Black Box Galois Representations.

Alejandro Argáez-García John Cremona

October 6, 2017

Abstract

We develop methods to study 2-dimensional 2-adic Galois representations ρ of the absolute Galois group of a number field K, unramified outside a known finite set of primes S of K, which are presented as *Black Box* representations, where we only have access to the characteristic polynomials of Frobenius automorphisms at a finite set of primes. Using suitable finite test sets of primes, depending only on K and S, we show how to determine the determinant $\det \rho$, whether or not ρ is residually reducible, and further information about the size of the *isogeny graph* of ρ whose vertices are homothety classes of stable lattices. The methods are illustrated with examples for $K = \mathbb{Q}$, and for K imaginary quadratic, ρ being the representation attached to a Bianchi modular form.

These results form part of the first author's thesis [1].

1 Introduction

Let K be a number field. Denote by $\overline{K}$ the algebraic closure K and by $G_K = \mathrm{Gal}(\overline{K}/K)$ the absolute Galois group of K. By an *ℓ-adic Galois representation* of K we mean a continuous representation $\rho\colon G_K \to \mathrm{Aut}(V)$, where V is a finite-dimensional vector space over $\mathbb{Q}_\ell$, which is unramified outside a finite set of primes of K. Such representations arise throughout arithmetic geometry, where typically V is a cohomology space attached to an algebraic variety. For example, modularity of elliptic curves over K can be interpreted as a statement that the 2-dimensional Galois representation arising from the action of G_K on the ℓ-adic Tate module of the elliptic curve is equivalent, as a representation, to a representation attached to a suitable automorphic form over K. In this 2-dimensional context and with $\ell = 2$, techniques have been developed by Serre [12], Faltings, Livné [10] and others to establish such an equivalence using only the characteristic polynomial of $\rho(\sigma)$ for a *finite* number of elements $\sigma \in G_K$. Here the ramified set of primes S is known in advance and the Galois automorphisms σ which are used in the Serre-Faltings-Livné method have the form $\sigma = \mathrm{Frob}\,\mathfrak{p}$ where $\mathfrak{p}$ is a prime not in S, so that ρ is unramified at $\mathfrak{p}$.

Motivated by such applications, in this paper we study Galois representations of K as "Black Boxes" where both the base field K and the finite ramified set S are specified in advance, and the only information we have about ρ is the characteristic polynomial of $\rho(\mathrm{Frob}\,\mathfrak{p})$ for certain primes $\mathfrak{p}$ not in S; we may specify these primes, but only finitely many of them. Using such a Black Box as an oracle, we seek to give algorithmic answers to questions such as the following (see the following section for definitions):

- Is ρ irreducible? Is ρ trivial, or does it have trivial semisimplification?
- What is the determinant character of ρ?
- What is the residual representation $\overline{\rho}$? Is it irreducible, trivial, or with trivial semisimplification?
- How many lattices in V (up to homothety) are stable under ρ – in other words, how large is the isogeny class of ρ?

In the case where $\dim V = 2$ and $\ell = 2$, we give substantial answers to these questions in the following sections. In Section 2 we recall basic facts about Galois representations and introduce key ideas and definitions, for arbitrary finite dimension and arbitrary prime ℓ. From Section 3 on, we restrict to $\ell = 2$, first considering the case of one-dimensional representations (characters); these are relevant in any dimension since $\det\rho$ is a character. Although in the applications $\det\rho$ is always a power of the ℓ-adic cyclotomic character of G_K, we will not assume this, and in fact the methods of Section 3 may be used to prove that the determinant of a Black Box Galois representation has this form. From Section 4 we restrict to 2-dimensional 2-adic representations, starting with the question of whether the residual representation $\overline{\rho}$ is or is not irreducible, and what is its splitting field (see Section 2 for definitions); a complete solution is given for both these questions, which we can express as answering the question of whether or not the isogeny class of ρ consists of only one element. In Section 5 we consider further the residually reducible case and determine whether or not the isogeny class of ρ contains a representative with trivial residual representation, or equivalently whether the size of the class is 2 or greater. In Section 6 we assume that ρ is trivial modulo 2^k for some $k \geq 1$ and determine the reduction of $\rho \pmod{2^{k+1}}$ completely, in particular whether it too is trivial. Hence, for example, we can determine $\rho \pmod 4$ when $\overline{\rho}$ is trivial, and also as a final application, in Section 7 we give a (finite) criterion for whether ρ has trivial semisimplification.

For each of these tasks we will define a finite set T of primes of K, disjoint from S, such that the Black Box information about $\rho(\mathrm{Frob}\,\mathfrak{p})$ for $\mathfrak{p} \in T$ is sufficient to answer the question under consideration. In each case except for the criterion for ρ to have trivial semisimplification, only finite 2-adic precision is needed about the determinant and trace of $\rho(\mathrm{Frob}\,\mathfrak{p})$, though we note that in the applications the 2-adic representation inside the Black Box is always part of a compatible family of ℓ-adic representations, so that in practice these are rational or algebraic integers and will be known exactly.

The following theorem summarises our results; we refer to later sections for the definitions of the sets T_0, T_1 and T_2 and for algorithms to compute them. Here $F_{\mathfrak{p}}(t)$ denotes the characteristic polynomial of $\rho(\mathrm{Frob}\,\mathfrak{p})$ for a prime $\mathfrak{p} \notin S$.

Theorem 1.1. *Let K be a number field and S a finite set of primes of K. There exist finite sets of primes T_0, T_1 and T_2, disjoint from S, depending only on K and S, such that for any 2-dimensional 2-adic Galois representation ρ of G_K which is continuous and unramified outside S,*

1. *the reducibility of the residual representation $\overline{\rho}$, and its splitting field when irreducible, are uniquely determined by the values of $F_{\mathfrak{p}}(1) \pmod 2$, i.e., by the traces of $\overline{\rho}(\operatorname{Frob}\mathfrak{p})$, for $\mathfrak{p} \in T_0$;*
2. *the determinant character $\det\rho$ is uniquely determined by the values of $F_{\mathfrak{p}}(0) = \det\rho(\operatorname{Frob}\mathfrak{p})$ for $\mathfrak{p} \in T_1$;*
3. *when $\overline{\rho}$ is reducible,*
   - *the existence of an equivalent representation whose residual representation is trivial is determined by the values of $F_{\mathfrak{p}}(1) \pmod 4$ for $\mathfrak{p} \in T_2$;*
   - *if $\rho \pmod{2^k}$ is trivial for some $k \geq 1$, the reduction $\rho \pmod{2^{k+1}}$ is uniquely determined by the values of $F_{\mathfrak{p}}(1) \pmod{2^{2k+1}}$ for $\mathfrak{p} \in T_2$; in particular, there is an equivalent representation which is trivial modulo 2^{k+1} if and only if $F_{\mathfrak{p}}(0) \equiv 1 \pmod{2^{k+1}}$ and $F_{\mathfrak{p}}(1) \equiv 0 \pmod{2^{2k+2}}$ for all $\mathfrak{p} \in T_2$;*
   - *ρ has trivial semisimplification if and only if $F_{\mathfrak{p}}(t) = (t-1)^2$ for all $\mathfrak{p} \in T_2$; that is if and only if $\operatorname{tr}\rho(\operatorname{Frob}\mathfrak{p}) = 2$ and $\det\rho(\operatorname{Frob}\mathfrak{p}) = 1$ for all $\mathfrak{p} \in T_2$.*

In each section we give examples to illustrate the methods, first from elliptic curves defined over $\mathbb{Q}$, and then in the final section, we give two examples arising from Bianchi modular forms, and elliptic curves over imaginary quadratic fields. In the examples we refer to elliptic curves and Bianchi modular forms using their LMFDB labels (see [11]) giving links to the relevant objects' home pages at `www.lmfdb.org`. We have implemented all the algorithms described in the paper in `Sage` (see [6]).

2 Background on Galois representations

Fix once and for all a number field K and a finite set S of primes of K.

Definition 2.1. An ℓ-adic Galois representation over K is a continuous homomorphism $\rho\colon G_K \to \operatorname{Aut}(V) \cong \mathrm{GL}_2(\mathbb{Q}_\ell)$, where V is a finite-dimensional vector space over $\mathbb{Q}_\ell$. Such a representation is said to be *unramified outside* S, if its restriction to the inertia subgroup at each $\mathfrak{p} \notin S$ is trivial.

We do not assume that the representation ρ is irreducible.

The condition that ρ is unramified outside S means that for each $\mathfrak{p} \notin S$, it factors through the Galois group $\operatorname{Gal}(L/K)$ of the maximal extension L of K

unramified at $\mathfrak{p}$. Since L/K is unramified at $\mathfrak{p}$, there is a well-defined conjugacy class of Frobenius automorphisms at $\mathfrak{p}$, denoted $\operatorname{Frob}\mathfrak{p}$, in $\operatorname{Gal}(L/K)$, and hence the conjugacy class of $\rho(\operatorname{Frob}\mathfrak{p})$ and the characteristic polynomial $F_{\mathfrak{p}}(t)$ of $\rho(\operatorname{Frob}\mathfrak{p})$ are also well-defined. By abuse of notation, therefore, we may refer to $\operatorname{Frob}\mathfrak{p}$ as if it were an element of G_K, noting that by the Čebotarev Density Theorem, every automorphism $\sigma \in G_K$ has this form in the sense that for infinitely many $\mathfrak{p} \notin S$, there is a Galois extension L/K unramified at $\mathfrak{p}$ such that the restriction of σ to $\operatorname{Gal}(L/K)$ lies in the Frobenius class $\operatorname{Frob}\mathfrak{p} \in \operatorname{Gal}(L/K)$. In this situation we simply write $\sigma = \operatorname{Frob}\mathfrak{p}$, noting that the conjugacy class of $\rho(\sigma) = \rho(\operatorname{Frob}\mathfrak{p})$ in $\operatorname{Aut}(V)$ is independent of the choices made.

From now on we only consider 2-dimensional representations. Choosing a basis for V we may express each $\rho(\sigma)$ as a matrix, and hence consider ρ to be a matrix representation $G_K \to \mathrm{GL}_2(\mathbb{Q}_\ell)$. Moreover with different choices of bases we obtain equivalent matrix representations. For $\sigma \in G_K$ define $F_\sigma(t)$ to be the characteristic polynomial of $\rho(\sigma)$, which is a well-defined monic quadratic polynomial in $\mathbb{Z}_\ell[t]$, and for each prime $\mathfrak{p} \notin S$ we set $F_{\mathfrak{p}} = F_{\operatorname{Frob}\mathfrak{p}}$, the *Frobenius polynomial* at $\mathfrak{p}$, which is also well-defined:

$$\begin{aligned} F_{\mathfrak{p}}(t) &= \det(\rho(\operatorname{Frob}\mathfrak{p}) - t\,\mathbf{I}) \\ &= t^2 - \operatorname{tr}(\rho(\operatorname{Frob}\mathfrak{p}))t + \det(\rho(\operatorname{Frob}\mathfrak{p})) \in \mathbb{Z}_\ell[t]. \end{aligned} \tag{1}$$

The fact that these polynomials have integral coefficients follows from the existence of a stable lattice in V, as we recall below. The information about the representation ρ that we assume will be provided consists of the set S and the values of $\det(\rho(\sigma))$ and $\operatorname{tr}(\rho(\sigma))$ for $\sigma = \operatorname{Frob}\mathfrak{p} \in G_K$ and $\mathfrak{p} \notin S$. We encapsulate this setup as an oracle, or *Black Box*:

Definition 2.2. An ℓ-adic *Black Box Galois representation* over K with respect to S is an oracle which, on being presented with a prime $\mathfrak{p}$ of K, responds with either "ramified" if $\mathfrak{p} \in S$, or with the value of the quadratic Frobenius polynomial $F_{\mathfrak{p}}(t)$ in $\mathbb{Z}_\ell[t]$ for $\mathfrak{p} \notin S$.

Equivalently, the Black Box delivers for each $\mathfrak{p} \notin S$ the values of the *trace* $\operatorname{tr}(\rho(\operatorname{Frob}\mathfrak{p})) \in \mathbb{Z}_\ell$ and the *determinant* $\det(\rho(\operatorname{Frob}\mathfrak{p})) \in \mathbb{Z}_\ell^*$.

2.1 Stable lattices and the Bruhat-Tits tree

It is well known [13, p.1] that continuity of ρ implies the existence of at least one *stable lattice* Λ, i.e., a free $\mathbb{Z}_\ell$-submodule of V such that $\rho(\sigma)(\Lambda) \subseteq \Lambda$ for all $\sigma \in G_K$. With respect to a $\mathbb{Z}_\ell$-basis of Λ, ρ determines an *integral matrix representation* $\rho_\Lambda \colon G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$. Any lattice homothetic to a stable lattice is also stable and induces the same integral matrix representation. Changing to a different $\mathbb{Z}_\ell$-basis of Λ gives rise to an equivalent integral representation (conjugate within $\mathrm{GL}_2(\mathbb{Z}_\ell)$). The existence of a stable lattice shows that the Frobenius polynomials $F_{\mathfrak{p}}(t)$ have coefficients in $\mathbb{Z}_\ell$.

If we change to a different stable lattice $\Lambda' \subset V$ which is not homothetic to Λ, however, the integral representation $\rho_{\Lambda'}$ we obtain, while rationally equivalent to ρ_Λ (conjugate within $\mathrm{GL}_2(\mathbb{Q}_\ell)$), is not necessarily integrally equivalent, over $\mathbb{Z}_\ell$. Integral representations related in this way are called *isogenous*. As we are assuming that the only information we have about ρ (for fixed K and S) are the characteristic polynomials of $\rho(\operatorname{Frob}\mathfrak{p})$ for primes outside S provided by the Black Box, we cannot distinguish isogenous integral representations, but still hope to be able to say something about the set of all of those isogenous to a given one.

Definition 2.3. The *isogeny class* of ρ is the set of pairs (Λ, ρ_Λ) where Λ is a stable lattice and ρ_Λ the induced map $G_K \to \operatorname{Aut}(\Lambda)$, modulo the equivalence relation which identifies homothetic lattices.

For each choice of stable lattice and induced integral representation we can define its associated residual representation.

Definition 2.4. Let $\rho\colon G_K \to \operatorname{Aut}(V)$ be an ℓ-adic Galois representation. To each stable lattice $\Lambda \subset V$ the associated *residual representation* $\overline{\rho_\Lambda}$ is the composite map $G_K \to \operatorname{Aut}(\Lambda) \to \operatorname{Aut}(\Lambda \otimes_{\mathbb{Z}_\ell} \mathbb{F}_\ell)$.

In matrix terms, $\overline{\rho}_\Lambda\colon G_K \to \mathrm{GL}_2(\mathbb{F}_\ell)$ is obtained by composing the integral matrix representation $\rho_\Lambda\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_\ell)$ with reduction modulo ℓ.

We cite the following facts (see [13, p.3] for the second one):

- ρ is irreducible if and only if the number of stable lattice, up to homothety, is finite; that is, if and only if the isogeny class of ρ is finite.
- Let Λ be any stable lattice. Then the residual representation $\overline{\rho_\Lambda}$ is irreducible if and only if Λ is the only stable lattice up to homothety. In other words, the residual representation is irreducible if and only if the isogeny class consists of a single element, in which case there is of course only one residual representation up to conjugacy in $\mathrm{GL}_2(\mathbb{F}_\ell)$.

From the second fact we see that either all the residual representations are reducible, or none of them are; in the latter case there is only one stable lattice up to homothety anyway. Thus it makes sense to describe ρ as “residually reducible” or “residually irreducible” respectively.

Recall that the ℓ-adic Bruhat-Tits tree is the infinite graph whose vertices are the homothety classes of lattices in $V \cong \mathbb{Q}_\ell^2$, with two vertices joined by an edge if their classes have representative lattices Λ_1, Λ_2 such that Λ_1 contains Λ_2 with index ℓ. (This is a symmetric relation since then Λ_2 contains $\ell\Lambda_1$ with index ℓ.) Each vertex has degree exactly $\ell + 1$. Restricting to lattices which are stable under our representation ρ, we obtain the following:

Definition 2.5. The *stable Bruhat-Tits tree* or *isogeny graph* of an ℓ-adic representation ρ is the full subgraph $\mathrm{BT}(\rho)$ of the Bruhat-Tits tree whose vertices are stable lattices.

It is easy to see that if $[\Lambda]$ and $[\Lambda']$ are stable homothety classes, all vertices in the unique path between them are also stable, and hence the stable Bruhat-Tits tree is indeed a tree. Its vertex set is the isogeny class of ρ as defined above, and we may refer to its edges as *ℓ-isogenies*. Given two adjacent stable lattices, then we may choose bases so that the associated integral matrix representations are conjugate within $\mathrm{GL}_2(\mathbb{Q}_\ell)$ via the matrix $\begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix}$. In $\mathrm{BT}(\rho)$ it is no longer the case that every vertex has degree $\ell+1$; considering the action of $\mathrm{GL}_2(\mathbb{F}_\ell)$ on $\mathbb{P}^1(\mathbb{F}_\ell)$ we see that for $\ell = 2$ the possible degrees are 0, 1 and 3 while for $\ell \geq 3$ the possible degrees are 0, 1, 2 or $\ell + 1$.

We define the *width* of the isogeny class $\mathrm{BT}(\rho)$ to be the length of the longest path in $\mathrm{BT}(\rho)$; by the facts above, this is finite if and only if ρ is irreducible, and is positive if and only if ρ is residually reducible.

3 Characters and quadratic extensions

The problem of distinguishing continuous 2-adic characters (1-dimensional representations) $\chi\colon G_K \to \mathbb{Z}_2^*$ reduces to that of distinguishing quadratic extensions of K, since $\mathbb{Z}_2^*$ is an abelian pro-2-group. Moreover, $\mathrm{GL}_2(\mathbb{Z}_2)$ is itself a pro-2-group in the case that the residual representation is reducible, so the technique we describe in this section will be used later to study both $\det \rho$ and ρ itself in the residually reducible case.

There are only finitely many quadratic extensions L of K unramified outside S, whose compositum is the maximal extension of K unramified outside S and with Galois group an elementary abelian 2-group. Each has the form $L = K(\sqrt{\Delta})$ for $\Delta \in K(S,2) \leq K^*/(K^*)^2$ where $K(S,2)$ is given by

$$K(S,2) = \{a \in K^*/(K^*)^2 : \mathrm{ord}_{\mathfrak{p}}(a) \equiv 0 \pmod 2 \text{ for all } \mathfrak{p} \notin S\}. \tag{2}$$

Moreover when S contains all primes of K dividing 2, every extension $K(\sqrt{\Delta})$ with $\Delta \in K(S,2)$ is unramified outside S. In general the Δ such that $K(\sqrt{\Delta})$ is unramified outside S forms a subgroup $K(S,2)_u$ of $K(S,2)$. We will call elements of $K(S,2)_u$ *discriminants*, and always regard two discriminants as equal when their quotient is a square in K^*. It is also convenient here to consider $\Delta = 1$ as a discriminant, corresponding to the trivial extension $L = K$.

The group of discriminants $K(S,2)_u$ is an elementary abelian 2-group, of cardinality 2^r with $r \geq 1$, and may also be viewed as an r-dimensional vector space over $\mathbb{F}_2$. Fixing a basis $\{\Delta_i\}_{i=1}^r$ for $K(S,2)_u$, we may identify

$$\begin{aligned} \mathbb{F}_2^r &\leftrightarrow K(S,2)_u \\ \mathbf{x} &\leftrightarrow \prod_{i=1}^r \Delta_i^{x_i}, \end{aligned} \tag{3}$$

where $\mathbf{x} = (x_i)_{i=1}^r$.

Each prime $\mathfrak{p} \notin S$ determines a linear map

$$\alpha_{\mathfrak{p}}\colon K(S,2)_u \to \mathbb{F}_2$$

defined by $\alpha_{\mathfrak{p}}(\Delta) = [\Delta \mid \mathfrak{p}]$, where we set

$$[\Delta \mid \mathfrak{p}] = \begin{cases} 0 \pmod 2 & \text{if } \mathfrak{p} \text{ splits in } K(\sqrt{\Delta}) \text{ or } \Delta = 1 \\ 1 \pmod 2 & \text{if } \mathfrak{p} \text{ is inert in } K(\sqrt{\Delta}). \end{cases}$$

Linearity follows from the relation $[\Delta\Delta'|\mathfrak{p}] = [\Delta|\mathfrak{p}] + [\Delta'|\mathfrak{p}]$.

For any prime $\mathfrak{p}$ not in S, we define

$$I(\mathfrak{p}) = \{i : [\Delta_i \mid \mathfrak{p}] = 1\} \subseteq \{1, 2, \ldots, r\}. \tag{4}$$

Conversely, for each subset $I \subseteq \{1, ..., r\}$, we denote by $\mathfrak{p}_I$ any prime such that $I(\mathfrak{p}_I) = I$, so that

$$[\Delta_i \mid \mathfrak{p}_I] = 1 \Leftrightarrow i \in I. \tag{5}$$

When $I = \{i\}$ or $I = \{i, j\}$ with $i \neq j$, we simply write $\mathfrak{p}_i = \mathfrak{p}_{\{i\}}$ and $\mathfrak{p}_{ij} = \mathfrak{p}_{\{i,j\}}$. By the Čebotarev Density Theorem applied to the compositum of the extensions $K(\sqrt{\Delta})$ for $\Delta \in K(S, 2)_u$, the set of primes of the form $\mathfrak{p}_I$ has density $1/2^r$ for each subset I, and in particular is infinite.

Each set of primes of the form $\{\mathfrak{p}_i \mid 1 \leq i \leq r\}$ determines a basis $\{\alpha_{\mathfrak{p}_i} \mid 1 \leq i \leq r\}$ for the dual space $K(S, 2)_u^* = \mathrm{Hom}_{\mathbb{F}_2}(K(S, 2)_u, \mathbb{F}_2)$, and may be used to distinguish between two characters unramified outside S. More generally we make the following definition.

Definition 3.1. A set T_1 of primes of K is *linearly independent with respect to* S if T_1 is disjoint from S and the linear functions $\{\alpha_{\mathfrak{p}} \mid \mathfrak{p} \in T_1\}$ form a basis for the dual space $K(S, 2)_u^*$.

As observed above, such a set always exists, for example any set of the form

$$\{\mathfrak{p}_1, ..., \mathfrak{p}_r\}, \tag{6}$$

defined above with respect to a basis of $K(S, 2)_u$, is a linearly independent set of primes. We fix once and for all a linearly independent set of primes, and denote it by T_1, and can assume that $\{\alpha_{\mathfrak{p}} \mid \mathfrak{p} \in T_1\}$ is a dual basis for the chosen basis $\{\Delta_i \mid 1 \leq i \leq r\}$ for $K(S, 2)_u$. In practice this is most easily done by computing $T_1 = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_r\}$ first (see Algorithm 1 below), and then taking $\{\Delta_i\}$ to be the basis dual to $\{\alpha_{\mathfrak{p}_i}\}$. We then see by (5) that for all $I \subseteq \{1, 2, \ldots, r\}$,

$$\alpha_{\mathfrak{p}_I}(\Delta) = \sum_{i \in I} \alpha_{\mathfrak{p}_i}(\Delta). \tag{7}$$

Algorithm 1: To determine a linearly independent set T_1 of primes of K.

```
   Input : A number field $K$.
           A finite set $S$ of primes of $K$.
   Output: $T_1$, a set of primes of $K$ linearly independent with respect to $S$.
1  Let $\{\Delta_i\}_{i=1}^{r}$ be a basis for $K(S,2)_u$;
2  Let $T_1 = \{\}$;
3  Let $A$ be a $0 \times r$ matrix over $\mathbb{F}_2$;
4  while rank$(A) < r$ do
5      Let $\mathfrak{p}$ be a prime not in $S \cup T_1$;
6      Let $\mathbf{v} = ([\Delta_1|\mathfrak{p}], ..., [\Delta_r|\mathfrak{p}])$;
7      if $\mathbf{v}$ is not in the row-space of $A$ then
8          Let $A = A + \mathbf{v}$;      # i.e., adjoin $\mathbf{v}$ as a new row of $A$
9          Let $T_1 = T_1 \cup \{\mathfrak{p}\}$.
10 return $T_1$.
```

In line 5 of the algorithm, and similarly with later algorithms to determine other special sets of primes, we systematically consider all primes of K in turn, for example in order of norm, omitting those in S.

Remark 3.2. Finding $K(S,2)$ is implemented in standard software packages. In `Sage`, `K.selmergroup(S,2)` returns a basis, while in MAGMA one obtains $K(S,2)$ as abelian group via `pSelmerGroup(2,S)`. See [6] or [3] respectively.

3.1 Identifying quadratic extensions

As an easy example of how to use a set T_1 of primes linearly independent with respect to S, we may identify any extension L/K known to be of degree at most 2 and unramified outside S. Enumerating $T_1 = \{\mathfrak{p}_1, \dots, \mathfrak{p}_r\}$ and the dual basis $\{\Delta_1, \dots, \Delta_r\}$ for $K(S,2)_u$, set

$$\Delta = \prod_{i=1}^{r} \Delta_i^{[L|\mathfrak{p}_i]},$$

where for $\mathfrak{p} \notin S$ we set $[L|\mathfrak{p}] = 0$ (respectively 1) if $\mathfrak{p}$ is split (respectively, is inert) in L. Then $L = K(\sqrt{\Delta})$ (or $L = K$ if $\Delta = 1$). The proof is clear from the fact that L is uniquely determined by the set of primes which split in L/K. In particular, $L = K$ if and only if all primes in T_1 split.

3.2 1-dimensional Galois representations

We first consider additive quadratic characters $\alpha\colon G_K \to \mathbb{F}_2$ which are unramified outside S, and see that a linear independent set T_1 can determine whether such a character is trivial, and more generally when two are equal.

Lemma 3.3. *Let $\alpha, \alpha_1, \alpha_2\colon G_K \to \mathbb{F}_2$ be additive quadratic characters unramified outside S.*

1. *If $\alpha(\operatorname{Frob}\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_1$, then $\alpha = 0$.*

2. *$\alpha_1 = \alpha_2$ if and only if $\alpha_1(\mathrm{Frob}\,\mathfrak{p}) = \alpha_2(\mathrm{Frob}\,\mathfrak{p})$ for all $\mathfrak{p} \in T_1$.*

Proof. If $\alpha \neq 0$, then the fixed field of $\ker(\alpha)$ is a quadratic extension $K(\sqrt{\Delta})$ for some non-trivial Δ in $K(S,2)$. But $[\Delta|\mathfrak{p}] = \alpha(\mathrm{Frob}\,\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_1$, which implies that $\Delta = 1$. For the second part, consider $\alpha = \alpha_1 - \alpha_2$. □

Now let $\chi\colon G_K \to \mathbb{Z}_2^*$ be a 2-adic character unramified outside S. For example we may take $\chi = \det\rho$ where ρ is a 2-adic Galois representation unramified outside S. Again, to show triviality of χ, or equality of two such characters, it is enough to consider their values on $\mathrm{Frob}\,\mathfrak{p}$ for $\mathfrak{p} \in T_1$.

Theorem 3.4. *Let $\chi, \chi_1, \chi_2\colon G_K \to \mathbb{Z}_2^*$ be continuous characters unramified outside S. Let T_1 be a linearly independent set of primes with respect to S.*

1. *If $\chi(\mathrm{Frob}\,\mathfrak{p}) = 1$ for all $\mathfrak{p} \in T_1$, then χ is trivial.*

2. *$\chi_1 = \chi_2$ if and only if $\chi_1(\mathrm{Frob}\,\mathfrak{p}) = \chi_2(\mathrm{Frob}\,\mathfrak{p})$ for all $\mathfrak{p} \in T_1$.*

Proof. As before, the second part follows from the first on considering $\chi = \chi_1\chi_2^{-1}$, which is again a character $G_K \to \mathbb{Z}_2^*$ unramified outside S.

Suppose that $\chi \neq 1$. Let $k \geq 1$ be the greatest integer such that $\chi(\sigma) \equiv 1 \pmod{2^k}$ for all $\sigma \in G_K$. Note that $\chi(\sigma) \equiv 1 \pmod 2$ for all $\sigma \in G_K$, so k does exist. We can write

$$\chi(\sigma) \equiv 1 + 2^k\alpha(\sigma) \pmod{2^{k+1}}$$

where $\sigma \mapsto \alpha(\sigma)$ is a non-trivial additive quadratic character $G_K \to \mathbb{F}_2$. However, $\alpha(\mathrm{Frob}\,\mathfrak{p}) \equiv 0 \pmod 2$ for all $\mathfrak{p} \in T_1$, since $\chi(\mathrm{Frob}\,\mathfrak{p}) = 1$, so by Lemma 3.3 we have that $\alpha = 0$, contradicting the minimality of k. □

4 Determining the residual representation

Given a Black Box Galois representation ρ, we would like to determine whether its residual representations are irreducible or reducible. Recall that this is a well-defined question, even when there is more than one stable lattice. In the irreducible case, we will moreover determine the (unique) residual representation completely, both its image (which has order 3 or 6, and is isomorphic to either C_3 (the cyclic group of order 3) or S_3 (the symmetric group of degree 3), and the fixed field of its kernel. Note that $\mathrm{GL}_2(\mathbb{F}_2) \cong S_3$, the isomorphism coming from the action of $\mathrm{GL}_2(\mathbb{F}_2)$ on $\mathbb{P}^1(\mathbb{F}_2)$.

This is our initial step in determining the size and structure of the attached Bruhat-Tits tree $\mathrm{BT}(\rho)$, as we will determine whether it has only one vertex (and width 0) or is larger (positive width).

Fixing one stable lattice Λ and residual representation $\overline{\rho}_\Lambda$, we define the *splitting field* of $\overline{\rho}_\Lambda$ to be the fixed field of its kernel. This is an extension L of K which is unramified outside S such that $\mathrm{Gal}(L/K) \cong \overline{\rho}_\Lambda(G_K) \leq \mathrm{GL}_2(\mathbb{F}_2)$, hence $\mathrm{Gal}(L/K)$ is isomorphic to one of: C_1 (the trivial group), C_2 (cyclic of order 2), C_3 or S_3. The first two cases occur when $\overline{\rho}_\Lambda$ is reducible, in which case a different choice of stable lattice may change the image between being trivial and of order 2, while in the residually irreducible case the image and kernel are both well-defined.

We now show how to identify the residual splitting field, leaving until a later section the task of saying more in the reducible case.

4.1 Identifying cubic extensions

The key to our method is that there are only finitely many Galois extensions L/K, unramified outside S, and with Galois group either C_3 or S_3, and we may determine these algorithmically. We will not discuss here details of this, except to remark that in the S_3 case we can first construct all possible quadratic extensions $K(\sqrt{\Delta})$ using $\Delta \in K(S,2)_u$ as in the previous section, and then use either Kummer Theory or Class Field Theory to construct all cyclic cubic extensions of K or $K(\sqrt{\Delta})$. Full details of the Kummer Theory method, using special cases of results by Cohen [4], can be found in the thesis [9] of Koutsianas; we have an implementation of this method in `Sage`. An alternate implementation, using Class Field Theory, was written in `Pari/GP` by Pacetti, as used in [7] in the case where K is an imaginary quadratic field. These implementations were used for the examples below.

For present purposes, we assume that, given K and S, we can write down a finite set $\mathcal{F}$ of irreducible monic cubic polynomials in $\mathcal{O}_K[x]$, whose splitting fields are the Galois extensions L/K unramified outside S with $\mathrm{Gal}(L/K)$ isomorphic to either S_3 or C_3. Note that the discriminants of the polynomials in $\mathcal{F}$ may be divisible by primes not in S, and these primes will need to be avoided, so we denote by $S(\mathcal{F})$ the union of S with all prime divisors of $\{\mathrm{disc}(f) \mid f \in \mathcal{F}\}$.

We can characterize the fields L by examining the splitting behaviour of primes $\mathfrak{p} \notin S(\mathcal{F})$, which depends only on the factorization of the respective $f \in \mathcal{F}$ modulo $\mathfrak{p}$.

Definition 4.1. For a monic cubic polynomial $f \in \mathcal{O}_K[x]$ and prime $\mathfrak{p} \nmid \mathrm{disc}\, f$, define

$$\lambda(f,\mathfrak{p}) = \begin{cases} 1 & \text{if } f \text{ is irreducible mod } \mathfrak{p}; \\ 0 & \text{otherwise.} \end{cases}$$

Elementary algebraic number theory gives the following.

Lemma 4.2. *Let f be an irreducible monic cubic polynomial in $\mathcal{O}_K[x]$ with splitting field L. Then for $\mathfrak{p} \nmid \mathrm{disc}\, f$,*

$$\lambda(f,\mathfrak{p}) = \begin{cases} 1 & \textit{if } \mathrm{Frob}\,\mathfrak{p} \textit{ has order } 3 \textit{ in } \mathrm{Gal}(L/K) \\ 0 & \textit{if } \mathrm{Frob}\,\mathfrak{p} \textit{ has order } 1 \textit{ or } 2 \textit{ in } \mathrm{Gal}(L/K). \end{cases}$$

Note that elements of $\mathrm{GL}_2(\mathbb{F}_2)$ have trace 1 (respectively, 0) if their order is 3 (respectively, 1 or 2). We can now define a finite set of primes which can distinguish between the possible splitting fields L.

Definition 4.3. Let $\mathcal{F}$ be a set of monic cubic polynomials in $\mathcal{O}_K$ whose splitting fields are exactly the S_3 and C_3 extensions of K unramified outside S. An ordered set of primes $T_0 = \{\mathfrak{p}_1, ..., \mathfrak{p}_t\}$ of K is a *distinguishing set* for $(\mathcal{F}, S)$ if

(1) $T_0 \cap S(\mathcal{F}) = \emptyset$ (equivalently, $T_0 \cap S = \emptyset$ and $\mathfrak{p} \nmid \operatorname{disc} f$ for all $\mathfrak{p} \in T_0$ and $f \in \mathcal{F}$);

(2) the vectors $(\lambda(f, \mathfrak{p}_1), ..., \lambda(f, \mathfrak{p}_t)) \in \mathbb{F}_2^t$ for $f \in \mathcal{F}$ are distinct and non-zero.

We will write $\mathbf{v}(f, T_0) = (\lambda(f, \mathfrak{p}_1), ..., \lambda(f, \mathfrak{p}_t))$ when $T_0 = \{\mathfrak{p}_1, ..., \mathfrak{p}_t\}$.

Lemma 4.4. *A distinguishing set of primes for* $(\mathcal{F}, S)$ *exists.*

Proof. Let $\mathcal{F} = \{f_i\}_{i=1}^n$ be the set of monic cubic polynomials defining the S_3 and C_3 extensions of K. Set $f_0 = x^3$ and define $\lambda(f_0, \mathfrak{p}) = 0$ for all $\mathfrak{p}$. It is enough to show that for all $0 \leq j < i \leq n$ there exists a prime $\mathfrak{p} \notin S(\mathcal{F})$ such that $\lambda(f_i, \mathfrak{p}) \neq \lambda(f_j, \mathfrak{p})$. For $i \geq 1$ let L_i be the splitting field of f_i. We divide the proof into three cases.

Case 1. When $j = 0$, we require for each $i \geq 1$ the existence of a prime $\mathfrak{p}$ such that $\lambda(f_i, \mathfrak{p}) = 1$. By the Čebotarev Density Theorem, there are infinitely many such primes, with density $\frac{1}{3}$ when $\operatorname{Gal}(L_i/K) \cong S_3$, or $\frac{2}{3}$ when $\operatorname{Gal}(L_i/K) \cong C_3$.

Case 2. When $i > j \geq 1$ and $\operatorname{disc}(L_i) \not\equiv \operatorname{disc}(L_j) \pmod{(K^*)^2}$, the fields L_i and L_j are disjoint. Then there are three possibilities for the Galois group of their composition, according to whether the discriminants are trivial (*i.e.*, square). In each case there are infinitely many primes which fulfill the condition, with density $\frac{4}{9}$ when $\operatorname{Gal}(L_iL_j) \cong S_3 \times S_3$, and $\frac{5}{9}$ when $\operatorname{Gal}(L_iL_j)$ is $S_3 \times C_3$.

Case 3. When $i, j \geq 1$ and $\operatorname{disc}(L_i) \equiv \operatorname{disc}(L_j) \pmod{(K^*)^2}$ we have two possibilities; the density is $\frac{4}{9}$ when both Galois groups are isomorphic to C_3 and is $\frac{2}{9}$ when both are isomorphic to S_3.

□

A distinguishing set T_0 of primes can computed using the following algorithm. The size t of T_0 depends on the total number n of C_3 and S_3 extensions of K unramified outside S; it is not difficult to see that $\lceil \log_2(n) \rceil \leq t \leq n$.

Algorithm 2: To determine a distinguishing set T_0 of primes of K.

```
Input : A number field $K$. A finite set $S$ of primes of $K$.
        A set $\mathcal{F}$ of cubics defining extensions unramified outside $S$.
Output: $T_0$, a distinguishing set of primes for $(\mathcal{F}, S)$.
Let $f_0 = x^3$;
Let $T_0 = \{\}$;
while $\#\{\mathbf{v}(f_i, T_0) \mid 0 \le i \le n\} < n + 1$ do
    Find $i \ne j$ such that $\mathbf{v}(f_i, T_0) = \mathbf{v}(f_j, T_0)$;
    Find a prime $\mathfrak{p} \notin S \cup T_0$ such that $\lambda(f_i, \mathfrak{p}) \ne \lambda(f_j, \mathfrak{p})$;
    Let $T_0 = T_0 \cup \{\mathfrak{p}\}$;
return $T_0$.
```

Example 1. Let $K = \mathbb{Q}$ and take $S = \{2, 37\}$. The only C_3 extension of $\mathbb{Q}$ unramified outside S is[I] the splitting field of $f = x^3 - x^2 - 12x - 11$ (with discriminant 37^2), while there are two such S_3 extensions with polynomials $g = x^3 - x^2 - 3x + 1$ and $h = x^3 - x^2 - 12x + 26$ (with discriminants $37 \cdot 2^2$ and $-(2 \cdot 37)^2$ respectively), so $\mathcal{F} = \{f, g, h\}$. We may take $T_0 = \{3, 5\}$ where the values of λ are $(1, 1)$, $(1, 0)$, $(0, 1)$ for f, g, h respectively.

4.2 Determining residual irreducibility and splitting field

As above, let ρ be a Black Box 2-adic Galois representation over K unramified outside S, let $\mathcal{F} = \{f_1, \dots, f_n\}$ be a set of irreducible cubics defining all C_3 and S_3 extensions of K unramified outside S, and let T_0 be a distinguishing set of primes for $(\mathcal{F}, S)$. For $1 \le i \le n$ let L_i be the splitting field of f_i over K, and let L be the residual splitting field of ρ with respect to one stable lattice.

Proposition 4.5. *With notation as above,*

1. *If $[L : K] = 6$ or 3 then, for exactly one value $i \ge 1$, we have $L = L_i$ and*

$$\lambda(f_i, \mathfrak{p}) \equiv \mathrm{tr}(\rho(\mathrm{Frob}\,\mathfrak{p})) \pmod 2$$

for all $\mathfrak{p} \notin S(\mathcal{F})$. Moreover, for infinitely many primes $\mathfrak{p}$ we have

$$\mathrm{tr}(\rho(\mathrm{Frob}\,\mathfrak{p})) \equiv 1 \pmod 2.$$

2. *$[L : K] \le 2$ if and only if*

$$\mathrm{tr}(\rho(\mathrm{Frob}\,\mathfrak{p})) \equiv 0 \pmod 2$$

for all $\mathfrak{p} \notin S(\mathcal{F})$.

[I] These fields may be found at www.lmfdb.org/NumberField; their LMFDB labels are 3.3.148.1, 3.3.1369.1 and 3.1.5476.1.

Proof. Suppose that $[L : K] = 6$ or 3. Then the image of $\overline{\rho}$ is C_3 or S_3 and $L = L_i$, the splitting field of f_i, for some i, $1 \leq i \leq n$. Hence for all $\mathfrak{p} \notin S(\mathcal{F})$, by Lemma 4.2, we have

$$\begin{aligned}\lambda(f_i, \mathfrak{p}) = 1 &\Leftrightarrow \text{Frob}\,\mathfrak{p} \text{ has order 3 in } \text{Gal}(L_i/K)\\ &\Leftrightarrow \overline{\rho}(\text{Frob}\,\mathfrak{p}) \text{ has order 3 in } \text{GL}_2(\mathbb{F}_2)\\ &\Leftrightarrow \text{tr}(\rho(\text{Frob}\,\mathfrak{p})) \equiv 1 \pmod 2.\end{aligned}$$

On the other hand, if $[L : K] \leq 2$, the image of $\overline{\rho}$ is either C_1 or C_2. Hence $\text{tr}(\rho(\text{Frob}\,\mathfrak{p})) \equiv 0 \pmod 2$ for all $\mathfrak{p} \notin S$. □

Note that irreducibility of the residual representation can be established with a single prime $\mathfrak{p}$ such that $\text{tr}(\rho(\text{Frob}\,\mathfrak{p}))$ is odd. Using this proposition, we can achieve more: first, that for $\overline{\rho}$ to be reducible it suffices to check that $\text{tr}(\rho(\text{Frob}\,\mathfrak{p}))$ is even for a *finite* set of primes, those in T_0; secondly, that when they are not all even, the values of $\text{tr}(\rho(\text{Frob}\,\mathfrak{p})) \pmod 2$ for $\mathfrak{p} \in T_0$ identify the residual image precisely as C_3 or S_3, and also identify the splitting field exactly. Moreover both the set of cubics $\mathcal{F}$ and the distinguishing set T_0 depend only on K and S and so may be computed once and then used to test many representations ρ with the same ramification restrictions.

Proposition 4.6. *With the same notation as above, the values*

$$\{\text{tr}(\rho(\text{Frob}\,\mathfrak{p})) \pmod 2 \mid \mathfrak{p} \in T_0\}$$

determine the residual representation $\overline{\rho}$ up to semisimplification. Hence (up to semisimplification) $\overline{\rho}$ may be identified from its Black Box presentation.

Proof. Let $\mathcal{F} = \{f_1, \dots, f_n\}$ and let $T_0 = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ be a distinguishing set for $(S, \mathcal{F})$ as above. The vectors

$$\mathbf{v}_i = (\lambda(f_i, \mathfrak{p}_1), ..., \lambda(f_i, \mathfrak{p}_t)) \in \mathbb{F}_2^t$$

for $1 \leq i \leq n$ are distinct and non-zero by definition of T_0. Using the Black Box, we compute the vector

$$\mathbf{v} = (\text{tr}(\overline{\rho}(\text{Frob}\,\mathfrak{p}_1)), ..., \text{tr}(\overline{\rho}(\text{Frob}\,\mathfrak{p}_t))) \in \mathbb{F}_2^t.$$

By Proposition 4.5, we have (with L and L_i as defined there)

$$\mathbf{v} = \mathbf{v}_i \Leftrightarrow L = L_i \Leftrightarrow [L : K] = 6 \text{ or } 3$$

and

$$\mathbf{v} = \mathbf{0} \Leftrightarrow [L : K] \leq 2.$$

Hence $\overline{\rho}$ is irreducible if and only if $\mathbf{v} = \mathbf{v}_i$ for some i, in which case its splitting field is that of f_i and its image is isomorphic to S_3, unless $\text{disc}\, f_i \in (K^*)^2$ in which case the image is C_3. Otherwise, $\mathbf{v} = \mathbf{0}$ and $\overline{\rho}$ is reducible, with trivial semisimplification. □

Theorem 4.7. *Let K be a number field, S a finite set of primes of K, and let ρ be a continuous 2-dimensional 2-adic Galois representation over K unramified outside S. Then the residual representations $\overline{\rho}$ have trivial semisimplification (equivalently, are reducible), if and only if*

$$\operatorname{tr}\rho\operatorname{Frob}\mathfrak{p} \equiv 0 \pmod{2} \qquad \forall \mathfrak{p} \in T_0,$$

where T_0 is a distinguishing set for S in the sense of Definition 4.3.

Algorithm 3: To determine the residual image of an integral 2-adic Galois representation, up to semisimplification.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
         A Black Box Galois representation $\rho$ unramified outside $S$.
Output: • (True, $f$, $G$) if $\overline{\rho}$ is irreducible, with splitting field that of $f$,
         and image $G \cong C_3$ or $S_3$.
         • False if $\overline{\rho}$ is reducible.
Let $\mathcal{F} = \{f_i\}_{i=1}^n$ be a set of monic irreducible cubics defining all $S_3$ and
$C_3$ extensions of $K$ unramified outside $S$;
Using Algorithm 2, compute a distinguishing set $T_0 = \{\mathfrak{p}_1, \dots, \mathfrak{p}_t\}$ of
primes for $(\mathcal{F}, S)$;
Let $\mathbf{v} = (\operatorname{tr}(\overline{\rho}(\operatorname{Frob}\mathfrak{p}_1)), ..., \operatorname{tr}(\overline{\rho}(\operatorname{Frob}\mathfrak{p}_t)))$;
for $i$=1...$n$ do
    if $\mathbf{v} = \mathbf{v}(f_i, T_0)$ then
        Let $G = C_3$ if disc $f_i$ is square, else $G = S_3$;
        return (True, $f_i$, $G$).
return False.
```

Example. (continued.) With $K = \mathbb{Q}$, $S = \{2, 37\}$ we have $\#\mathcal{F} = 3$ and $T_0 = \{3, 5\}$. Hence for a mod 2 representation over $\mathbb{Q}$ unramified outside $\{2, 37\}$ we may test irreducibility by inspecting the parity of the trace a_p at $p = 3$ and $p = 5$. As an example, we consider the 156 isogeny classes of elliptic curves of conductor $2^a 37^b$. Of these, 36 have $a_3 \equiv a_5 \equiv 0 \pmod{2}$, hence the representation is reducible; indeed, these curves have rational 2-torsion. There are 8 with $a_3 \equiv a_5 \equiv 1 \pmod{2}$ with 2-division field the splitting field of $f = x^3 - x^2 - 12x - 11$. The remaining 112 classes comprise 80 with $a_3 \equiv 1, a_5 \equiv 0 \pmod{2}$ and 32 with $a_3 \equiv 0, a_5 \equiv 1 \pmod{2}$, whose 2-division fields have Galois group S_3 and are the splitting fields of $g = x^3 - x^2 - 3x + 1$ and $h = x^3 - x^2 - 12x + 26$, respectively. These curves have no rational 2-torsion.

Here we could have considered the curves up to isogeny and up to quadratic twist, since quadratic twists obviously have the same mod 2 representation. The number of cases then reduces to 22 (6 reducible and 1, 11, and 4 for each irreducible case).

5 Determining triviality of the residual representation up to isogeny

Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a continuous Galois representation unramified outside S with reducible residual representation. Depending on the choice of stable lattice Λ, the order of $\overline{\rho}_\Lambda(G_K) \le \mathrm{GL}_2(\mathbb{F}_2)$ is either 1 or 2, though the semisimplification of $\overline{\rho}_\Lambda$ is always trivial. In this section we will give a method to decide whether within the isogeny class of ρ there is an integral representation ρ_Λ whose residual representation $\overline{\rho}_\Lambda$ is trivial. If this is the case, the isogeny class $\mathrm{BT}(\rho)$ has width at least 2 and contains at least 4 elements, while otherwise its width is 1 and its size is exactly 2. We call these *large* and *small* isogeny classes respectively.

Vertices of $\mathrm{BT}(\rho)$ either have degree 1, non-trivial residual representation, and quadratic splitting field with non-trivial discriminant in $K(S,2)_u$; or degree 3 and trivial residual representation. So each vertex of $\mathrm{BT}(\rho)$ has an associated discriminant, and we would like to describe the graph structure of $\mathrm{BT}(\rho)$—the number of vertices, and width—as well as the discriminants of its extremal (degree 1) vertices.

In this section we show how to distinguish the small and large cases; in Section 6 we will continue under the assumption that the class is large. The following notation will be useful for the tests we will develop; note that since we are now assuming that ρ is residually reducible, $\mathrm{tr}(\rho(\mathrm{Frob}\,\mathfrak{p})) \equiv 0 \pmod 2$ for all $\mathfrak{p} \notin S$ so that $F_\mathfrak{p}(1) \equiv 0 \pmod 2$. Define

$$v(\mathfrak{p}) = \mathrm{ord}_2(F_\mathfrak{p}(1)). \tag{8}$$

When $v(\mathfrak{p}) \ge k$ for some $k \ge 1$, we define the *test function*

$$\begin{aligned} t_k(\mathfrak{p}) &= \frac{1}{2^k} F_\mathfrak{p}(1) \pmod 2 \\ &= \frac{1}{2^k}(1 - \mathrm{tr}(\rho(\mathrm{Frob}\,\mathfrak{p})) + \det(\rho(\mathrm{Frob}\,\mathfrak{p}))) \pmod 2. \end{aligned} \tag{9}$$

so that $t_k(\mathfrak{p}) = 0$ if and only if $v(\mathfrak{p}) \ge k+1$. Write $t_k(\sigma) = t_k(\mathfrak{p})$ when $\sigma = \mathrm{Frob}\,\mathfrak{p}$.

5.1 The test function for small isogeny classes

Let Λ_1 be a stable lattice under the action of ρ. Since $\overline{\rho}$ is reducible, there is an index 2 sublattice Λ_2 which is also stable under ρ. Choosing the bases $\Lambda_1 = \langle v, w\rangle$ and $\Lambda_2 = \langle 2v, w\rangle$ we have that

$$\rho(\sigma) = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod 2$$

for all $\sigma \in G_K$. There are two ways in which the graph Λ_1—Λ_2 could be extended within $\mathrm{BT}(\rho)$, either or both of which could happen:

(a) If $c \equiv 0 \pmod 4$ for all $\sigma \in G_K$ then

$$\rho(\sigma) \equiv \begin{pmatrix} \pm 1 & * \\ 0 & \pm 1 \end{pmatrix} \pmod 4$$

and $\Lambda_3 = \langle 4v, w \rangle$ is also stable, extending the stable graph to Λ_1—Λ_2—Λ_3. The lattice $\Lambda_4 = \langle 2v + w, 2w \rangle$ is also stable and adjacent to Λ_2, so Λ_2 has degree 3 in $\mathrm{BT}(\rho)$.

(b) If $b \equiv 0 \pmod 2$ for all $\sigma \in G_K$ then

$$\rho(\sigma) \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod 2$$

so $\overline{\rho}$ is trivial. Then $\Lambda_3' = \langle v, 2w \rangle$ is also stable and extends the graph to Λ_3'—Λ_1—Λ_2. The lattice $\Lambda_4' = \langle 2v, v + w \rangle$ is also stable and adjacent to Λ_1, so Λ_1 has degree 3 in $\mathrm{BT}(\rho)$.

These two situations are not essentially different, since by conjugating with the matrix $\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$ we interchange the roles of Λ_1 and Λ_2, and the two cases.

The following maps are easily seen to define two additive quadratic characters of G_K, unramified outside S:

$$\chi_c \colon \sigma \mapsto \frac{c}{2} \pmod 2 \quad \text{and} \quad \chi_b \colon \sigma \mapsto b \pmod 2,$$

which correspond to two extensions $K(\sqrt{\Delta_b})$, $K(\sqrt{\Delta_c})$ with $\Delta_b, \Delta_c \in K(S,2)_u$, possibly equal or trivial, and the isogeny class $\mathrm{BT}(\rho)$ is large if and only if at least one is trivial. This establishes the following criterion.

Proposition 5.1. $\mathrm{BT}(\rho)$ *is small if and only if the characters* χ_b *and* χ_c *are both non-trivial.*

In order to turn this criterion into an algorithm we must see how to obtain information about these two characters using only the Black Box and a finite set of primes $\mathfrak{p} \notin S$. Taking $k = 1$ in (9) we use the test function

$$\begin{aligned} t_1(\sigma) &= \frac{1}{2}(F_\sigma(1)) \pmod 2 \\ &\equiv \frac{1}{2}(1 - \mathrm{tr}(\rho(\sigma)) + \det(\rho(\sigma))) \pmod 2. \end{aligned} \tag{10}$$

Proposition 5.2. *With notation as above,*

$$t_1(\sigma) = \chi_b(\sigma)\chi_c(\sigma).$$

Proof. We compute $t_1(\sigma) = \frac{1}{2}((a-1)(d-1)-bc) \equiv bc/2 \equiv \chi_b(\sigma)\chi_c(\sigma) \pmod 2$, using $a \equiv d \equiv 1 \pmod 2$. □

So the Black Box reveals the value of the *product* of the two characters.

Corollary 5.3. *The following are equivalent, assuming that ρ is residually reducible:*

1. $\mathrm{BT}(\rho)$ *is large;*
2. $t_1(\sigma) = 0$ *for all* $\sigma \in G_K$*;*
3. $t_1(\mathfrak{p}_I) = 0$ *for all primes* $\mathfrak{p}_I$*, one such prime for each of the* 2^r *subsets* $I \subseteq \{1, 2, \ldots, r\}$*.*

Proof. The equivalence of the first two statements is because $\ker \chi_b$ and $\ker \chi_c$ are subgroups of G_K, and no group is the union of two proper subgroups. For the second equivalence, note that the pair of values $(\chi_b(\operatorname{Frob} \mathfrak{p}), \chi_c(\operatorname{Frob} \mathfrak{p}))$ depends only on the restriction of $\operatorname{Frob} \mathfrak{p}$ to the maximal elementary 2-extension of K unramified outside S whose Galois group consists of these $\operatorname{Frob} \mathfrak{p}_I$. □

Although the corollary already reduces the current problem to a finite number of tests, we will show in the next subsection how to use some linear algebra over $\mathbb{F}_2$ to reduce the test set of primes from a set of size 2^r (one for each subset I) to a set of $r(r+1)/2$ *quadratically independent* primes (with respect to S). Using these, we will be able to determine not only whether at least one of Δ_b, Δ_c is trivial, in which case the class is large; when both characters are non-trivial, we will also be able to determine the unordered pair $\{\Delta_b, \Delta_c\}$ exactly.

5.2 Quadratically independent sets of primes

Let $\{\Delta_i\}_{i=1}^r$ be a basis for $V = K(S, 2)_u$. The discriminants $\Delta_b, \Delta_c \in V$ may be expressed as

$$\Delta_b = \prod_{i=1}^{r} \Delta_i^{x_i}, \quad \Delta_c = \prod_{i=1}^{r} \Delta_i^{y_i}$$

with unknown coefficient vectors $\mathbf{x} = (x_i)$ and $\mathbf{y} = (y_i)$ in $\mathbb{F}_2^r$. We will determine the vectors $\mathbf{x}$ and $\mathbf{y}$ in the restricted sense of knowing whether either (a) at least one of $\mathbf{x}$ and $\mathbf{y}$ is zero, or (b) they are both non-zero, in which case we will identify them precisely, as an unordered pair.

Let $T_1 = \{\mathfrak{p}_1, ..., \mathfrak{p}_r\}$ be a linearly independent set of primes chosen so that the $\alpha_{\mathfrak{p}_i}$ are a dual basis for V. Then by (7) we have $\chi_b(\mathfrak{p}_i) = x_i$ and $\chi_c(\mathfrak{p}_i) = y_i$. Hence, by Proposition 5.2, we have that $t_1(\mathfrak{p}_i) = x_i y_i$. More generally for a prime $\mathfrak{p}_I$ (defined in Section 3) we have, by (7),

$$t_1(\mathfrak{p}_I) = x_I y_I$$

where we set $x_I = \sum_{i \in I} x_i$ and similarly for y_I.

Define

$$\begin{aligned} \psi \colon V \times V \times V^* &\to \mathbb{F}_2 \\ (\Delta, \Delta', \alpha) &\mapsto \alpha(\Delta)\alpha(\Delta') \end{aligned} \tag{11}$$

For fixed α, the map $\psi_\alpha = \psi(-,-,\alpha)$ is a symmetric bilinear function $V \times V \to \mathbb{F}_2$, i.e., an element of the space $\mathrm{Sym}^2(V)^*$ which has dimension $r(r+1)/2$ and basis the functions $x_i y_i$ and $x_i y_j + x_j y_i$ for $i \neq j$. This leads us to define our third (and last) set of test primes:

Definition 5.4. A set T_2 of primes $\mathfrak{p} \notin S$ is *quadratically independent with respect to* S if $\{\psi_{\alpha_\mathfrak{p}} \mid \mathfrak{p} \in T_2\}$ is a basis for $Sym^2(V)^*$.

The simplest quadratically independent sets consist of primes $\mathfrak{p}_i$ for $1 \leq i \leq r$ (these already form a linearly independent set, previously denoted T_1), together with $\mathfrak{p}_{ij}$ for $1 \leq i < j \leq r$. We will call quadratically independent sets of this form *special*.

Remark 5.5. If we fix instead (Δ, Δ') in (11) we obtain a quadratic function $\psi_{(\Delta,\Delta')} = \psi(\Delta, \Delta', -)$ on V^*:

$$\begin{aligned} \psi_{(\Delta,\Delta')} \colon V^* &\to \mathbb{F}_2 \\ \alpha &\mapsto \alpha(\Delta)\alpha(\Delta'). \end{aligned}$$

It is not hard to show when T_2 is a quadratically independent set of primes, the set $\{\alpha_\mathfrak{p} \mid \mathfrak{p} \in T_2\}$ is a *non-quadratic* subset of V^* in the sense of Livné [10].

We now proceed to show that the values of the test function $t_1(\mathfrak{p})$ for $\mathfrak{p}$ in a special quadratically independent set of primes are sufficient to solve our problem concerning the identification of the vectors $\mathbf{x}$ and $\mathbf{y}$. Define $\mathbf{v} = (v_1, ..., v_r) \in \mathbb{F}_2^r$ to be the vector with entries

$$v_i = x_i y_i = t(\mathfrak{p}_i).$$

Next let $\mathbf{W} = (w_{ij})$ be the skew-symmetric $r \times r$ matrix over $\mathbb{F}_2$ with entries $w_{ii} = 0$ and, for $i \neq j$,

$$\begin{aligned} w_{ij} = x_i y_j + x_j y_i &= (x_i + x_j)(y_i + y_j) + x_i y_i + x_j y_j \\ &= t(\mathfrak{p}_{ij}) + t(\mathfrak{p}_i) + t(\mathfrak{p}_j). \end{aligned}$$

Then the i-th row of $\mathbf{W}$ is given by

$$y_i \, \mathbf{x} + x_i \, \mathbf{y} = \begin{cases} \mathbf{0} & \text{if } (x_i, y_i) = (0,0); \\ \mathbf{x} & \text{if } (x_i, y_i) = (0,1); \\ \mathbf{y} & \text{if } (x_i, y_i) = (1,0); \\ \mathbf{x} + \mathbf{y} & \text{if } (x_i, y_i) = (1,1), \end{cases} \tag{12}$$

so that the rank of $\mathbf{W}$ is either 0 or 2. Moreover,

- if $\mathbf{x} = \mathbf{0}$ or $\mathbf{y} = \mathbf{0}$, then $\mathbf{v} = \mathbf{0}$ and $\mathbf{W} = \mathbf{0}$;
- if $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{y} \neq \mathbf{0}$ and $\mathbf{x} = \mathbf{y}$, then $\mathbf{v} = \mathbf{x} = \mathbf{y} \neq \mathbf{0}$ and $\mathbf{W} = \mathbf{0}$;
- if $\mathbf{x} \neq \mathbf{0}$ and $\mathbf{y} \neq \mathbf{0}$ and $\mathbf{x} \neq \mathbf{y}$, then $\mathbf{W} \neq \mathbf{0}$. Moreover, at least two out of $\mathbf{x}$, $\mathbf{y}$, $\mathbf{x} + \mathbf{y}$ (which are non-zero and distinct) appear as rows of $\mathbf{W}$, and

– if $\mathbf{v} \neq \mathbf{0}$, then the rows of $\mathbf{W}$ for which $v_i = 1$ are $\mathbf{x}+\mathbf{y}$ and the remaining non-zero rows are equal to either $\mathbf{x}$ or $\mathbf{y}$;

– if $\mathbf{v} = \mathbf{0}$, then the non-zero rows of $\mathbf{W}$ are all equal to either $\mathbf{x}$ and $\mathbf{y}$.

It follows that by inspecting $\mathbf{v}$ and $\mathbf{W}$, whose entries we can obtain from our Black Box test function on $r(r+1)/2$ primes, we can indeed determine whether $\mathbf{x}$ or $\mathbf{y}$ is zero, and if both are non-zero then we can determine their values, and hence determine the unordered pair of the discriminants $\{\Delta_b, \Delta_c\}$.

Proposition 5.6. *Let ρ be residually reducible. From the set of values $\{t_1(\mathfrak{p}) \mid \mathfrak{p} \in T_2\}$ of the test function t_1 defined in (10), for T_2 a quadratically independent set of primes with respect to S, we may determine whether the isogeny class of ρ is small or large, and in the first case we can determine the two non-trivial associated discriminants.*

See Algorithm 6, where we follow the procedure above, assuming that we take for T_2 a special set $\{\mathfrak{p}_i \mid 1 \leq i \leq r\} \cup \{\mathfrak{p}_{ij} \mid 1 \leq i < j \leq r\}$. In practice it might not be efficient to insist on using a quadratically independent set of this form, because we may need to test many primes $\mathfrak{p}$ before finding primes of the form $\{\mathfrak{p}_{ij}\}$ for all $i < j$; also, the resulting primes are likely to be large. In applications, it may be computationally expensive to compute the trace of $\rho(\operatorname{Frob}\mathfrak{p})$ for primes $\mathfrak{p}$ of large norm. This is the case, for example, when ρ is the Galois representation attached to a Bianchi modular form (see [7] for numerical examples when K is an imaginary quadratic field of class number 3). In our implementation we adjust the procedure to allow for arbitrary quadratically independent sets. The details are simply additional book-keeping, and we omit them here.

We give two algorithms to compute quadratically independent sets. In both cases we consider the primes of K systematically in turn (omitting those in S), by iterating through primes on order of norm. The first algorithm returns the smallest such set (in terms of the norms of the primes), while the second only uses primes for which $\#I(\mathfrak{p}) \in \{1, 2\}$ and returns a set of the special form.

In Algorithm 4, we construct a matrix $\mathbf{A}$ whose columns are indexed by the subsets of $\{1, 2, ..., r\}$ of size 1 and 2, i.e., the sets $\{i\}$ for $1 \leq i \leq r$ and $\{i, j\}$ for $1 \leq i < j \leq r$, initially with 0 rows. For each prime $\mathfrak{p}$ we compute $I(\mathfrak{p})$ and define $\mathbf{v}(\mathfrak{p})$ in $\mathbb{F}_2^{\frac{r(r+1)}{2}}$ by setting its coordinates to be

$$\begin{cases} 1 & \text{in position } i \text{ if } i \in I(\mathfrak{p}) \\ 1 & \text{in position } \{i,j\} \text{ if } \{i,j\} \subseteq I(\mathfrak{p}) \\ 0 & \text{otherwise.} \end{cases} \tag{13}$$

We add $\mathbf{v}(\mathfrak{p})$ as a new row of $\mathbf{A}$, provided that this increases the rank of $\mathbf{A}$, and we stop when $\operatorname{rk} \mathbf{A} = r(r+1)/2$.

Algorithm 4: To determine a quadratically independent set T_2 of primes of K.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
Output: A finite quadratically independent set $T_2$ of primes of $K$.
Let $\{\Delta_i\}_{i=1}^{r}$ be a basis for for $K(S,2)_u$;
Let $T_2 = \{\}$;
Let $\mathbf{A}$ be a $0 \times \frac{r(r+1)}{2}$ matrix over $\mathbb{F}_2$;
while $\mathbf{A}$ has $< r(r+1)/2$ rows do
    Let $\mathfrak{p}$ be a prime not in $S \cup T_2$;
    Compute $I(\mathfrak{p})$ using (4);
    Compute $\mathbf{v}(\mathfrak{p})$ from (13);
    Let $\mathbf{A}' = \mathbf{A} + \mathbf{v}(\mathfrak{p})$ (adjoin $\mathbf{v}(\mathfrak{p})$ as a new row of $\mathbf{A}$);
    if $\operatorname{rk}(\mathbf{A}') > \operatorname{rk}(\mathbf{A})$ then
        Let $\mathbf{A} = \mathbf{A}'$;
        Let $T_2 = T_2 \cup \{\mathfrak{p}\}$.
return $T_2$.
```

This variant produces a special quadratically independent set by only including primes $\mathfrak{p}$ for which $I(\mathfrak{p})$ has size 1 or 2.

Algorithm 5: To determine a special quadratically independent set T_2 of primes of K.

```
Input  : A number field $K$.
         A finite set $S$ of primes of $K$.
Output: An indexed special quadratically independent set $T_2$ of primes.
Let $A = \{\}$;
Let $B = \{\}$;
while $\#(A \cup B) < r(r+1)/2$ do
    Let $\mathfrak{p}$ be a prime not in $S \cup T_2$;
    Compute $I(\mathfrak{p})$ using (4);
    if $\#I = 1$ with $I = \{i\}$ then
        if $i \notin A$ then
            Let $\mathfrak{p}_i = \mathfrak{p}$;
            Let $A = A \cup \{i\}$;
            Let $T_2 = T_2 \cup \{\mathfrak{p}_i\}$.
    if $\#I = 2$ with $I = \{i,j\}$ and $i < j$ then
        if $(i,j) \notin B$ then
            Let $\mathfrak{p}_{ij} = \mathfrak{p}$;
            Let $B = B \cup \{(i,j)\}$;
            Let $T_2 = T_2 \cup \{\mathfrak{p}_{ij}\}$.
return $T_2$.
```

Example. (continuation of Example 1) As before, we take $K = \mathbb{Q}$ and $S = \{2, 37\}$. Using $[-1, 2, 37]$ as an ordered basis for $K(S,2) = K(S,2)_u$ we find, using Algorithm 5, $T_2 = \{7, 53, 17, 3, 5, 23\}$. For example, $p = 23$ is inert in $\mathbb{Q}(\sqrt{d})$ for $d = -1$ and $d = 37$ but not for $d = 2$, so $I(23) = \{1, 3\}$. The data for these primes is as follows:

I	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{2,3\}$	$\{1,3\}$
p_I	7	53	17	3	5	23

Applying Algorithm 6 to the 36 isogeny classes of elliptic curves with good reduction outside $\{2, 37\}$ and rational 2-torsion, we find that in 4 cases the class is large, so contains an elliptic curve with full 2-torsion defined over $\mathbb{Q}$ and hence trivial mod-2 representation (these are the classes labelled `32a`, `64a`, `43808a`, `87616z`); while in all other cases the class is small. The discriminant pairs $\{\Delta_1, \Delta_2\}$ returned by Algorithm 6 in these cases are $\{-1, 37\}$ (4 cases); $\{37, -37\}$ (8 cases); $\{-1, 2\}$ (8 cases); $\{2, -2\}$ (4 cases); $\{2, 2\}$ (4 cases); and $\{74, -74\}$ (4 cases). For example, isogeny class `350464h` gives $a_p = 0$ for $p = 5, 7, 23$ and 53 while $a_{17} = 6$ and $a_3 = 2$; this yields $\mathbf{v} = (0, 1, 0)$ and $\mathbf{W} = \mathbf{0}$, so both discriminants are 2 (modulo squares). Indeed, this isogeny class consists of two elliptic curves linked by 2-isogeny, each having a discriminant which is twice a square.

We leave it to the reader to explain why in every case the Hilbert Symbol $(\Delta_1, \Delta_2) = +1$.

Algorithm 6: To determine whether the stable Bruhat-Tits tree of ρ has width exactly 1 or at least 2, together with the associated discriminants.

```
Input : A number field $K$.
        A finite set $S$ of primes of $K$.
        A Black Box Galois representation $\rho$ unramified outside $S$
        whose residual image is reducible.
Output: If $BT(\rho)$ has width 1, return: True, $\{\Delta_1, \Delta_2\}$.
        If $BT(\rho)$ has width $\geq 2$, return: False.
Let $\{\Delta_1, \dots, \Delta_r\}$ be a basis for $K(S,2)_u$;
Let $T_2 = \{\mathfrak{p}_i \mid 1 \leq i \leq r\} \cup \{\mathfrak{p}_{ij} \mid 1 \leq i < j \leq r\}$ be a special quadratically
  independent set for $S$;
Let $\mathbf{v} = (t_1(\mathfrak{p}_1), ..., t_1(\mathfrak{p}_r)) \in \mathbb{F}_2^r$;
Let $\mathbf{W} = (t_1(\mathfrak{p}_{ij}) + t_1(\mathfrak{p}_i) + t_1(\mathfrak{p}_j)) \in M_r(\mathbb{F}_2)$;
if $\mathbf{W} = \mathbf{0}$ and $\mathbf{v} = \mathbf{0}$ then
    return False;
if $\mathbf{W} = \mathbf{0}$ then
    Let $\mathbf{x} = \mathbf{y} = \mathbf{v}$;
else
    if $\mathbf{v} = \mathbf{0}$ then
        Let $\mathbf{x}$ and $\mathbf{y}$ be any two distinct non-zero rows of $\mathbf{W}$.
    else
        Let $\mathbf{z}$ be the $i$th row of $\mathbf{W}$, where $i$ is such that $t_1(\mathfrak{p}_i) = 1$;
        Let $\mathbf{x}$ be any non-zero row of $\mathbf{W}$ distinct from $\mathbf{z}$;
        Let $\mathbf{y} = \mathbf{x} + \mathbf{z}$.
return True, $\{\prod_{i=1}^r \Delta_i^{x_i}, \prod_{i=1}^r \Delta_i^{y_i}\}$.
```

The methods of this section give an algorithm to determine whether the isogeny class of ρ contains an integral representation whose residual representation is trivial.

Theorem 5.7. *Let K be a number field, S a finite set of primes of K, and let ρ be a continuous 2-dimensional 2-adic Galois representation over K unramified outside S. Assume that ρ has reducible residual representation. Then there exists a stable lattice with respect to which the residual representation $\overline{\rho}$ is trivial, if and only if*

$$t_1(\mathfrak{p}) \equiv 0 \pmod 2 \qquad \forall \mathfrak{p} \in T_2;$$

that is,

$$1 - \operatorname{tr}\rho(\operatorname{Frob}\mathfrak{p}) + \det\rho(\operatorname{Frob}\mathfrak{p}) \equiv 0 \pmod 4 \qquad \forall \mathfrak{p} \in T_2;$$

where T_2 is any quadratically independent set of primes for S.

6 Large isogeny classes

From now on we will assume that ρ has trivial residual representation, so that its isogeny class $\mathrm{BT}(\rho)$ consists at least of ρ together with the three 2-isogenous integral representations: recall that each lattice Λ has three sublattices, and the condition that $\overline{\rho}_\Lambda$ is trivial is equivalent to each of these being stable. The next step is to determine whether the class is larger than this, i.e., whether it has width greater than 2. This is not the case if and only if each of the 2-isogenous representations has a non-trivial discriminant, in which case we would like to determine this (unordered) set of three discriminants. Furthermore, we would like to determine $\rho \pmod 4$ completely.

It turns out that it is no more work to deal with the more general situation, where we assume that $\rho \pmod{2^k}$ is trivial for some $k \geq 1$, and determine $\rho \pmod{2^{k+1}}$ completely. The description of $\rho \pmod{2^{k+1}}$ will be in terms of a collection of four additive quadratic characters, which we will be able to determine using only the values of $F_{\mathfrak{p}}(1)$ for $\mathfrak{p}$ in the same quadratically independent set T_2 used in the previous section. The reason for this is that $\mathrm{GL}(\mathbb{Z}/2^{k+1}\mathbb{Z})$ is an extension of $\mathrm{GL}(\mathbb{Z}/2^k\mathbb{Z})$ by $M_2(\mathbb{F}_2)$, which is (as additive group) an elementary abelian of order 2^4, as can be seen by the following short exact sequence:

$$0 \longrightarrow M_2(\mathbb{F}_2) \longrightarrow \mathrm{GL}(\mathbb{Z}/2^{k+1}\mathbb{Z}) \longrightarrow \mathrm{GL}(\mathbb{Z}/2^k\mathbb{Z}) \longrightarrow 1$$

where the second arrow maps $A \in M_2(\mathbb{F}_2)$ to $\mathbf{I} + 2^k A \in \mathrm{GL}(\mathbb{Z}/2^{k+1}\mathbb{Z})$.

Thus let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be an integral Galois representation unramified outside S, and assume that ρ is trivial modulo 2^k for some positive integer k. Write

$$\rho(\sigma) = \mathbf{I} + 2^k \mu(\sigma), \tag{14}$$

where

$$\mu(\sigma) = \begin{pmatrix} a(\sigma) & b(\sigma) \\ c(\sigma) & d(\sigma) \end{pmatrix} \in M_2(\mathbb{Z}_2).$$

Then $F_\sigma(1) = 2^{2k} \det \mu(\sigma) \equiv 0 \pmod{2^{2k}}$, and we can use the test function $t_{2k}(\mathfrak{p}) = \frac{1}{2^{2k}} F_{\mathfrak{p}}(1) = \det \mu(\sigma) \equiv ad - bc \pmod 2$ for $\mathfrak{p} \notin S$.

Secondly, with the same notation,

$$\det \rho(\sigma) \equiv 1 + 2^k(a + d) \pmod{2^{2k}},$$

so

$$a + d \equiv \frac{1}{2^k}(\det \rho(\sigma) - 1) \pmod 2.$$

Thus we see that the Black Box gives us the values of both $\operatorname{tr} \mu(\sigma)$ and $\det \mu(\sigma) \pmod 2$ for $\sigma = \operatorname{Frob} \mathfrak{p} \in G_K$. Now the map $\sigma \mapsto \mu(\sigma) \pmod 2$ is a group homomorphism $G_K \to M_2(\mathbb{F}_2)$; composing with the four characters

$$\begin{aligned} &M_2(\mathbb{F}_2) \to \mathbb{F}_2 \\ &\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto a, b, c, d \end{aligned}$$

we obtain four additive characters of G_K

$$\begin{aligned} G_K &\to \mathbb{F}_2 \\ \sigma &\mapsto a(\sigma), b(\sigma), c(\sigma), d(\sigma) \pmod 2 \end{aligned}$$

all unramified outside S, which we denote by χ_a, χ_b, χ_c and χ_d. To each character there is associated a discriminant, named $\Delta_a, \Delta_b, \Delta_c, \Delta_d \in K(S,2)_u$. Set $\chi_{abcd} = \chi_a + \chi_b + \chi_c + \chi_d$ and $\chi_{\det} = \chi_a + \chi_d$; the latter has discriminant $\Delta_{\det} = \Delta_a\Delta_d$ (the reason for this notation will be clear after the following lemma). Our task is to use the values of $a+d$ and $ad-bc$ at suitably chosen primes to obtain information about these four characters.

The previous computation of determinants gives the following result linking $\operatorname{tr}\mu(\sigma) = a+d$ with $\det\rho(\sigma) \pmod{2^{k+1}}$. Recall that by equality of discriminants we always mean modulo squares.

Lemma 6.1. *Assume that ρ is trivial modulo 2^k. With notation as above, the following are equivalent:*

1. $\det\rho$ *is trivial modulo* 2^{k+1}*;*
2. $a(\sigma) \equiv d(\sigma) \pmod 2$ *for all* $\sigma \in G_K$*;*
3. $\chi_{\det} = 0$*;*
4. $\Delta_{\det} = 1$.

The characters we have just defined depend not only on the stable lattice (here $\Lambda = \mathbb{Z}_2^2$, since we are treating ρ as an integral matrix representation) but also on a choice of basis. If we change basis via $\mathbf{U} \in \mathrm{GL}_2(\mathbb{Z}_2)$, the result is to conjugate the matrices $\rho(\sigma)$ and $\mu(\sigma)$ by $\mathbf{U}$ and replace the four characters χ_a, $\dots$, χ_d by $\mathbb{F}_2$-linear combinations. By using suitable matrices $\mathbf{U}$ of orders 2 and 3 we may obtain all 6 permutations of $\{b, c, a+b+c+d\}$: taking $\mathbf{U} = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix}$ (of order 3) cycles $b \mapsto c \mapsto a+b+c+d \mapsto b$, while $\mathbf{U} = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (of order 2) transposes $b \leftrightarrow c$ while fixing $a+b+c+d$. Of course the determinant character $a+d$ (which is the sum of these three) is unchanged. We will make use of this symmetry in what follows.

More generally, if $\mathbf{U} \in \mathrm{GL}_2(\mathbb{Q}_2) \cap M_2(\mathbb{Z}_2)$ is such that conjugation by $\mathbf{U}$ maps the image of ρ into $\mathrm{GL}_2(\mathbb{Z}_2)$, then $\sigma \mapsto \mathbf{U}\,\rho(\sigma)\,\mathbf{U}^{-1}$ is another integral representation isogenous to ρ. We will use this construction below with $\mathbf{U} = \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$.

6.1 Stable sublattices of index 2^{k+1}

We continue to assume that ρ is trivial modulo 2^k and use the notation introduced in the previous subsection. Clearly all sublattices of index 2^k in $\Lambda = \mathbb{Z}_2^2$ are stable under ρ. Here we consider the sublattices of index 2^{k+1} and show that the condition of whether they are also stable may be expressed in terms of the characters $\{\chi_b, \chi_c, \chi_{a+b+c+d}\}$. In terms of the isogeny graph $\mathrm{BT}(\rho)$, it contains all paths of length k (of which there are $3\cdot 2^{k-1}$) starting at the "central" vertex associated with Λ—so the graph has width at least $2k$—and we are determining whether any such paths may be extended within $\mathrm{BT}(\rho)$ by one edge. This turns out to depend only on the first edge in the path (adjacent to Λ itself).

When considering sublattices we restrict to those which are *cocyclic*, i.e. for which the quotient is cyclic, or equivalently are not contained in 2Λ. The cocyclic sublattices Λ' of index 2^{k+1} in $\Lambda = \mathbb{Z}_2^2$ are given by

$$\Lambda' = \langle \mathbf{v} \rangle + 2^{k+1}\Lambda, \quad \text{with} \quad \mathbf{v} = \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}_2^2,$$

where x, y are not both even, and Λ' only depends on the image of $\mathbf{v}$ in $\mathbb{P}^1(\mathbb{Z}/2^{k+1}\mathbb{Z})$. Now Λ' is fixed by ρ if and only if for all $\sigma \in G_K$

$$\rho(\sigma)\,\mathbf{v} \equiv \lambda\,\mathbf{v} \pmod{2^{k+1}}$$

for some $\lambda \in \{1, 1+2^k\}$. Since $\rho(\sigma) = \mathbf{I} + 2^k\mu(\sigma)$, this is if and only if $\mathbf{v}$ is an eigenvector of $\mu(\sigma) \pmod 2$. Hence the stability of Λ' only depends on the image of $\mathbf{v}$ in $\mathbb{P}^1(\mathbb{Z}/2\mathbb{Z})$, and the three possible values of $\mathbf{v} \pmod 2$ correspond to the three edges in the graph adjacent to Λ itself. The following is now immediate (where to save space we write $\mathbf{v}$ as a row vector):

Lemma 6.2.

1. *$\mathbf{v} \equiv (1,0) \pmod 2$ is an eigenvector of $\mu(\sigma)$ if and only if $c(\sigma) \equiv 0 \pmod 2$; hence such Λ' are stable if and only if $\chi_c = 0$;*

2. *$\mathbf{v} \equiv (0,1) \pmod 2$ is an eigenvector of $\mu(\sigma)$ if and only if $b(\sigma) \equiv 0 \pmod 2$; hence such Λ' are stable if and only if $\chi_b = 0$;*

3. *$\mathbf{v} \equiv (1,1) \pmod 2$ is an eigenvector of $\mu(\sigma)$ if and only if $a(\sigma) + b(\sigma) + c(\sigma) + d(\sigma) \equiv 0 \pmod 2$; such Λ' are stable if and only if $\chi_{a+b+c+d} = 0$.*

For example, when $k = 1$, the generic stable Bruhat-Tits tree of width at least 2 looks like

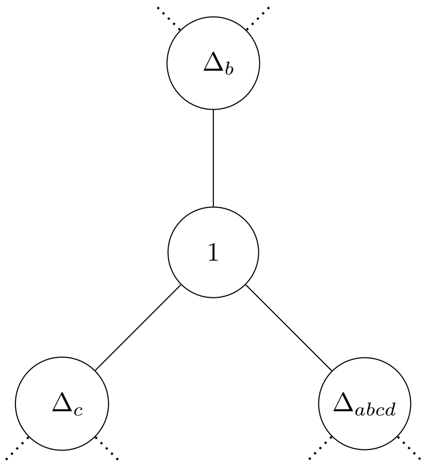


Figure A1: Tree of width at least 2.

Note that the three discriminants at the vertices adjacent to the central one (which has trivial discriminant) have product Δ_{det}, only depending on $\det \rho$.

In the case $k = 1$ we deduce the following.

Corollary 6.3. *When ρ is trivial modulo 2, the isogeny graph $\mathrm{BT}(\rho)$ has width at least 3 if and only if at least one of the characters χ_b, χ_c, $\chi_{a+b+c+d}$ is trivial.*

Below we will see how to determine all four characters (up to S_3 symmetry). In the case $k = 1$, we will determine when all three characters in the Corollary are non-trivial, so that the graph has width exactly 2, and in this case we will determine precisely the unordered set of three discriminants in the diagram.

6.2 Determining the four characters: the test

As before, let $\{\Delta_i\}_{i=1}^r$ be a fixed basis of $K(S,2)_u$ and write

$$\Delta_b = \prod_{i=1}^r \Delta_i^{x_i}, \qquad \Delta_c = \prod_{i=1}^r \Delta_i^{y_i}, \qquad \Delta_{abcd} = \prod_{i=1}^r \Delta_i^{z_i}, \tag{15}$$

$$\Delta_a = \prod_{i=1}^r \Delta_i^{u_i}, \qquad \Delta_d = \prod_{i=1}^r \Delta_i^{v_i},$$

where

$$\mathbf{x} = \{x_i\}_{i=1}^r, \mathbf{y} = \{y_i\}_{i=1}^r, \mathbf{z} = \{z_i\}_{i=1}^r, \mathbf{u} = \{u_i\}_{i=1}^r, \mathbf{v} = \{v_i\}_{i=1}^r \in \mathbb{F}_2^r.$$

To determine ρ modulo 2^{k+1} it is enough to determine these vectors, noting that $\mathbf{x}+\mathbf{y}+\mathbf{z} = \mathbf{u}+\mathbf{v}$, and bearing in mind the S_3 symmetry.

For primes $\mathfrak{p} \notin S$, we use the test function $t_{2k}(\mathfrak{p}) \equiv ad - bc \pmod{2}$, dividing into cases according to $\det \rho(\mathrm{Frob}\,\mathfrak{p}) \pmod{2^{k+1}}$:

- If $\det(\rho(\mathrm{Frob}\,\mathfrak{p})) \equiv 1 \pmod{2^{k+1}}$, then $a + d \equiv 0 \pmod{2}$, hence $ad \equiv a \pmod{2}$, so
$$t_{2k}(\mathfrak{p}) \equiv a + bc \pmod{2}. \tag{16}$$
- If $\det(\rho(\mathrm{Frob}\,\mathfrak{p})) \equiv 1 + 2^k \pmod{2^{k+1}}$, then $a + d \equiv 1 \pmod{2}$, so $ad \equiv 0 \pmod{2}$, and
$$t_{2k}(\mathfrak{p}) \equiv bc \pmod{2}. \tag{17}$$

Note that we will know from the Black Box which case we are in from the value of $\operatorname{tr} \rho(\mathrm{Frob}\,\mathfrak{p})$, since

$$\operatorname{tr}(\rho(\mathrm{Frob}\,\mathfrak{p})) = 2 + 2^k(a + d). \tag{18}$$

Now it is convenient to divide into two cases, depending on whether or not $\det \rho$ is trivial modulo 2^{k+1}; equivalently, whether or not $\Delta_{\det} = 1$.

6.3 Determining the four characters: the case $\Delta_{\det} = 1$

In this case the character $\chi_{\det}$ is trivial, $\Delta_a = \Delta_d$, and $\mathbf{u} = \mathbf{v}$. Moreover, $\Delta_{abcd} = \Delta_b\Delta_c$, so $\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{0}$. By S_3 symmetry, only the set $\{\mathbf{x}, \mathbf{y}, \mathbf{z}\}$ is well-defined.

Taking $T_2 = \{\mathfrak{p}_i \mid 1 \le i \le r\} \cup \{\mathfrak{p}_{ij} \mid 1 \le i < j \le r\}$ as in Section 5, we have

$$\begin{aligned} t_{2k}(\mathfrak{p}_i) &= u_i + x_i y_i, \quad i \ge 1, \\ t_{2k}(\mathfrak{p}_{ij}) &= u_i + u_j + (x_i + x_j)(y_i + y_j), \quad i, j \ge 1. \end{aligned} \tag{19}$$

Define

$$\begin{aligned} w_{ij} &= x_i y_j + x_j y_i \\ &= t_{2k}(\mathfrak{p}_i) + t_{2k}(\mathfrak{p}_j) + t_{2k}(\mathfrak{p}_{ij}), \quad i, j \ge 1 \end{aligned} \tag{20}$$

and construct the matrix $\mathbf{W} = (w_{ij}) \in M_r(\mathbb{F}_2)$. Each non-zero row of $\mathbf{W}$ is equal to one of $\mathbf{x}$, $\mathbf{y}$ or $\mathbf{z}$, and as in Section 5, if $\mathbf{W} \ne 0$ then $\mathbf{W}$ has at least two distinct non-zero rows and has rank 2.

Case 1. $\operatorname{rk} \mathbf{W} = 2$. Now $\mathbf{W}$ contains at least two distinct non-zero rows, which by symmetry we can take to be the values of $\mathbf{x}$ and $\mathbf{y}$. Then $\mathbf{z} = \mathbf{x} + \mathbf{y}$, and we obtain the value of $\mathbf{u}$ (which equals $\mathbf{v}$), using (19) and the now known values of $\mathbf{x}$ and $\mathbf{y}$. Therefore we have computed all the exponent vectors $\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}, \mathbf{z}$ and obtained $\Delta_a, \Delta_b, \Delta_c, \Delta_d$ and Δ_{abcd}.

Case 2. $\mathbf{W} = \mathbf{0}$. Now at least one of $\mathbf{x}$, $\mathbf{y}$ or $\mathbf{z}$ is zero; by symmetry we may take $\mathbf{y} = \mathbf{0}$, and $\mathbf{x} = \mathbf{z}$, but we do not yet know the common value of $\mathbf{x}$ and $\mathbf{z}$. However we have $t_{2k}(\mathfrak{p}_i) = u_i + x_i y_i = u_i$, so we recover $\mathbf{u}$.

To determine $\mathbf{x}$ and hence obtain the final discriminant Δ_b, we need to go a step further and consider the values of $F_{\mathfrak{p}}(1) \pmod{2^{2k+2}}$. At the end we may need to replace ρ by a 2-isogenous representation; recall that the Black Box only determines ρ up to isogeny, so this is valid.

Recalling the notation of (14), since $\mathbf{y} = \mathbf{0}$ we observe that the entry c is always even; put $c = 2c_1$. Denote by χ_{c_1} the character $\sigma \mapsto c_1(\sigma) \pmod 2$ and let Δ_{c_1} be its discriminant. From the information already known and further tests using the Black Box with the same primes in T_2 but to higher 2-adic precision, we can determine the values of the product $\chi_b\chi_{c_1}$. As in Section 5, we can then determine whether either Δ_b or Δ_{c_1} is trivial, and their values if both are non-trivial. In the first case we may assume (conjugating if necessary) that $\Delta_b = 1$ (equivalently, $\mathbf{x} = \mathbf{0}$). In the second case, we may take either of the non-trivial discriminants to be Δ_b. This apparent ambiguity is illusory, since we are free to replace the initial integral representation ρ by an isogenous one.

For $\mathfrak{p} \notin S$ we have

$$F_{\mathfrak{p}}(1) = 2^{2k}(ad - 2bc_1). \tag{21}$$

In order to proceed, we will need the value of $ad \pmod 4$. Recall that we know the exact value of $a + d$ from (18), and we also know the common parity of a and d, namely u_I if $\mathfrak{p} = \mathfrak{p}_I$.

1. If $\mathfrak{p}$ is such that $a \equiv d \equiv 0 \pmod 2$, then $ad \equiv 0 \pmod 4$ and we obtain

   $$F_{\mathfrak{p}}(1) \equiv 2^{2k+1}bc_1 \pmod{2^{2k+2}},$$

   so our standard test function

   $$t_{2k+1}(\mathfrak{p}) = \frac{F_{\mathfrak{p}}(1)}{2^{2k+1}} \equiv bc_1 \pmod 2 \tag{22}$$

   gives the required value.

2. If $\mathfrak{p}$ is such that $a \equiv d \equiv 1 \pmod 2$ and $a + d \equiv 0 \pmod 4$, then $ad \equiv -1 \pmod 4$, so (21) becomes

   $$F_{\mathfrak{p}}(1) \equiv -2^{2k} + 2^{2k+1}bc_1 \pmod{2^{2k+2}}.$$

   Hence we define a modified test function as follows:

   $$\tilde{t}_{2k+1}(\mathfrak{p}) = \frac{F_{\mathfrak{p}}(1) + 2^{2k}}{2^{2k+1}} \equiv bc_1 \pmod 2. \tag{23}$$

3. If $\mathfrak{p}$ is such that $a \equiv d \equiv 1 \pmod 2$ and $a + d \equiv 2 \pmod 4$, then $ad \equiv 1 \pmod 4$ and (21) becomes

   $$F_{\mathfrak{p}}(1) \equiv 2^{2k} + 2^{2k+1}bc_1 \pmod{2^{2k+2}};$$

   we define

   $$\tilde{t}_{2k+1}(\mathfrak{p}) = \frac{F_{\mathfrak{p}}(1) - 2^{2k}}{2^{2k+1}} \equiv bc_1 \pmod 2. \tag{24}$$

In summary, when ρ is trivial modulo 2^k and has trivial determinant modulo 2^{k+1}, we can use the test function values $t_{2k}(\mathfrak{p})$ for $\mathfrak{p} \in T_2$ (where T_2 is a quadratically independent set of primes for S), together with either t_{2k+1} or one of the modified tests $\tilde{t}_{2k+1}$ depending on $\mathfrak{p}$, to determine the full set of characters χ_a, χ_b, χ_c, χ_d, satisfying $\chi_a + \chi_d = 0$, if necessary replacing ρ by a $\mathrm{GL}_2(\mathbb{Z}_2)$-equivalent representation, or by a 2-isogenous representation. In particular, if all the characters are trivial then (up to a 2-isogeny) we conclude that ρ is trivial modulo 2^{k+1}.

6.4 Determining the four characters: the case $\Delta_{\mathrm{det}} \neq 1$

Now assume that the determinant character χ_{det} is non-trivial, i.e. that $\det \rho$ is not identically $1 \pmod{2^{k+1}}$. To ease notation, we choose a basis $\{\Delta_i\}_{i=1}^r$ of $K(S,2)_u$ such that $\Delta_1 = \Delta_{\mathrm{det}}$. The unknown vectors in $\mathbb{F}_2^r$ then satisfy

$$\mathbf{x} + \mathbf{y} + \mathbf{z} = \mathbf{u} + \mathbf{v} = \mathbf{e}_1 \,.$$

where $\mathbf{e}_1 = (1, 0, ..., 0)$. Denote by $\mathbf{x}'$, $\mathbf{y}'$ *etc.* the vectors in $\mathbb{F}_2^{r-1}$ obtained by deleting the first coordinate. These satisfy

$$\mathbf{x}' + \mathbf{y}' + \mathbf{z}' = \mathbf{u}' + \mathbf{v}' = \mathbf{0}$$

and we will determine them first.

Take primes $\mathfrak{p}_i, \mathfrak{p}_{ij} \in T_2$ with $i, j \geq 2$ and $i \neq j$. For such primes (as for all $\mathfrak{p}_I$ when $1 \notin I$) we have $\det \rho(\mathrm{Frob}\,\mathfrak{p}) \equiv 1 \pmod{2^{k+1}}$, so from (16) and using $u_i = v_i$ for $i \geq 2$ we see that

$$\begin{aligned} t_{2k}(\mathfrak{p}_i) &= u_i + x_i y_i, \quad i \geq 2, \\ t_{2k}(\mathfrak{p}_{ij}) &= u_i + u_j + (x_i + x_j)(y_i + y_j), \quad 2 \leq i \neq j \leq r, \end{aligned} \tag{25}$$

and hence we can compute

$$\begin{aligned} w_{ij} &= x_i y_j + x_j y_i \\ &= t_{2k}(\mathfrak{p}_i) + t_{2k}(\mathfrak{p}_j) + t_{2k}(\mathfrak{p}_{ij}), \quad i, j \geq 2. \end{aligned} \tag{26}$$

Just as in Section 6.3 we can determine the shortened vectors $\mathbf{x}', \mathbf{y}', \mathbf{z}', \mathbf{u}', \mathbf{v}'$ (possibly replacing ρ by an isogenous representation).

The final step is to determine the first coordinates u_1, v_1, x_1, y_1 and z_1 with $x_1 + y_1 + z_1 = u_1 + v_1 = 1$, using the remaining primes in T_2 and test values $t_{2k}(\mathfrak{p}_1)$ and $t_{2k}(\mathfrak{p}_{1i})$, for $2 \leq i \leq r$. We first note the following symmetries:

(1) $\mathbf{u}'$ and $\mathbf{v}'$, and hence $\mathbf{u}$ and $\mathbf{v}$, are interchangeable (by conjugation); hence we can arbitrarily set $u_1 = 1$ and $v_1 = 0$;

(2) concerning $\mathbf{x}'$, $\mathbf{y}'$ and $\mathbf{z}'$:

   (a) if all are non-zero, and hence also distinct, then we can permute them arbitrarily;

(b) if all are zero, then again we can permute $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$ arbitrarily;

(c) otherwise, one of them is zero and the others equal and non-zero; we have chosen them so that $\mathbf{y}' = \mathbf{0}$ and $\mathbf{x}' = \mathbf{z}'$, so we can still swap $\mathbf{x}$ and $\mathbf{z}$.

Now $t_{2k}(\mathfrak{p}_1) = x_1y_1$, since $u_1v_1 = 0$. Hence if $t_{2k}(\mathfrak{p}_1) = 1$ then we deduce that $x_1 = y_1 = z_1 = 1$; prepending a 1 to $\mathbf{x}'$, $\mathbf{y}'$ and $\mathbf{z}'$ gives $\mathbf{x}$, $\mathbf{y}$ and $\mathbf{z}$. Otherwise, $x_1y_1 = 0$ and we need to determine which one of x_1, y_1 or z_1 is 1, the other two being 0. We can compute

$$\begin{aligned} t_{2k}(\mathfrak{p}_{1i}) &= (u_1+u_i)(v_1+v_i) + (x_1+x_i)(y_1+y_i) \\ &= (x_1+x_i)(y_1+y_i) \end{aligned}$$

for $i \geq 2$ (using $u_1+u_i \neq v_1+v_i$) and hence get the values $y_1x_i + x_1y_i$ for $i \geq 2$, since we already know x_1y_1 and all x_iy_i for $i \geq 2$.

Define

$$\mathbf{q} = (t_{2k}(\mathfrak{p}_i) + t_{2k}(\mathfrak{p}_{1i}) + u_i)_{i=2}^{r} = y_1\,\mathbf{x}' + x_1\,\mathbf{y}' \in \mathbb{F}_2^{r-1}.$$

Consider the three cases under (2) above:

- In (2)a, $\mathbf{x}'$ and $\mathbf{y}'$ are linearly independent so $\mathbf{q}$ determines x_1 and y_1 uniquely;
- In (2)b, we have complete symmetry and may set $\mathbf{x} = \mathbf{y} = \mathbf{0}$ and $\mathbf{z} = \mathbf{e}_1$;
- In (2)c, since $\mathbf{y}' = \mathbf{0}$ we have $\mathbf{q} = y_1\,\mathbf{x}'$ and $\mathbf{x}'$ is not zero, so if $\mathbf{q} \neq \mathbf{0}$ then $y_1 = 1$ and $x_1 = z_1 = 0$. On the other hand, if $\mathbf{q} = \mathbf{0}$ then $y_1 = 0$ and we can set $x_1 = 0$, $z_1 = 1$ (or vice versa, it does not matter since $\mathbf{x}' = \mathbf{z}'$).

This completes the method to determine the vectors $\mathbf{u}, \mathbf{v}, \mathbf{x}, \mathbf{y}, \mathbf{z}$ and hence the discriminants Δ_a, Δ_b, Δ_c, Δ_d and Δ_{abcd} and the associated characters.

In summary, when ρ is trivial modulo 2^k and has non-trivial determinant modulo 2^{k+1}, we can again use the test function values $t_{2k}(\mathfrak{p})$ for $\mathfrak{p} \in T_2$ (where T_2 is a quadratically independent set of primes for S), together with either t_{2k+1} or one of the modified tests $\tilde{t}_{2k+1}$ depending on $\mathfrak{p}$, to determine the full set of characters χ_a, χ_b, χ_c, χ_d, satisfying $\chi_a + \chi_d = \chi_{\det} \neq 0$, if necessary replacing ρ by a $\mathrm{GL}_2(\mathbb{Z}_2)$-equivalent representation, or by a 2-isogenous representation. Unlike subsection 6.3, it is not possible for all the characters to be trivial, and ρ is certainly not trivial modulo 2^{k+1} as $\det\rho$ is nontrivial modulo 2^{k+1}.

We now summarise the results of this section.

Theorem 6.4. *Let K be a number field, S a finite set of primes of K, and ρ a 2-dimensional 2-adic Galois representation over K unramified outside S. Suppose that there exists a stable lattice under the action of ρ with respect to which $\rho \pmod{2^k}$ is trivial, for some $k \geq 1$. Then, using the output of the Black Box for ρ for a set T_2 of primes which are quadratically independent with respect to S, we can determine whether there exists a (possibly different) stable lattice with respect to which $\rho \pmod{2^{k+1}}$ is trivial. More generally we can completely determine the representation $\rho \pmod{2^{k+1}}$ on some stable lattice for ρ.*

Example. (continuation of Example 1) With $K = \mathbb{Q}$ and $S = \{2, 37\}$, let ρ be the Galois representation attached to elliptic curve isogeny class `43808a`, which is one of those which in the previous section was seen to be large, indicating that there exists an elliptic curve in the class with full rational 2-torsion. In fact, `43808a1` is such a curve, but we stress that the following facts about the isogeny class are being determined from only the knowledge of the trace of Frobenius at the six primes in T_2:

I	$\{1\}$	$\{2\}$	$\{3\}$	$\{1,2\}$	$\{2,3\}$	$\{1,3\}$
p_I	7	53	17	3	5	23
a_p	0	14	-2	0	2	2

Now, $\Delta_{\text{det}} = -1$, this being the discriminant of the cyclotomic character on the 4th roots of unity. Using the method of subsection 6.4, we compute $t_2(p_2) = t_2(53) \equiv 0$, $t_2(p_3) = t_2(17) \equiv 1$, $t_2(p_{2,3}) = t_2(5) \equiv 1$, from which $x_2y_3 + x_3y_2 \equiv 0+1+1 \equiv 0$, hence (without loss of generality) $\mathbf{y}' \equiv \mathbf{0}$ and $\mathbf{x}' \equiv \mathbf{z}'$ but the common value is not yet known. Write $\mathbf{y}'_1 = (y'_2, y'_3)$ for the exponent vector on $2, 37$ of the discriminant of the character denoted c_1 above. We find $x_2y'_2 \equiv 1$, $x_3y'_3 \equiv 0$ and $(x_2+x_3)(y'_2+y'_3) \equiv 1$ using three computations involving the special test functions t_3 and $\tilde{t_3}$ as in (22), (23) and (24) (once each). We give details of one of these. Let $p = 5 = p_{2,3}$, for which the trace is (exactly) $a_5 = 2$. Now $u_2 \equiv t_2(p_2) \equiv t_2(53) \equiv 0$ and $u_3 \equiv t_2(p_3) \equiv t_2(17) \equiv 1$, so $u_2 + u_3 \equiv 1$ and hence we are in the case where a and d are both odd with $ad \equiv -1 \pmod 4$, so $\tilde{t_3}(5) = ((1 + 5 - a_5 + 4)/8) \equiv 1$; this implies that $(x_2 + x_3)(y'_2 + y'_3) \equiv 1 \pmod 2$. The two similar computations use $a_{53} = 14$ and $a_{17} = -2$ to obtain $t_3(53) \equiv 1$ and $\tilde{t_3}(17) \equiv 0$.

Solving the congruences for x_2, x_3, y'_2, y'_3 we find $\mathbf{x}' \equiv \mathbf{y}'_1 \equiv (1, 0)$.

Next, $\mathbf{q} \equiv (t_2(p_i) + t_2(p_{1,i}) + u_i)_{i=2}^{3} = (1, 0) \not\equiv \mathbf{0}$, so $y_1 \equiv 1$ and $x_1 \equiv z_1 \equiv 0$. Finally we have $\mathbf{x} \equiv \mathbf{z} \equiv (0, 1, 0)$, $\mathbf{y} \equiv (1, 0, 0)$, and so $\Delta_b = \Delta_{abcd} = 2$ while $\Delta_c = -1$. Also $\mathbf{u} = (1, 0, 1)$ and $\mathbf{v} = (0, 0, 1)$, so $\Delta_a = -37$ and $\Delta_d = +37$. The image of the mod 4 representation has order $2^3 = 8$ since the space spanned by $\mathbf{x}, \mathbf{y}, \mathbf{z}, \mathbf{u}, \mathbf{v}$ has dimension 3, and its kernel has fixed field $\mathbb{Q}(\sqrt{-1}, \sqrt{2}, \sqrt{37})$.

To confirm this, the three elliptic curves 2-isogenous to `43808a1` do indeed have discriminants which are square multiples of -1, 2 and 2.

7 Detecting triviality of the semisimplification

In the past three sections we have given algorithms for determining the following properties of a continuous 2-dimensional 2-adic Galois representation ρ, unramified outside a given finite set of primes S, using only the output from a Black Box oracle giving for any prime $\mathfrak{p} \notin S$ the Frobenius polynomial $F_{\mathfrak{p}}(t)$:

1. whether or not ρ is residually reducible (Theorem 4.7: using the primes in a distinguishing set T_0 for S);

2. if ρ is residually reducible, whether or not ρ is residually trivial up to

isogeny (Theorem 5.7: using the primes in a quadratically independent set T_2 with respect to S);

3. if ρ is trivial modulo 2^k up to isogeny, whether or not ρ is trivial modulo 2^{k+1} up to isogeny (Theorem 6.4: again using the primes in a quadratically independent set T_2);

We also showed in Section 3 how to verify that $\det\rho$ was equal to a given 2-adic character (Theorem 3.4, using the primes in a linearly independent set T_1 with respect to S).

So far we have only needed finite 2-adic precision from our Black Box oracle. In this section we assume that the oracle can provide us with the Frobenius polynomials $F_{\mathfrak{p}}(t)$ exactly, which is usually the case in practice when they are monic polynomials in $\mathbb{Z}[t]$. By putting together the previous results we can determine whether ρ has trivial semisimplification; since we only know ρ through the characteristic polynomials of the $\rho(\sigma)$, this is as close as we can get to showing that ρ is trivial.

We start with a lemma taken from the proof of Theorem 3.4:

Lemma 7.1. *Let $\chi\colon G_K \to \mathbb{Z}_2^*$ be a continuous character unramified outside S. If*

1. $\chi(\sigma) \equiv 1 \pmod{2^{k-1}}$ *for all $\sigma \in G_K$, and*
2. $\chi(\operatorname{Frob}\mathfrak{p}) \equiv 1 \pmod{2^k}$ *for all $\mathfrak{p} \in T_1$,*

where T_1 is a linearly independent set with respect to S, then $\chi(\sigma) \equiv 1 \pmod{2^k}$ for all $\sigma \in G_K$.

Proposition 7.2. *Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a Galois representation unramified outside S such that*

$$\rho(\sigma) \equiv \mathbf{I} \pmod{2^k} \text{ for all } \sigma \in G_K.$$

Suppose that

1. $\det(\rho(\operatorname{Frob}\mathfrak{p})) \equiv 1 \pmod{2^{k+1}}$ *for all $\mathfrak{p} \in T_1$, and*
2. $F_{\mathfrak{p}}(1) \equiv 0 \pmod{2^{2k+2}}$ *for all $\mathfrak{p} \in T_2$,*

where T_1 is a linearly independent set and T_2 a quadratically independent set with respect to S. Then there exists an isogenous representation ρ' such that $\rho'(\sigma) \equiv \mathbf{I} \pmod{2^{k+1}}$ for all $\sigma \in G_K$.

Proof. First, by Lemma 7.1, the first condition implies that $\det(\rho(\sigma)) \equiv 1 \pmod{2^{k+1}}$ for all $\sigma \in G_K$.

Next we use the notation of the previous section, specifically (14). The determinant condition just established shows that $a + d \equiv 0 \pmod 2$ and we are in the case $\Delta_{\det} = 1$ as in subsection 6.3 with $\mathbf{u} = \mathbf{v}$. Next, $F_{\mathfrak{p}}(1) \equiv 0 \pmod{2^{2k+2}}$ means that all the test function values are 0. This gives in turn $\mathbf{W} = \mathbf{0}$, $\mathbf{y} = \mathbf{0}$ and $\mathbf{u} = \mathbf{v} = \mathbf{0}$. Finally we have $bc_1 \equiv 0 \pmod 2$ so (applying a 2-isogeny if necessary) we may assume that $b \equiv 0$, so $\mathbf{x} = \mathbf{0}$. Hence all the characters are trivial, as required. □

Using this proposition, we can prove our final result.

Theorem 7.3. *Let $\rho\colon G_K \to \mathrm{GL}_2(\mathbb{Z}_2)$ be a continuous Galois representation unramified outside S which is residually reducible. If*

1. $\det(\rho(\operatorname{Frob}\mathfrak{p})) = 1$ *for all* $\mathfrak{p} \in T_1$*, and*
2. $\operatorname{tr}(\rho(\operatorname{Frob}\mathfrak{p})) = 2$ *for all* $\mathfrak{p} \in T_2$*,*

(in particular, if $\operatorname{Frob}\mathfrak{p}$ *has characteristic polynomial* $(t-1)^2$ *for all* $\mathfrak{p} \in T_2$*), then* ρ *is reducible, with trivial semisimplification, and is of the form*

$$\rho(\sigma) = \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix}$$

with respect to a suitable basis.

Proof. Suppose that ρ were irreducible; then $\mathrm{BT}(\rho)$ is finite, and none of the finitely many integral forms ρ_Λ is trivial (otherwise ρ would be) so there is a maximal $k \geq 1$ such that ρ_Λ is trivial modulo 2^k for some stable lattice Λ. This contradicts Proposition 7.2. Hence ρ is reducible.

With respect to a suitable basis all the matrices $\rho(\sigma)$ are upper triangular. The diagonal entries determine characters of G_K, which are both trivial on $\operatorname{Frob}\mathfrak{p}$ for all $\mathfrak{p} \in T_1$ (since the product of their values is 1 and their sum 2). By Theorem 3.4 both diagonal characters are trivial. □

8 Further examples

We finish by presenting two examples with base field $K = \mathbb{Q}(\sqrt{-1})$, where the Black Box Galois representations come from Bianchi modular newforms with rational Hecke eigenvalues. The existence of suitable Galois representations in this case was first developed by Taylor *et al.* in [8], [14] with subsequent results by Berger and Harcos in [2]. For our purposes we only need the existence of the representation and the knowledge that it is unramified outside the primes dividing the level of the newform, with the determinant and trace of Frobenius at an unramified prime $\mathfrak{p}$ equal to the norm $N(\mathfrak{p})$ and the Hecke eigenvalue $a_\mathfrak{p}$ respectively. These eigenvalues were computed in these examples using the methods of [5]. The newforms we use here are in the LMFDB [11] and may be found at `http://www.lmfdb.org/ModularForm/GL2/ImaginaryQuadratic/`.

In both these examples (as in several hundred thousand others we have) there exist elliptic curves defined over K whose 2-adic Galois representation can be proved to be equivalent to the representation attached to the newform, using the Serre-Faltings-Livné method as detailed in [7]. However in preparing the examples we did not use the elliptic curves themselves, but used modular symbol methods to obtain the traces of Frobenius as Hecke eigenvalues. As $\det(\rho(\operatorname{Frob}\mathfrak{p})) = N(\mathfrak{p})$ and we include the prime above 2 in S, for $K = \mathbb{Q}(\sqrt{-1})$ we always have $N(\mathfrak{p}) \equiv 1 \pmod 4$, and hence the determinant of the representation is trivial modulo 4.

In this way we can obtain information about the elliptic curves conjecturally associated to a rational Bianchi newform, even in cases where we have not been able to find a suitable elliptic curve.

Example 2. The base field is $K = \mathbb{Q}(i)$, where we write $i = \sqrt{-1}$. The Galois representation we consider is that attached to the Bianchi newform with LMFDB label 2.0.4.1-3140.3-c (see `http://www.lmfdb.org/ModularForm/GL2/ImaginaryQuadratic/2.0.4.1/3140.3/c/`). Here, 2.0.4.1 is the LMFDB label for K; then 3140.3 is the label for the level $\mathfrak{N} = (56{+}2i) = (1{+}i)^2(1{+}2i)(11{+}6i)$ of norm 3140 (it is the 3rd ideal of this norm in the ordering used by the LMFDB). Finally the suffix c identifies the newform itself: the new space at level $\Gamma_0(\mathfrak{N})$ is three-dimensional with a basis of three newforms (labelled a, b and c) each with rational Hecke eigenvalues.

Let $S = \{1+i, 1+2i, 11+6i\}$ be the set of primes dividing the level, outside which the representation is unramified. Then

$$K(S,2) = \langle 1+i, 1+2i, 11+6i, i\rangle \cong (\mathbb{Z}/2\mathbb{Z})^4.$$

There is one C_3 extension of K unramified outside S, and 5 S_3 extensions, so we have a set $\mathcal{F}$ of 6 possible cubics. Using Algorithm 2 we find that a suitable distinguishing set is $T_0 = \{2+i, 2+3i, 3+2i, 1+4i\}$. Checking that $a_\mathfrak{p}$ is even for all $\mathfrak{p} \in T_0$ shows that the mod-2 representation is reducible.

Using Algorithm 5 we find the following set of ten primes forms a special quadratically independent set. (We only use primes of degree 1 here, noting that the cost of computing $a_\mathfrak{p}$ grows with $N(\mathfrak{p})$.)

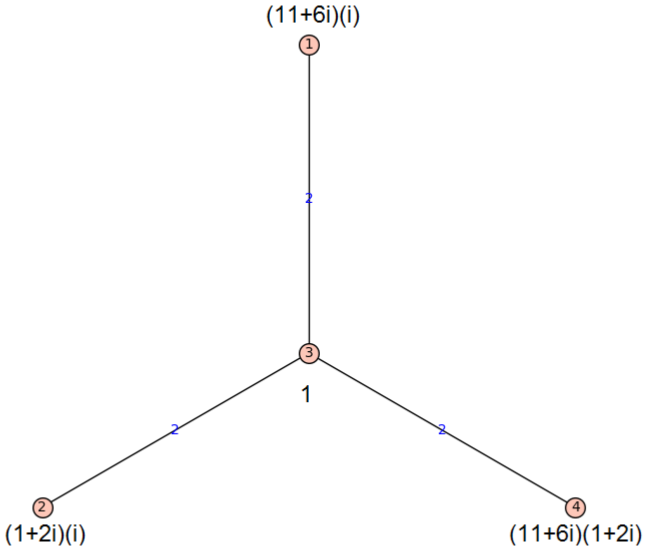
I	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{1,2\}$	$\{1,3\}$	$\{1,4\}$	$\{2,3\}$	$\{2,4\}$	$\{3,4\}$
$\mathfrak{p}_I$	$(1+4i)$	$(4+5i)$	$(8+7i)$	$(5+2i)$	$(4+i)$	$(5+8i)$	$(6+i)$	$(5+4i)$	$(2+i)$	$(2+3i)$
$a_\mathfrak{p}$	2	10	10	6	2	-14	-2	-2	2	-6
$F_\mathfrak{p}(1)$	16	32	104	24	16	104	40	44	4	20
$t_1(\mathfrak{p})$	0	0	0	0	0	0	0	0	0	0
$t_2(\mathfrak{p})$	0	0	0	0	0	0	0	1	1	1

Applying the test $t_1(\mathfrak{p})$, given by (10), amounts to testing whether each $a_\mathfrak{p} \equiv 0$ or $2 \pmod 4$; here, all $a_\mathfrak{p} \equiv 2 \pmod 4$. (In the notation of subsection 5.2, we have $\mathbf{v} = \mathbf{0}$.) This implies that the width of the isogeny class is at least 2; we have a large isogeny class.

To determine whether the width of the isogeny class is actually 2, we apply the test $t_2(\mathfrak{p})$, given by (16) (since the determinant is trivial mod 4) with $k = 1$. Using the method of subsection 6.3 we construct the matrix

$$\mathbf{W} = \begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix}$$

which has rank 2, so (without loss of generality) we take $\mathbf{x} = (0,0,1,1)$, $\mathbf{y} = (0,1,0,1)$ (two distinct non-zero rows of $\mathbf{W}$) and $\mathbf{z} = \mathbf{x} + \mathbf{y} = (0,1,1,0)$. Then from (19) we find that $\mathbf{u} = \mathbf{v} = (0,0,0,1)$. Therefore $\Delta_b = (11+6i)(i)$, $\Delta_c = (1+2i)(i)$, $\Delta_{abcd} = (11+6i)(1+2i)$. So in this case the stable Bruhat-Tits tree (see Figure A1) has four vertices, with discriminants as shown here:



We can match the data presented in this example to the isogeny class 2.0.4.1-3140.3-c of elliptic curves of conductor $\mathfrak{N}$ over $\mathbb{Q}(i)$. See http://www.lmfdb.org/EllipticCurve/2.0.4.1/3140.3/c/ for details of the four elliptic curves in the class: one (with label c3) has full K-rational 2-torsion, while each of the others (labelled c1,c2,c4) has a single K-rational point of order 2 as expected. Moreover the discriminants of the other three curves are (up to square factors) $i(11+6i)$, $i(1+2i)$ and $(1+2i)(11+6i)$ respectively.

Example 3. Again with $K = \mathbb{Q}(i)$ as base field, let $S = \{1+i, 2+i, 2-i\}$. For this example we take the Bianchi newform with LMFDB label 2.0.4.1-200.2-a with level $\mathfrak{N} = (10+10i) = (1+i)^3(2+i)(2-i)$ of norm 200 (see http://www.lmfdb.org/ModularForm/GL2/ImaginaryQuadratic/2.0.4.1/200.2/a/), a base-change of a classical newform on $\Gamma_0(40)$. Now

$$K(S,2) = \langle i, i+1, -i-2, 2i+1 \rangle \cong (\mathbb{Z}/4\mathbb{Z})^4;$$

we have put the unit i first since we will be using the method of subsection 6.4. Now $\mathcal{F}$ has only one element and $T_0 = \{4+i\}$. Since $a_{4+i} = 2$ the representation is residually reducible.

We find T_2 as before and obtain the following data from the newform, acting as our Black Box:

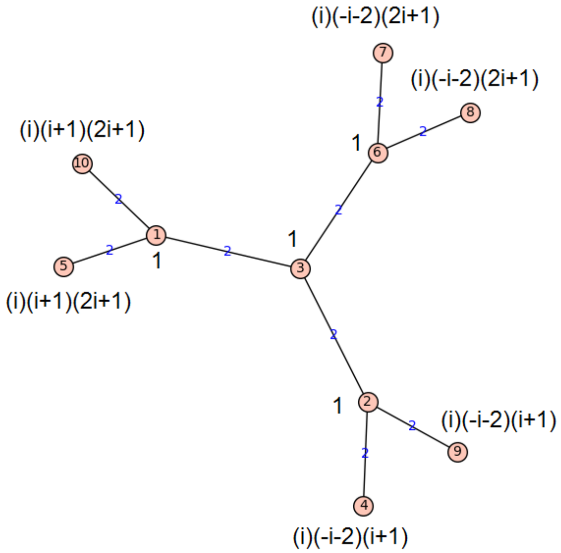
I	$\{1\}$	$\{2\}$	$\{3\}$	$\{4\}$	$\{1,2\}$	$\{1,3\}$	$\{1,4\}$	$\{2,3\}$	$\{2,4\}$	$\{3,4\}$
$\mathfrak{p}$	$(2+3i)$	$(5+8i)$	$(8+7i)$	$(7+8i)$	$(6+i)$	$(5+2i)$	$(6+5i)$	$(1+4i)$	$(4+i)$	$(4+5i)$
$N(\mathfrak{p})$	13	89	113	113	37	29	61	17	17	41
$a_{\mathfrak{p}}$	-2	-6	18	18	6	-2	-2	2	2	-6
$F_{\mathfrak{p}}(1)$	16	96	96	96	32	32	64	16	16	48
$t_4(\mathfrak{p})$	1	0	0	0	0	0	0	1	1	1

Since $t_k(\mathfrak{p}) = 0$ for all $\mathfrak{p} \in T_2$ for $k = 1, 2, 3$ we see that not only is ρ residually reducible, it is even trivial modulo 4 (up to isogeny). Fixing a stable lattice with respect to which ρ is trivial mod 4, we will determine $\rho \pmod 8$, noting that it does not have trivial determinant, as some primes have norm $\not\equiv 1 \pmod 8$.

Using the method of subsection 6.4, we evaluate $t_4(\mathfrak{p})$ for $\mathfrak{p} \in T_2$ (see the last row of the table above). From this we evaluate the 3×3 matrix

$$\boldsymbol{W}' = \begin{pmatrix} 0 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

and observe that it has rank 2. Thus we may take $\mathbf{x}' = (0, 1, 1)$, $\mathbf{y}' = (1, 0, 1)$ and $\mathbf{z}' = (1, 1, 0)$. From $t_4(\mathfrak{p}_1) = 1$ we then get $x_1 = y_1 = z_1 = 1$, so $\mathbf{x} = (1, 0, 1, 1)$, $\mathbf{y} = (1, 1, 0, 1)$, and $\mathbf{z} = (1, 1, 1, 0)$. Using (25) gives $\mathbf{u}' = \mathbf{v}' = (0, 0, 1)$ so $\mathbf{u} = (1, 0, 0, 1)$, $\mathbf{v} = (0, 0, 0, 1)$, completing the determination of $\rho \pmod 8$: it is the full subgroup of $\mathrm{GL}_2(\mathbb{Z}/8\mathbb{Z})$ consisting of matrices congruent to the identity modulo 4. Since all of $\mathbf{x}$, $\mathbf{y}$, $\mathbf{z}$ are non-zero, we have also determined the entire isogeny class (stable Bruhat-Tits tree), and know that the discriminants of its leaves are (modulo squares) $\Delta_b = i(2+i)(1+2i)$, $\Delta_c = i(1+i)(1+2i)$ and $\Delta_{abcd} = i(1+i)(2+i)$. The isogeny graph therefore looks like this:



We can match the data presented in this example to the isogeny class 2.0.4.1-200.2-a of elliptic curves of conductor $\mathfrak{N}$ over $\mathbb{Q}(i)$. See `http://www.lmfdb.org/EllipticCurve/2.0.4.1/200.2/a/`. The class includes the base-change to K of isogeny class 40a of elliptic curves defined over $\mathbb{Q}$ with conductor 40; it consists of ten curves a1–a10 and the graph of 2-isogenies between them is as in this diagram, where the vertex labels match the number labels of the curves in the class. Consulting the LMFDB page cited, we can check that the discriminants of the ten curves are as indicated in the diagram (up to squares).

Acknowledgments

This work formed part of the 2016 PhD thesis [1] of the first author, during which he was supported by a Chancellor's Scholarship from the University of Warwick. The second author is supported by EPSRC Programme Grant EP/K034383/1 *LMF: L-Functions and Modular Forms*, and the Horizon 2020 European Research Infrastructures project *OpenDreamKit* (#676541).

References

[1] Alejandro Argáez García. Computational aspects of Galois representations. *PhD Thesis, University of Warwick*, 2016. (document), 8

[2] Tobias Berger and Gergely Harcos. l-adic representations associated to modular forms over imaginary quadratic fields. *Int. Math. Res. Not. IMRN*, 23:Art. ID rnm113, 16, 2007. 8

[3] Wieb Bosma, John Cannon, and Catherine Playoust. The Magma algebra system. I. The user language. *J. Symbolic Comput.*, 24(3-4):235–265, 1997. Computational algebra and number theory (London, 1993). 3.2

[4] Henri Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993. 4.1

[5] J. E. Cremona. Hyperbolic tessellations, modular symbols, and elliptic curves over complex quadratic fields. *Compositio Math.*, 51(3):275–324, 1984. 8

[6] The Sage Developers. *Sage Mathematics Software (Version 8.0)*, 2017. `http://www.sagemath.org`. 1, 3.2

[7] Luis Dieulefait, Lucio Guerberoff, and Ariel Pacetti. Proving modularity for a given elliptic curve over an imaginary quadratic field. *Math. Comp.*, 79(270):1145–1170, 2010. 4.1, 5.2, 8

[8] Michael Harris, David Soudry, and Richard Taylor. l-adic representations associated to modular forms over imaginary quadratic fields. I. Lifting to $\mathrm{GSp}_4(\mathbf{Q})$. *Invent. Math.*, 112(2):377–411, 1993. 8

[9] Angelos Koutsianas. Applications of S-unit Equations to the Arithmetic of Elliptic Curves. *PhD Thesis, University of Warwick*, 2016. 4.1

[10] Ron Livné. Cubic exponential sums and Galois representations. In *Current trends in arithmetical algebraic geometry (Arcata, Calif., 1985)*, volume 67 of *Contemp. Math.*, pages 247–261. Amer. Math. Soc., Providence, RI, 1987. 1, 5.5

[11] The LMFDB Collaboration. The L-functions and modular forms database. `http://www.lmfdb.org`, 2017. [Online; accessed 12 September 2017]. 1, 8

[12] J.-P. Serre. Résumé des cours au Collège de France. preprint, 1984. 1

[13] Jean-Pierre Serre. *Abelian l-adic representations and elliptic curves*. McGill University lecture notes written with the collaboration of Willem Kuyk and John Labute. W. A. Benjamin, Inc., New York-Amsterdam, 1968. 2.1, 2.1

[14] Richard Taylor. l-adic representations associated to modular forms over imaginary quadratic fields. II. *Invent. Math.*, 116(1-3):619–643, 1994. 8