tian Wang, *On the effective version of Serre's open image theorem*, 2021, arXiv:2109.08656.

[Poo17] Bjorn Poonen, *Rational points on varieties*, Graduate Studies in Mathematics, vol. 186, American Mathematical Society, Providence, RI, 2017. MR 3729254

[Ray74] Michel Raynaud, *Schémas en groupes de type* $(p, \dots, p)$, Bull. Soc. Math. France **102** (1974), 241–280. MR 419467

[Ser72] Jean-Pierre Serre, *Propriétés Galoisienne des points d'ordre fini des courbes elliptiques*, Inventiones Mathematicae **15** (1972), 259–331.

[Ser81] Jean-Pierre Serre, *Quelques applications du théorème de densité de Chebotarev*, Publications Mathématiques de l'IHÉS **54** (1981), 123–201 (fr). MR 83k:12011

[Ser87] ———, *Sur les représentations modulaires de degré* 2 *de* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, Duke Math. J. **54** (1987), no. 1, 179–230.

[Ser00] ———, *Lettre à Marie-France Vignéras du 10/2/1986*, Oeuvres - Collected Papers IV, Springer-Verlag Berlin Heidelberg, 2000.

[Shi82] Ken-ichi Shinoda, *The characters of the finite conformal symplectic group,* $\mathrm{CSp}(4, q)$, Comm. Algebra **10** (1982), no. 13, 1369–1419. MR 662708

[ST68] Jean-Pierre Serre and John Tate, *Good reduction of abelian varieties*, Ann. of Math. (2) **88** (1968), 492–517. MR 236190

[The20] The Sage Developers, *Sagemath, the Sage Mathematics Software System (Version 9.2)*, 2020, https://www.sagemath.org.

[vBCCK22] Raymond van Bommel, Shiva Chidambaram, Edgar Costa, and Jean Kieffer, *Computing isogeny classes of typical principally polarized abelian surfaces over the rationals*, In preparation, 2022.

[Zyw22] David Zywina, *On the surjectivity of* $\bmod \ell$ *representations associated to elliptic curves*, Bull. Lond. Math. Soc. **54** (2022), no. 6, 2404–2417. MR 4549128

Appendix A. Exceptional maximal subgroups of $\mathrm{GSp}_4(\mathbb{F}_\ell)$

ℓ	type	choices	generators
$\ell \equiv 5 \bmod 8$	G_{1920}	$b^2 = -1$ in $\mathbb{F}_\ell$	$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 & b \\ 0 & 1 & b & 0 \\ 0 & b & 1 & 0 \\ b & 0 & 0 & 1 \end{pmatrix},$ $\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$
$\ell \equiv 3 \bmod 8$	G_{1920}	$b^2 = -2$ in $\mathbb{F}_\ell$	$\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & b \\ 0 & 0 & b & 0 \\ 0 & b & 2 & 0 \\ b & 0 & 0 & 2 \end{pmatrix},$ $\begin{pmatrix} 1 & 0 & 0 & -1 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 1 & 0 \\ 1 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ -1 & 0 & 1 & 0 \\ 0 & -1 & 0 & 1 \end{pmatrix}$
$\ell \equiv 7 \bmod 12$	G_{720}	$a^2 + a + 1 = 0$ in $\mathbb{F}_\ell$	$\begin{pmatrix} a & 0 & 0 & 0 \\ 0 & a & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} a & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & a & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$ $\begin{pmatrix} a & 0 & -a-1 & a+1 \\ 0 & a & -a-1 & -a-1 \\ -a-1 & -a-1 & -1 & 0 \\ a+1 & -a-1 & 0 & -1 \end{pmatrix}, \begin{pmatrix} 0 & -1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$
$\ell \equiv 5 \bmod 12$	G_{720}	$b^2 = -1$ in $\mathbb{F}_\ell$	$\begin{pmatrix} -1 & 0 & 0 & -1 \\ 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & -1 & -1 & 0 \\ 0 & 1 & 0 & 0 \\ -1 & 0 & 0 & -1 \end{pmatrix},$ $\begin{pmatrix} -b-1 & b & 2b & -2b+1 \\ b & b-1 & 2b+1 & 2b \\ b & b-1 & -b-2 & -b \\ -b-1 & b & -b & b-2 \end{pmatrix}, \begin{pmatrix} 0 & -b & -2b & 0 \\ b & 0 & 0 & 2b \\ -2b & 0 & 0 & -b \\ 0 & 2b & b & 0 \end{pmatrix}$
$\ell = 7$	G_{5040}	$a = 2$ satisfies $a^2 + a + 1 = 0$	$\begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$ $\begin{pmatrix} 6 & 0 & 5 & 2 \\ 0 & 6 & 5 & 5 \\ 5 & 5 & 4 & 0 \\ 2 & 5 & 0 & 4 \end{pmatrix}, \begin{pmatrix} 0 & 6 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 6 \\ 0 & 0 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 4 & 6 & 0 & 0 \\ 6 & 6 & 0 & 0 \\ 0 & 0 & 4 & 1 \\ 0 & 0 & 1 & 6 \end{pmatrix}$

Table 7. Explicit generators for each exceptional maximal subgroup in $\mathrm{GSp}_4(\mathbb{F}_\ell)$ (up to conjugacy). The matrices described in Table 7 depend on an auxiliary choice of a parameter denoted either a and b in each case. In each row, any one choice of the corresponding a and b satisfying the equations described in the table suffices.

Barinder S. Banwait, Department of Mathematics & Statistics, Boston University, Boston, MA
Email address: barinder@bu.edu
URL: https://barinderbanwait.github.io/

Armand Brumer, Department of Mathematics, Fordham University, New York, NY
Email address: brumer@fordham.edu

Hyun Jong Kim, Department of Mathematics, University of Wisconsin-Madison, Madison, WI
Email address: hyunjong.kim@math.wisc.edu
URL: https://sites.google.com/wisc.edu/hyunjongkim

Zev Klagsbrun, Center for Communications Research, San Diego, CA
Email address: zdklags@ccr-lajolla.org

Jacob Mayle, Department of Mathematics, Wake Forest University, Winston-Salem, NC
Email address: maylej@wfu.edu

Padmavathi Srinivasan, ICERM, Providence, RI
Email address: padmavathi_srinivasan@brown.edu
URL: https://padmask.github.io/

Isabel Vogt, Department of Mathematics, Brown University, Providence, RI
Email address: ivogt.math@gmail.com
URL: https://www.math.brown.edu/ivogt/