THE ESSENTIAL DIMENSION OF CONGRUENCE COVERS

BENSON FARB, MARK KISIN AND JESSE WOLFSON

Abstract. Consider the algebraic function $\Phi_{g,n}$ that assigns to a general g-dimensional abelian variety an n-torsion point. A question first posed by Kronecker and Klein asks: What is the minimal d such that, after a rational change of variables, the function $\Phi_{g,n}$ can be written as an algebraic function of d variables?

Using techniques from the deformation theory of p-divisible groups and finite flat group schemes, we answer this question by computing the essential dimension and p-dimension of congruence covers of the moduli space of principally polarized abelian varieties. We apply this result to compute the essential p-dimension of congruence covers of the moduli space of genus g curves, as well as its hyperelliptic locus, and of certain locally symmetric varieties M.

Contents

1. Introduction

This article grew out an attempt to answer questions first raised by Kronecker and Klein.[1] Let K be a field of characteristic 0, and consider the algebraic function $\Phi_{g,n}$ that assigns to a general g-dimensional (principally polarized) abelian K-variety an n-torsion point.

The authors are partially supported by NSF grants DMS-1811772 (BF), DMS-0017749000 (MK) and DMS-1811846 (JW).

[1] See [Kl1888, p. 171], [Kr1861, p. 309] and [Bu1890, Bu1891, Bu1893], esp. the footnote to [Bu1891, Ch. 11] on p. 216, and the treatment in §51-55 that follows.

Question 1. *Let $g, n \geq 2$. What is the minimum d such that, after a rational change of variables, the function $\Phi_{g,n}$ can be written as an algebraic function of d variables?*

We can rephrase Question 1 in more modern language using the moduli space of principally polarized abelian varieties and the notion of *essential dimension* introduced by Buhler–Reichstein [BR97]. Let $\mathcal{A}_g$ denote the coarse moduli space of g-dimensional, principally polarized abelian varieties over K, and let $\mathcal{A}_{g,n}$ be the moduli space of pairs $(A, \mathcal{B})$ where $A \in \mathcal{A}_g$ and $\mathcal{B}$ is a basis for $H^1(A; \mathbb{Z}/n\mathbb{Z})$. The generically finite, étale map

$$\mathcal{A}_{g,n} \to \mathcal{A}_g$$

given by $(A, \mathcal{B}) \mapsto A$ corresponds to the Galois closure of the extension of functions fields $K(\mathcal{A}_g)[\Phi_{g,n}]/K(\mathcal{A}_g)$, generated by $\Phi_{g,n}$.

For any generically finite étale map $X' \to X$, define the *essential dimension* $\mathrm{ed}_K(X' \to X)$, or $\mathrm{ed}_K(X'/X)$ if the map is implicit, to be the minimal d for which $X' \to X$ is a pullback:

$$\begin{tikzcd} X' \arrow[r, dashed] \arrow[d] & Y' \arrow[d] \\ X \arrow[r, dashed, "f"] & Y \end{tikzcd}$$

of a generically finite dominant map $Y' \to Y$ of d-dimensional K-varieties via a rational map $f : X \dashrightarrow Y$. In this case we call f a *(rational) compression* of $p : X' \to X$. In terms of the function fields $K(X')$ and $K(X)$, the Primitive Element Theorem produces a monic, separable polynomial $h \in K(X)[T]$ so that

$$K(X') = K(X)[T]/(h).$$

One can think of $\mathrm{ed}_K(X'/X)$ as the smallest integer d such that a solution of $h(T) = 0$ is a function of d parameters on X. Because essential dimension is invariant under passing to a Galois closure [BR97, Lemma 2.3], Question 1 is equivalent to asking for $\mathrm{ed}_K(\mathcal{A}_{g,n} \to \mathcal{A}_g)$.

Following Klein [Kl1884], we can ask the related question where we allow certain *accessory irrationalities*; that is, we can ask for

$$\min_{E \to \mathcal{A}_g} \mathrm{ed}(\mathcal{A}_{g,n}|_E \to E)$$

for some class of generically finite maps $E \to \mathcal{A}_g$.[2] For example, the *essential p-dimension* $\mathrm{ed}_K(X'/X; p)$ is defined (see [RY00], Definition 6.3) as the minimum of $\mathrm{ed}_K(X' \times_X E \to E)$ where $E \to X$ runs over generically finite étale maps of K-varieties of degree prime to p.

In this paper we apply techniques from the deformation theory of p-divisible groups and finite flat group schemes to compute the essential p-dimension of congruence covers of certain locally symmetric varieties, such as $\mathcal{A}_g$.

Theorem 2. *Let $g, n \geq 2$, and let p be any prime with $p|n$. Then*

$$\mathrm{ed}_K(\mathcal{A}_{g,n}/\mathcal{A}_g; p) = \mathrm{ed}_K(\mathcal{A}_{g,n}/\mathcal{A}_g) = \dim \mathcal{A}_g = \binom{g+1}{2}.$$

[2] Given maps $X' \to X$ and $E \to X$, we use the notations $X'|_E$ and $X' \times_X E$ interchangeably to denote the fiber product.

Theorem 2 thus answers Question 1: the minimal d equals $\binom{g+1}{2}$. We in fact prove a more general result, that for subvarieties of $\mathcal{Z} \subset \mathcal{A}_g$ satisfying some mild technical hypotheses, $\mathrm{ed}_K(\mathcal{A}_{g,n}|_{\mathcal{Z}}/\mathcal{Z}) = \dim\mathcal{Z}$. More precisely, we prove the following (see Theorem 3.2.6 below).

Theorem 3. *Let p be prime. Suppose that $L = \bar{\mathbb{Q}}_p$, an algebraic closure of $\mathbb{Q}_p$, let $\mathcal{O}_L$ be its ring of integers and let k be its residue field. Let $\mathcal{Z} \subset \mathcal{A}_{g,n/\mathcal{O}_L}$ be a locally closed subscheme that is equidimensional and smooth over $\mathcal{O}_L$, and whose special fiber $\mathcal{Z}_k$ meets the ordinary locus $\mathcal{A}_{g,n}^{\mathrm{ord}} \subset \mathcal{A}_{g,n/k}$. Then*

$$\mathrm{ed}_L(\mathcal{A}_{g,p}|_{\mathcal{Z}_L}/\mathcal{Z}_L;p) = \mathrm{ed}_L(\mathcal{A}_{g,p}|_{\mathcal{Z}_L}/\mathcal{Z}_L) = \dim\mathcal{Z}_L.$$

We give three applications of Theorem 3. The first is an analogue of Theorem 2 for $\mathcal{M}_g$, the coarse moduli space of smooth, genus $g \geq 2$ curves over K. For any integer n, consider the *level n congruence cover* $\mathcal{M}_g[n] \to \mathcal{M}_g$, where $\mathcal{M}_g[n]$ denotes the moduli space of pairs $(C, \mathcal{B})$ consisting of a curve $C \in \mathcal{M}_g$ together with a choice $\mathcal{B}$ of basis for $H_1(C;\mathbb{Z}/n\mathbb{Z})$. Applying Theorem 3 and the Torelli theorem, we will deduce the following.

Corollary 4. *Let $g, n \geq 2$. Let p be any prime with $p \mid n$. Then*

$$\mathrm{ed}_K(\mathcal{M}_g[n]/\mathcal{M}_g) = \mathrm{ed}_K(\mathcal{M}_g[n]/\mathcal{M}_g;p) = \dim\mathcal{M}_g = 3g-3.$$

As a second application of Theorem 3, we answer a question encountered by Burkhardt in his study of hyperelliptic functions (see in particular [Bu1891, Ch. 11]). Let $\mathcal{H}_g$ denote the coarse moduli of smooth, hyperelliptic curves of genus $g \geq 2$ over K. For any integer n, consider the *level n congruence cover* $\mathcal{H}_g[n] \to \mathcal{H}_g$, where $\mathcal{H}_g[n]$ denotes the moduli space of pairs $(C, \mathcal{B})$ consisting of a curve $C \in \mathcal{H}_g$ together with a choice $\mathcal{B}$ of basis for $H_1(C;\mathbb{Z}/n\mathbb{Z})$. Analogously to the case of $\mathcal{M}_g$, we prove the following.

Corollary 5. *Let $g, n \geq 2$. Let $p \mid n$ be any odd prime. Then*

$$\mathrm{ed}_K(\mathcal{H}_g[n]/\mathcal{H}_g) = \mathrm{ed}_K(\mathcal{H}_g[n]/\mathcal{H}_g;p) = \dim\mathcal{H}_g = 2g-1.$$

The hypothesis that p is odd in Corollary 5 is necessary; see 3.3.5 below.

Our third application of Theorem 3 generalizes Theorem 2 to many locally symmetric varieties. Recall that a *locally symmetric variety* is a variety whose complex points have the form $\Gamma\backslash X$ where X is a Hermitian symmetric domain and Γ is an arithmetic lattice in the corresponding real semisimple Lie group (see 4.2.3 below). By a *principal p-level covering* $\Gamma_1\backslash X \to \Gamma\backslash X$ we mean that the definition of Γ does not involve any congruences at p, and $\Gamma_1 \subset \Gamma$ is the subgroup of elements that are trivial mod p. A sample of what we prove is the following (see Theorem 4.3.4 below for the most general statement).

Theorem 6. *With notation as just given, suppose that each irreducible factor of X is associated to (the adjoint group of) one of $U(n,n)$, $\mathrm{SO}(n,2)$ with $n \neq 6$, or $\mathrm{Sp}(2n)$ for some positive integer n. Then for any principal p-level covering $\Gamma_1\backslash X \to \Gamma\backslash X$, we have*

$$\mathrm{ed}(\Gamma_1\backslash X \to \Gamma\backslash X;p) = \dim X.$$

In fact our results apply to any Hermitian symmetric domain of classical type, but in general they require a condition on the $\mathbb{Q}$-group G giving rise to Γ; for example they apply if G splits over $\mathbb{Q}$. Note that these results include cases where the locally symmetric variety $\Gamma\backslash X$ is *proper*. As far as we know, these are the first examples of nontrivial lower bounds on the essential dimension of an unramified, non-abelian covering of a proper algebraic variety. The only prior result for unramified covers of proper varieties of which we are aware is due to Gabber [CT02, Appendix], who proved that if $\{E_i' \to E_i\}$ is a collection of connected, unramified $\mathbb{Z}/p\mathbb{Z}$ covers of elliptic curves E_i, then under certain conditions, the cover $E_1' \times \cdots \times E_r' \to E_1 \to \cdots E_r$ has essential dimension at p equal to r.

There are many examples of finite simple groups of Lie type for which our methods give a lower bound on the essential p-dimension of a covering of locally symmetric varieties with that group.

Corollary 7. *Let H be a classical, absolutely simple group over $\mathbb{F}_q$, with $q = p^r$. Then there is a congruence $H(\mathbb{F}_q)$-cover of locally symmetric varieties $Y' \to Y$ such that $e := \mathrm{ed}_K(Y'/Y;p)$ satisfies :*

- *If H is a form of PGL_n which is split if n is odd, then $e = r\lfloor \frac{n^2}{4} \rfloor$.*
- *If H is PSp_{2n} then $e = r(\frac{n^2+n}{2})$.*
- *If H is a split form of PO_{2n} then $e = r(\frac{n^2-n}{2})$.*
- *If H is a form of PO_n and H is not of type D_4, then $e = r(n-2)$.*

Historical Remarks.

(1) The study of essential dimension originates in Hermite's study of the quintic [He1858], Kronecker's response to this [Kr1861], and Klein's "Resolvent Problem" (see [Kl1893, Lecture IX] and [Kl1884] esp. Part II, Ch. 1.7, as well as [Kl1887], [Kle05], and more generally the papers [Kle22, p. 255-506]; see also [Tsc43]). Following Buhler-Reichstein [BR97], the last two decades have seen an array of computations, new methods, generalizations, and applications of this invariant (see [Rei10] or [Mer17] for recent surveys), but computations to date have largely focused on a different set of problems than those we consider here.

(2) In contrast to Kronecker, Klein also advocated for the consideration of accessory irrationalities as a "characteristic feature" of higher degree equations, and called upon his readers to "fathom the nature and significance of the necessary accessory irrationalities." [Kl1884, p. 174, Part II, Ch.1.7] While essential dimension at p partially answers this call, a full answer requires the notion of *resolvent degree* $RD(X \to Y)$, which asks for the minimum d such that an algebraic function admits a formula using only algebraic functions of d or fewer variables (see [FW17]). At present, we do not know of a single example which provably has $RD(X \to Y) > 1$.

Idea of Proof. To prove Theorem 2 and its generalization to subvarieties, we use arithmetic techniques, and specifically Serre-Tate theory, which describes the deformation theory of an ordinary abelian variety in characteristic p in terms of its p-divisible group. Let $\mathcal{A}$ denote the universal abelian scheme over $\mathcal{A}_g$ (now considered over $\mathbb{Z}$), let $\mathcal{A}[p]$ be its p-torsion group scheme, and let $\mathcal{A}_x$ denote the fiber of $\mathcal{A}$ at x. Given a rational compression of $\mathcal{A}_{g,p} \to \mathcal{A}_g$ (in characteristic 0) onto a smaller-dimensional variety, we show that there is an ordinary mod p point x of $\mathcal{A}_g$, and a tangent direction t_x at x, such that the deformation of $\mathcal{A}_x[p]$ corresponding to t_x is trivial. From this we deduce that the deformation of $\mathcal{A}_x$ corresponding to t_x is trivial, a contradiction.

One might view our method as an arithmetic analogue of the "fixed point method" in the theory of essential dimension (see [Rei10]), where the role of fixed points for a group action is now played by wild ramification at a prime. In the fixed point method one usually works over a field where the order of the group is invertible. In contrast, for us the presence of wild ramification plays an essential role.

Acknowledgements. We thank Zinovy Reichstein for detailed comments on an earlier version of this paper and for extensive helpful correspondence. We thank Eric Rains and Alexander Polishchuk for a useful discussion on hyperelliptic curves. We thank Burt Totaro and Maxime Bergeron for helpful comments on a draft, we also thank Burt Totaro for calling Gabber's result to our attention.

2. Preliminary results

2.1. **Finite étale maps.** We begin with some general lemmas on finite étale maps.

2.1.1. Let X be a scheme, and $f : Y \to X$ a finite étale cover. In the next three lemmas we consider a map of schemes $g : X \to X'$ and a finite étale cover $f' : Y' \to X'$ such that $Y \xrightarrow{\sim} Y' \times_{X'} X$.

Lemma 2.1.2. *If f is Galois, then there is an finite étale $h : X'' \to X'$ such that g factors through X'' and $Y'' = X'' \times_X Y' \to X''$ is Galois.*

Proof. We may assume that X and X' are connected. We write $\pi_1(X)$ for the étale fundamental group, with a choice of base point which we suppress from the notation.

The finite cover f' corresponds to a finite set $S_{Y'}$ with an action of $\pi_1(X')$, and f corresponds to $S_{Y'}$ with the induced action of $\pi_1(X)$. Let N denote the open subgroup of $\pi_1(X')$ corresponding to the Galois closure of f', and let $H \subset \pi_1(X')$ denote the subgroup generated by the image of $\pi_1(X)$ and N. We denote by $X'' \to X'$ the finite étale cover corresponding to H.

Now $X'' \to X'$ corresponds to a finite set $S_{X''}$ with $\pi_1(X')$-action, on which H acts trivially. In particular, $\pi_1(X)$ acts trivially on $X \times_{X'} X''$, which implies that this cover of X is completely split, so that g factors through X''.

Now Y'' corresponds to H acting on $S_{Y'}$. For any $s \in S_{Y'}$, N fixes s, and the stabilizer $G_s \subset \pi_1(X)$ of s is a normal subgroup, which is independent of s, since f is Galois. Since N is normal in H, the stabilizer H_s of s in H, is generated by N and the image of G_s. In particular, H_s is independent of s and hence is normal in H. This implies that Y''/X'' is Galois. □

2.1.3. Let A be a finite ring. Recall that an A-local system $\mathcal{F}$ on X is an étale sheaf of A-modules which is locally isomorphic to the constant A-module A^n for some n. Such an $\mathcal{F}$ is representable by a finite étale map $Y(\mathcal{F}) \to X$. This is clear étale locally on X, and follows from étale descent in general. Isomorphism classes of A-local systems are in bijective correspondence with equivalence classes of representations $\pi_1(X) \to \mathrm{GL}_n(A)$.

For $X \to X_1$ a map of schemes, and $\mathcal{F}$ an A-local system on X_1, we will denote by $\mathcal{F}|_X$ the pullback of $\mathcal{F}$ to X. It will be convenient to continue to use the notation introduced in Lemma 2.1.2 in the proofs of the next two lemmas. In particular, we have the cover $X'' \to X$ corresponding to the group H.

Lemma 2.1.4. *Suppose that $f : Y = Y(\mathcal{F}) \to X$ corresponds to an A-local system $\mathcal{F}$. Then there is a finite étale $h : X'' \to X'$ such that g factors through X'' and $Y'' = X'' \times_X Y' \to X''$ represents an A-local system $\mathcal{F}''$, with $\mathcal{F}''|_X \xrightarrow{\sim} \mathcal{F}$.*

Proof. The finite set $S_{Y'}$ naturally has the structure of a finite free A-module on which $\pi_1(X)$ acts A-linearly. Since N acts trivially on $S_{Y'}$, the group $H = \pi_1(X'')$ acts A-linearly on $S_{Y'}$, so $Y'' \to X''$ represents an A-local system whose pullback to X is $\mathcal{F}$. □

2.1.5. For any integer $N \geq 1$ we denote by μ_N the kernel of $\mathbb{G}_m \xrightarrow{N} \mathbb{G}_m$. This is a finite flat group scheme on $\mathbb{Z}$, and we denote by the same symbol its pullback to any scheme X. This pullback is étale if any only if X is a $\mathbb{Z}[1/N]$-scheme.

For any $\mathbb{Z}/N\mathbb{Z}$ algebra A, we again denote by μ_N the fppf sheaf $\mu_N \otimes_{\mathbb{Z}/N\mathbb{Z}} A$. For any non-negative integer i we write $\mu_N^{\otimes i}$ for the fppf sheaf on X given by the i-fold tensor product of μ_N over $\mathbb{Z}/N\mathbb{Z}$. For i negative we set $\mu_N^{\otimes i}$ equal to the $\mathbb{Z}/N\mathbb{Z}$-linear dual of $\mu_N^{\otimes -i}$.

Lemma 2.1.6. *Let $N \geq 1$ be an integer, i, j integers, and A a finite $\mathbb{Z}/N\mathbb{Z}$-algebra. Suppose that X is a $\mathbb{Z}[1/N]$-scheme and that $f : Y = Y(\mathcal{F}) \to X$ corresponds to an A-local system $\mathcal{F}$, which is an extension of $(\mu_N^{\otimes i})^h$ by $(\mu_N^{\otimes j})^g$, for some positive integers h, g.*

Then there is a finite étale map $X'' \to X'$ such that g factors through X'' and the cover $Y'' = X'' \times_X Y' \to X''$ represents an A-local system $\mathcal{F}''$, which is an extension of $(\mu_N^{\otimes i})^h$ by $(\mu_N^{\otimes j})^g$, with $\mathcal{F}''|_X \xrightarrow{\sim} \mathcal{F}$ as extensions.

Proof. Replacing $\mathcal{F}$ by $\mathcal{F} \otimes \mu_N^{\otimes -j}$, we may suppose that $j = 0$. By Lemma 2.1.4, Y'' represents an A-local system and $g^*(\mathcal{F}') \xrightarrow{\sim} \mathcal{F}$ as A-local systems. Let $\mathcal{F}_1 \subset \mathcal{F}$ denote the sub A-local system corresponding to $(\mu_N^{\otimes j})^g$, so that $\mathcal{F}_1$ corresponds to an A-submodule $S_{Y',1} \subset S_{Y'}$.

Since the group H acts trivially on $S_{Y',1}$, after replacing X' by X'', we may assume that $\mathcal{F}'$ is an extension of $\mathcal{F}'/(\mu_N^{\otimes i})^h$, by $(\mu_N^{\otimes j})^g$, and $g^*(\mathcal{F}') \xrightarrow{\sim} \mathcal{F}$ is an isomorphism of extensions. A similar argument, applied to $\mathcal{F}/(\mu_N^{\otimes j})^g \otimes \mu_N^{-\otimes i}$, shows that we may assume that $\mathcal{F}'$ is an extension of $(\mu_N^{\otimes i})^g$ by $(\mu_N^{\otimes j})^g$, with $\mathcal{F}'|_X \xrightarrow{\sim} \mathcal{F}$ as extensions. □

2.2. Essential dimension.

2.2.1. Let K be a field, X a K-scheme of finite type, and $f : Y \to X$ a finite étale cover. The *essential dimension* [BR97, §2] $\mathrm{ed}_K(Y/X)$ of Y over X is the smallest integer e such that there exists a finite type K-scheme W of dimension e, a dense open subscheme $U \subset X$, and a map $U \to W$, such that $Y|_U$ is the pullback of an finite étale covering over W. The *essential p-dimension* $\mathrm{ed}_K(Y/X; p)$ is defined as the minimum of $\mathrm{ed}_K(Y \times_X E/E)$ where $E \to X$ runs over dominant, generically finite maps, which have degree prime to p at all generic points of X.

Lemma 2.2.2. *Let A be a finite ring, K a field, $\mathcal{F}$ an A-local system on a connected K-scheme X, and $\rho_{\mathcal{F}} : \pi_1(X) \to \mathrm{GL}_n(A)$ the representation corresponding to $\mathcal{F}$. Let Y' be the covering of X corresponding to* $\ker \rho_{\mathcal{F}}$.

Then Y' is the composite of the Galois closures of the connected components of $Y(\mathcal{F})$. In particular,

$$\mathrm{ed}_K(Y'/X) = \mathrm{ed}_K(Y(\mathcal{F})/X).$$

For any prime p we also have

$$\mathrm{ed}_K(Y'/X;p) = \mathrm{ed}_K(Y(\mathcal{F})/X;p).$$

Proof. Consider the action of $\pi_1(X)$ on A^n corresponding to $\mathcal{F}$. The connected components of $Y(\mathcal{F})$ correspond to the stabilizers $\pi_1(X)_s$ for $s \in A^n$. The Galois closure of such a component corresponds to

$$\cap_{g\in\pi_1(X)} g\pi_1(X)_s g^{-1} = \cap_{g\in\pi_1(X)}\pi_1(X)_{gs}.$$

Thus the composite of the Galois closures corresponds to $\cap_s \pi_1(X)_s = \ker \rho_{\mathcal{F}}$.

This implies [BR97, lem. 2.3] that $\mathrm{ed}_K(Y'/X) \geq \mathrm{ed}_K(Y(\mathcal{F})/X)$. For the converse suppose that $U \subset X$ is dense open, and let $g: U \to W$ be a map such that $Y(\mathcal{F})|_U$ is the pullback of a finite cover of W and $\dim W = \mathrm{ed}_K(Y(\mathcal{F})/X)$. By Lemma 2.1.4 we may assume that $\mathcal{F}$ is the pullback of an A-local system $\mathcal{F}'$ on W. Then $\rho_{\mathcal{F}}$ arises from the corresponding representation $\rho_{\mathcal{F}'}$, so $Y'|_U$ is the pullback of a finite cover of W.

The claim involving essential p-dimension, follows by applying the above arguments after pulling back by a cover $E \to X$ of degree prime to p. In particular, note that $Y'|_E$ is a disjoint union of coverings corresponding to the representation $\rho|_{\pi_1(E)}$. □

Lemma 2.2.3. *Let $K' \subset K$ be algebraically closed fields of characteristic* 0. *If $Y \to X$ is a finite étale covering of K'-schemes then*

$$\mathrm{ed}_{K'}(Y/X) = \mathrm{ed}_K(Y_K/X_K).$$

Proof. Let $U_K \subset X_K$ be a dense open and $U_K \to W_K$ a morphism with $\dim W_K = \mathrm{ed}_K(Y_K/X_K)$ such that $Y_K|_{U_K}$ arises from a finite cover $f': Y'_K \to W_K$. Then U_K, the finite cover f' and the isomorphism $f'^*Y'_K \xrightarrow{\sim} Y_K|_{U_K}$ are all defined over some finitely generated K'-algebra $R \subset K$. Specializing by a map $R \to K'$ produces the required data for the covering $Y \to X$. □

2.2.4. It will be convenient to make the following definition. Suppose that $Y \to X$ is a finite étale covering over a field K of characteristic 0. We set $\mathrm{ed}(Y/X) = \mathrm{ed}_{\bar{K}}(Y/X)$ where $\bar{K}$ is any algebraically closed field containing K. By Lemma 2.2.3 this does not depend on the choice of $\bar{K}$.

Lemma 2.2.5. *Let K be an algebraically closed field, and $Y \to X$ a finite Galois covering of connected K-schemes with Galois group G. Let $H \subset G$ be a normal, cyclic subgroup of order n with* $\mathrm{char}(K) \nmid n$. *Then for any prime $p \nmid n$ we have*

$$\mathrm{ed}(Y/X;p) = \mathrm{ed}(Y/H \to X;p)$$

Proof. To show $\mathrm{ed}(Y/X;p) \geq \mathrm{ed}(Y/H \to X;p)$, after shrinking X, we may assume there is a map $f: X \to X'$ such that $Y = f^*Y'$ for a finite étale covering $Y' \to X'$, which may be assumed to be connected and Galois by Lemma 2.1.2. The Galois group of Y'/X' is necessarily equal to G, and we have $f^*(Y'/H) \xrightarrow{\sim} Y/H$.

For the converse inequality, we may assume there is a map $f: X \to X'$ such that $Y/H = f^*Y'$ for a finite étale covering $Y' \to X'$, which we may again assume is connected and Galois with group G/H. The image, c, of $Y' \to X'$ under

$$H^1(X', G/H) \to H^2(X', H) \xrightarrow{\sim} H^2(X', \mu_n)$$

is the obstruction to lifting $Y' \to X'$ to a G-covering. Here, for the final isomorphism, we are using that K is algebraically closed of characteristic prime to n.

Viewing c as a Brauer class, we see that it has order dividing n. This implies that (after perhaps shrinking X further) there is a Galois covering $X'_1 \to X'$ of order a power n such that $c|_{X_1}$ is trivial [FD93, Lemma 4.17]. In particular, $X'_1 \to X'$ has prime to p order. Replacing $Y \to X \to X'$ by their pullbacks to X'_1, we may assume that $c = 0$, and that $Y' = Y''/H$ for some Galois covering $Y'' \to X'$ with group G.

The difference between the G-coverings $Y \to X$ and $f^*Y'' \to X$ is measured by a class in $H^1(X, H)$. After replacing X by the H-covering corresponding to this class, we may assume that this class is trivial, and so $Y \xrightarrow{\sim} f^*Y''$. This shows that $\mathrm{ed}(Y/X; p) \leq \mathrm{ed}(Y/H \to X; p)$, □

3. Essential dimension and moduli of abelian varieties

3.1. **Ordinary finite flat group schemes.** In this subsection, we fix a prime p, and we consider a complete discrete valuation ring V of characteristic 0, with perfect residue field k of characteristic p, and a uniformizer $\pi \in V$.

By a *finite flat group scheme* on a $\mathbb{Z}_p$-scheme X we will always mean a finite flat group scheme on X of p-power order. A finite flat group scheme on X is called *ordinary* if étale locally on X, it is an extension of a constant group scheme $\oplus_{i\in I}\mathbb{Z}/p^{n_i}\mathbb{Z}$ by a group scheme of the form $\oplus_{j\in J}\mu_{p^{m_j}}$ for integers $n_i, m_j \geq 1$. In this subsection we study the classification of these extensions.

3.1.1. Now let $\tilde{X} = \operatorname{Spec} A$ be an affine $\mathbb{Z}_p$-scheme, and set $X = \tilde{X} \otimes \mathbb{Q}$. Let $n \geq 1$, and consider the exact sequence of sheaves

$$1 \to \mu_{p^n} \to \mathbb{G}_m \xrightarrow{p^n} \mathbb{G}_m \to 1$$

in the flat topology of $\tilde{X}$. Taking flat cohomology of this sequence and its restriction to X we obtain a commutative diagram with exact rows

$$\begin{tikzcd}
1 \arrow[r] & A^\times/(A^\times)^{p^n} \arrow[r] \arrow[d] & H^1(\tilde{X}, \mu_{p^n}) \arrow[r] \arrow[d] & H^1(\tilde{X}, \mathbb{G}_m) \arrow[d] \\
1 \arrow[r] & A[1/p]^\times/(A[1/p]^\times)^{p^n} \arrow[r] & H^1(X, \mu_{p^n}) \arrow[r] & H^1(X, \mathbb{G}_m)
\end{tikzcd}$$

The group $H^1(\tilde{X}, \mathbb{G}_m)$ classifies line bundles on $\tilde{X}$. Hence, if A is local it vanishes, and this can be used to classify extensions of $\mathbb{Z}/p^n\mathbb{Z}$ by μ_{p^n} as finite flat group schemes. We have

$$\mathrm{Ext}^1_{\tilde{X}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) \xrightarrow{\sim} H^1(\tilde{X}, \mu_{p^n}) \xrightarrow{\sim} A^\times/(A^\times)^{p^n}.$$

Similarly, we can classify extensions of $\mathbb{Q}_p/\mathbb{Z}_p$ by $\mu_{p^\infty} = \lim_n \mu_{p^n}$ as p-divisible groups:

$$\hat{\theta}_A : \mathrm{Ext}^1_{\tilde{X}}(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) \xrightarrow{\sim} \varprojlim_n A^\times/(A^\times)^{p^n} = A^{\times,1},$$

where $A^{\times,1} \subset A^\times$ denotes the subgroup of units which map to 1 in $k^\times$.

3.1.2. For the rest of this subsection we assume that $A = V[\![x_1, \dots, x_n]\!]$. Then $H^1(X, \mathbb{G}_m) = 0$ by [Gro68, Thm 3.13], and we have a commutative diagram

$$\begin{tikzcd}
A^\times/(A^\times)^{p^n} \arrow[r, "\sim"] \arrow[d] & H^1(\tilde{X}, \mu_{p^n}) \arrow[d] \\
A[1/p]^\times/(A[1/p]^\times)^{p^n} \arrow[r, "\sim"] & H^1(X, \mu_{p^n})
\end{tikzcd}$$

3.1.3. We call an element of $\mathrm{Ext}^1_X(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) = H^1(X, \mu_{p^n})$ *syntomic* if it arises from an element of $A^\times$, or equivalently from a class in $\mathrm{Ext}^1_{\tilde{X}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$, and we denote by $\mathrm{Ext}^{1,\mathrm{syn}}_X(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n}) \subset \mathrm{Ext}^1_X(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$ the subgroup of syntomic elements.

Lemma 3.1.4. *A syntomic class in* $\mathrm{Ext}^1_X(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$ *arises from a unique class in* $\mathrm{Ext}^1_{\tilde{X}}(\mathbb{Z}/p^n\mathbb{Z}, \mu_{p^n})$.

Proof. If $a \in A^\times$ is a $p^{n\mathrm{th}}$-power in $A[1/p]$ then it is a $p^{n\mathrm{th}}$ power in A, as A is normal. Hence the map $A^\times/(A^\times)^{p^n} \to A[1/p]^\times/(A[1/p]^\times)^{p^n}$ is injective, and the lemma follows from the description of Ext^1's above. □

Lemma 3.1.5. *Let* $B = V[\![y_1, \dots, y_s]\!]$ *for some integer* $s \geq 0$, *and*

$$f : \tilde{X} \to \tilde{Y} = \mathrm{Spec}\, B$$

a local flat map of complete local V*-algebras. Suppose that* $c \in H^1(Y, \mu_{p^n})$, *where* $Y = \mathrm{Spec}\, B[1/p]$, *and that* $f^*(c) \in H^1(X, \mu_{p^n})$ *is syntomic. Then* c *is syntomic.*

Proof. Let $b \in B[1/p]^\times$ be an element giving rise to c. Since B is a unique factorization domain we may write $b = b_0\pi^i$ with $b_0 \in B^\times$ and $i \in \mathbb{Z}$. Since $f^*(c)$ is syntomic, we may write $\pi^i = a_0 a^{p^n}$ with $a_0 \in A^\times$ and $a \in A[1/p]^\times$. Comparing the images of both sides in the group of divisors on A, one sees that $p^n | i$. So c arises from b_0. □

3.1.6. Let $\mathfrak{m}_A$ be the radical of A, and $\bar{\mathfrak{m}}_A$ its image in $A/\pi A$. The natural map

$$\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2 \overset{a \mapsto 1+a}{\to} k^\times \backslash A^\times/(\pi, \mathfrak{m}_A^2)$$

is a bijection; both sides are k-vector spaces spanned by $x_1, \dots, x_n$. We denote by θ_A the composite

$$\theta_A : \mathrm{Ext}^{1,\mathrm{syn}}_X(\mathbb{Z}/p\mathbb{Z}, \mu_p) \xrightarrow{\sim} A^\times/(A^\times)^p \to k^\times \backslash A^\times/(\pi, \mathfrak{m}_A^2) \xrightarrow{\sim} \bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2.$$

Here we have used Lemma 3.1.4 to identify $\mathrm{Ext}^{1,\mathrm{syn}}_X(\mathbb{Z}/p\mathbb{Z}, \mu_p)$ and $\mathrm{Ext}^1_{\tilde{X}}(\mathbb{Z}/p\mathbb{Z}, \mu_p)$.

Lemma 3.1.7. *With the notation of Lemma 3.1.5, suppose that*

$$L \subset \mathrm{Ext}^{1,\mathrm{syn}}_Y(\mathbb{Z}/p\mathbb{Z}, \mu_p)$$

is a subset such that the k*-span of* $\theta_A(f^*(L))$ *is* $\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2$. *Then* f *is an isomorphism.*

Proof. By functoriality of the association $A \mapsto \theta_A$, we have $\theta_A(f^*(L)) = f^*(\theta_B(L))$. Hence the k-span of $\theta_A(f^*(L))$ is contained in image of $\bar{\mathfrak{m}}_B/\bar{\mathfrak{m}}_B^2$. It follows that $\bar{\mathfrak{m}}_B/\bar{\mathfrak{m}}_B^2$ surjects onto $\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2$. Since A and B are complete local V-algebras, this implies that B, which is a subring of A, surjects onto A. Hence f is an isomorphism. □

3.2. **Monodromy of p-torsion in an abelian scheme.** We now use the results of the previous section to obtain results about the essential dimension of covers of of the moduli space of abelian varieties.

3.2.1. Recall that an abelian scheme $\mathcal{A}$ over a $\mathbb{Z}_p$-scheme is called ordinary if the group scheme $\mathcal{A}[p^n]$ is ordinary for all $n \geq 1$. This is equivalent to requiring the condition for $n = 1$.

Let k be an algebraically closed field of characteristic $p > 0$, and let V be a complete discrete valuation ring with residue field k, so that $W(k) \subset V$. Let $\mathcal{A}_0$ be an abelian scheme over k of dimension g. We assume that $\mathcal{A}_0$ is ordinary. Since k is algebraically closed, this implies that $\mathcal{A}_0[p^\infty]$ is isomorphic to $(\mathbb{Q}_p/\mathbb{Z}_p)^g \oplus \mu_{p^\infty}^g$.

Consider the functor $D_{\mathcal{A}_0}$ on the category of Artinian V-algebras C with residue field k, which attaches to C the set of isomorphism classes of deformations of $\mathcal{A}_0$ to an abelian scheme over C. Recall [Kat81, §2] that $D_{\mathcal{A}_0}$ is equivalent to the functor which attaches to C the set of isomorphism classes of deformations of $\mathcal{A}_0[p^\infty]$, and that $D_{\mathcal{A}_0}$ is pro-representable by a formally smooth V-algebra R of dimension g^2, called the universal deformation V-algebra of $\mathcal{A}_0$.

We denote by $\mathcal{A}_R$ the universal (formal) abelian scheme over R. Note that although $\mathcal{A}_R$ is only a formal scheme over R, the torsion group schemes $\mathcal{A}_R[p^n]$ are finite over R, and so can be regarded as genuine R-schemes.

Since $\mathcal{A}_0$ is ordinary the p-divisible group $\mathcal{A}_R[p^\infty] = \lim_n \mathcal{A}_R[p^n]$ is an extension of $(\mathbb{Q}_p/\mathbb{Z}_p)^g$ by $\mu_{p^\infty}^g$. Hence $\mathcal{A}_R[p]$ is an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g. This extension class is given by a $g \times g$ matrix of classes $(c_{i,j})$ with $c_{i,j} \in \mathrm{Ext}^1_R(\mathbb{Z}/p\mathbb{Z}, \mu_p)$.

Lemma 3.2.2. *With the notation of §3.1, the elements $\theta_R(\{c_{i,j}\}_{i,j})$ span $\bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$.*

Proof. Consider the isomorphism

$$\hat{\theta}_R : \mathrm{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty}) \xrightarrow{\sim} R^{\times,1}$$

introduced in §3.1. The universal extension of p-divisible groups over R gives rise to a $g \times g$ matrix of elements $(\hat{c}_{i,j}) \in \mathrm{Ext}^1_R(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty})$ which reduce to $(c_{i,j})$.

Let $L \subset \bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$ be the k-span of the images of the elements $\hat{\theta}_R(\hat{c}_{i,j}) - 1$, or equivalently, the elements $\theta_R(c_{i,j}) - 1$, and set $R' = k \oplus L \subset R/(\pi, \mathfrak{m}_R^2)$. Using the isomorphism $\hat{\theta}_{R'}$, one sees that $\mathcal{A}_R[p^\infty]|_{R/(\pi,\mathfrak{m}_R^2)}$ is defined over R'. If $L \subsetneq \bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$, then there exists a surjective map $R/(\pi, \mathfrak{m}_R^2) \to k[x]/x^2$ which sends L to zero. Specializing $\mathcal{A}_R[p^\infty]|_{R/(\pi,\mathfrak{m}_R^2)}$ by this map induces the trivial deformation of $\mathcal{A}_0[p^\infty]$ (that is the split extension of $(\mathbb{Q}_p/\mathbb{Z}_p)^g$ by μ_{p^∞}) over $\operatorname{Spec} k[x]/x^2$. This contradicts the fact that R pro-represents $D_{\mathcal{A}_0}$. Hence $L = \bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$, which proves the lemma. □

3.2.3. Let A be a quotient of R which is formally smooth over V. That is, A is isomorphic as a complete V-algebra to $V[\![x_1, \dots x_n]\!]$. As in §3.1, we set $X = \operatorname{Spec} A[1/p]$ and $\tilde{X} = \operatorname{Spec} A$.

Lemma 3.2.4. *Let $B = V[\![y_1, \dots y_s]\!]$ for some integer $s \geq 0$, and*

$$f : \tilde{X} \to \tilde{Y} = \operatorname{Spec} B$$

a local flat map of complete local V-algebras. Set $Y = \operatorname{Spec} B[1/p]$. Suppose that k is algebraically closed, and that there exists an $\mathbb{F}_p$-local system $\mathcal{L}$ on Y which is an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g such that $f^*\mathcal{L} \xrightarrow{\sim} \mathcal{A}_R[p]|_X$ as extensions of $\mathbb{F}_p$-local systems. Then f is an isomorphism.

Proof. Using the notation of 3.2.1, we have $\theta_R(\{c_{i,j}\}_{i,j})$ spans $\bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$ by Lemma 3.2.2. In particular, if we again denote by $c_{i,j}$ the restrictions of these classes to A, then $\theta_A(\{c_{i,j}\}_{i,j})$ spans $\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2$.

Now by Lemma 3.1.5 the g^2 extension classes defining $\mathcal{L}$ are syntomic. So $\mathcal{L}$ arises from an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g as finite flat group schemes over $\tilde{Y}$. If we denote by $(d_{i,j})$ the corresponding $g\times g$ matrix of elements of $\mathrm{Ext}^1_{\tilde{Y}}(\mathbb{Z}/p\mathbb{Z},\mu_p)$, then Lemma 3.1.4, together with the fact that $f^*\mathcal{L}\xrightarrow{\sim}\mathcal{A}_R[p]|_X$ implies that $f^*(d_{i,j})=c_{i,j}$. It follows that the elements $\theta_A(f^*(\{d_{i,j}\}))_{i,j}$ span $\bar{\mathfrak{m}}_A/\bar{\mathfrak{m}}_A^2$, which implies that f is an isomorphism by Lemma 3.1.7. □

3.2.5. Fix an integer $g\geq 1$, a prime $p\geq 2$, and a positive integer $N\geq 2$ coprime to p. We denote by $\mathcal{A}_{g,N}$ the $\mathbb{Z}[1/N]$-scheme which is the coarse moduli space principally polarized abelian varieties of dimension g with full level N structure. When $N\geq 3$, this is a fine moduli space which is smooth over $\mathbb{Z}[1/N]$. For a $\mathbb{Z}[1/N]$-algebra B, we denote by $\mathcal{A}_{g,N/B}$ the base change of $\mathcal{A}_{g,N}$ to B. If no confusion is likely to result we sometimes denote this base change simply by $\mathcal{A}_{g,N}$.

Let $\mathcal{A}\to\mathcal{A}_{g,N}$ be the universal abelian scheme. The p-torsion subgroup $\mathcal{A}[p]\subset\mathcal{A}$ is a finite flat group scheme over $\mathcal{A}_{g,N}$ which is étale over $\mathbb{Z}[1/Np]$. Let $x\in\mathcal{A}_{g,N}$ be a point with residue field $\kappa(x)$ of characteristic p, and $\mathcal{A}_x$ the corresponding abelian variety over $\kappa(x)$. The set of points x such that $\mathcal{A}_x$ is ordinary is an open subscheme $\mathcal{A}^{\mathrm{ord}}_{g,N}\subset\mathcal{A}_{g,N}\otimes\mathbb{F}_p$.

We now denote by k a perfect field of characteristic p, and $K/W[1/p]$ a finite extension with ring of integers $\mathcal{O}_K$ and uniformizer π.

Theorem 3.2.6. *Let $g\geq 1$ and let p be any prime. Let $N\geq 3$ and coprime to p, and let $\mathcal{Z}\subset\mathcal{A}_{g,N/\mathcal{O}_K}$ be a locally closed subscheme which is equidimensional and smooth over $\mathcal{O}_K$, and whose special fiber, $\mathcal{Z}_k$, meets the ordinary locus $\mathcal{A}^{\mathrm{ord}}_{g,N}\subset\mathcal{A}_{g,N/k}$. Then*

$$\mathrm{ed}(\mathcal{A}[p]|_{\mathcal{Z}_K}/\mathcal{Z}_K;p)=\dim\mathcal{Z}_K.$$

Proof. It suffices to prove the theorem when k is algebraically closed which we assume from now on. Moreover, since K is an arbitrary finite extension of $W[1/p]$, it is enough to show that $\mathrm{ed}_K(\mathcal{A}[p]|_{\mathcal{Z}_K}/\mathcal{Z}_K;p)=\dim\mathcal{Z}_K$. We may replace $\mathcal{Z}$ by a component whose special fibre meets the ordinary locus, and assume that $\mathcal{Z}_K$ and $\mathcal{Z}_k$ are geometrically connected.

Suppose that $\mathrm{ed}(\mathcal{A}[p]|_{\mathcal{Z}_K}/\mathcal{Z}_K;p)<\dim\mathcal{Z}_K$. Then there exists a dominant, generically finite map $U_K\to\mathcal{Z}_K$ of degree prime to p at the generic points of U_K, and a map $h:U_K\to Y_K$ to a finite type K-scheme Y_K with $\dim Y_K<\dim\mathcal{Z}_K$, such that $\mathcal{A}[p]|_{U_K}$ arises as the pullback of a finite étale covering of Y_K. We may assume that Y_K is the scheme-theoretic image of U_K under h. Next, after replacing both U_K and Y_K by dense affine opens, we may assume that both these schemes are affine corresponding to K-algebras B_K and C_K respectively, and that $U_K\to Y_K$ is flat.

Let $\tilde{\mathcal{Z}}$ be the normalization of $\mathcal{Z}$ in U_K. By Abhyankar's Lemma, after increasing K, we may assume that the map $\tilde{\mathcal{Z}}\to\mathcal{Z}$ is étale over the generic points of $\mathcal{Z}_k$. Shrinking U_K further if necessary, we may assume that there is an affine open $\operatorname{Spec}B=U\subset\tilde{\mathcal{Z}}$ such that $U_k\subset\mathcal{Z}_k$ is dense, $U\otimes K=U_K$, and $U\to\mathcal{Z}$ is étale. In particular, U is smooth over $\mathcal{O}_K$.

Now choose a finitely generated $\mathcal{O}_K$-subalgebra $C\subset C_K\cap B$ such that $C\otimes K=C_K$. This is possible as C_K is finitely generated over K. Then h extends to a map $h:U\to Y=\operatorname{Spec}C$. Let $J\supset(p)$ be an ideal of C, and $Y_J\to Y$ the blow up of J.

Denote by U_J the proper transform of U by this blow up. That is, U_J is the closure of U_K in $U \times Y_J$. By the Raynaud-Gruson flattening theorem, [RG71, Thm 5.2.2], we can choose J so that $U_J \to Y_J$ is flat. Since U is normal, the map $U_J \to U$ is an isomorphism over the generic points of $U \otimes k$. Hence, after replacing Y be an affine open in Y_J, and shrinking U, we may assume that $U \to Y$ is flat.

Shrinking U further, we may assume that the special fiber U_k maps to the ordinary locus of $\mathcal{A}_{g,N}$. Now let $\widehat{B}$ and $\widehat{C}$, denote the p-adic completions of B and C respectively, and set $\widehat{U} = \operatorname{Spec} \widehat{B}$ and $\widehat{Y} = \operatorname{Spec} \widehat{C}$. [3] Since $\mathcal{A}[p]|_{\widehat{U}}$ is ordinary, there is a finite étale covering $\widehat{U}' = \operatorname{Spec} \widehat{B}' \to \widehat{U}$ such that $\mathcal{A}[p]|_{\widehat{U}'}$ is an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g. Hence by Lemmas 2.1.4 and 2.1.6, $\widehat{U}'_K \to \widehat{Y}_K$ factors through a finite étale map $\widehat{Y}'_K \to \widehat{Y}_K$ such that $\mathcal{A}[p]|_{\widehat{U}'_K}$ is the pullback of an extension $\mathcal{F}'$ of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g on $\widehat{Y}'_K$. As $\widehat{U}'$ is normal, we may assume $\widehat{Y}'_K$ is normal.

Let $\widehat{Y}' = \operatorname{Spec} \widehat{C}'$ be the normalization of $\widehat{Y}$ in $\widehat{Y}'_K$. As $\widehat{U}'$ is normal, we have

$$\widehat{U}' \to \widehat{Y}' \to \widehat{Y}.$$

As $\widehat{Y}'$ is normal, $\widehat{U}' \to \widehat{Y}'$ is flat over the generic points of $\widehat{Y}'_k$. Hence, there exists $f_0 \in \widehat{C}'/\pi\widehat{C}'$ which is nowhere nilpotent on $\widehat{Y}'_k$, and such that $\widehat{U}'_k \to \widehat{Y}'_k$ is flat over the complement of the support of the ideal (f_0). Now let $f \in \widehat{C}'$ be a lift of f_0, and let $\widehat{C}'' = \widehat{C'[1/f]}$ and $\widehat{B}'' = \widehat{B'[1/f]}$, the p-adic completions [4] of $C'[1/f]$ and $B'[1/f]$. Let $\widehat{U}'' = \operatorname{Spec} B''$ and $\widehat{Y}'' = \operatorname{Spec} \widehat{C}''$. Then $\widehat{U}''$ is flat over $\widehat{Y}''$ by [Gro61, IV, 11.3.10.1]. Moreover, since $\widehat{U} \to \widehat{Y}$ is flat, the generic points of $\widehat{U}'_k$ map to generic points of $\widehat{Y}'_k$. So the image of $\widehat{U}''_k$ is dense in $\widehat{U}'_k$, and in particular $\widehat{U}''(k)$ is non-empty.

Finally, choose a point $x \in \widehat{U}''(k)$, and denote by $y \in \widehat{Y}''(k)$ its image. We write $\mathcal{O}_{\widehat{U}'',x}$ and $\mathcal{O}_{\widehat{Y}'',y}$ for the complete local rings at x and y. Since the maps

$$\widehat{U}'' \to \widehat{U}' \to \widehat{U} \to \mathcal{Z}$$

are formally étale, $\mathcal{O}_{\widehat{U}'',x}$ is naturally isomorphic to the complete local ring at the image of x in $\mathcal{A}_{g,N}$. Let R be the universal deformation $\mathcal{O}_K$-algebra of the abelian scheme $\mathcal{A}_x$. Then $\mathcal{O}_{\widehat{U}'',x}$ is naturally a quotient of R. The map $\mathcal{O}_{\widehat{Y}'',y} \to \mathcal{O}_{\widehat{U}'',x}$ satisfies the conditions of Lemma 3.2.4, (cf. [Gro61, IV, 17.5.3]) and it follows that this map is an isomorphism. In particular, this implies that

$$\dim Y_K = \dim \mathcal{O}_{\widehat{Y}'',y} - 1 = \dim \mathcal{O}_{\widehat{U}'',x} - 1 = \dim \mathcal{Z}_K$$

which contradicts our initial assumption. □

Corollary 3.2.7. *Let $g, n \geq 2$ and N a positive integer coprime to n. Consider the finite étale map of $\mathbb{Q}$-schemes $\mathcal{A}_{g,nN} \to \mathcal{A}_{g,N}$. Then for any $p \mid n$ we have*

$$\operatorname{ed}(\mathcal{A}_{g,nN}/\mathcal{A}_{g,N}; p) = \dim \mathcal{A}_g = \binom{g+1}{2}.$$

[3] Although it would in some sense be more natural to work with formal schemes here, we stay in world of affine schemes, so as to be able to apply the results proved in §1, and to deal with generic fibers without resorting to p-adic analytic spaces.

[4] $\widehat{C}''$ corresponds to a formal affine open in the formal scheme $\operatorname{Spf} \widehat{C}'$.

Proof. A fortiori it suffices to consider the case when $n = p$ is prime. When $N \geq 3$, this follows from Theorem 3.2.6.

For $N = 1, 2$ the map $\mathcal{A}_{g,pN} \to \mathcal{A}_{g,N}$, viewed over $\bar{\mathbb{Q}}$ corresponds to a covering with group $\mathrm{Sp}_{2g}(\mathbb{F}_p)/\{\pm 1\}$. More precisely, the geometrically connected components of $\mathcal{A}_{g,pN}$ are all quotients of such a covering. Let $N' \geq 3$ be an integer coprime to p, and N and consider the maps

$$\mathcal{A}_{g,pNN'} \to \mathcal{A}_{g,pN} \times_{\mathcal{A}_{g,N}} \mathcal{A}_{g,NN'} =: \mathcal{A}'_{g,pNN'} \to \mathcal{A}_{g,NN'}.$$

Then $\mathcal{A}'_{g,pNN'} \to \mathcal{A}_{g,NN'}$ again corresponds to a $\mathrm{Sp}_{2g}(\mathbb{F}_p)/\{\pm 1\}$ covering, and $\mathcal{A}_{g,pNN'} \to \mathcal{A}_{g,NN'}$ corresponds to a $\mathrm{Sp}_{2g}(\mathbb{F}_p)$ covering. When $p = 2$ these two coverings coincide.

Using this, Lemma 2.2.5 when $p > 2$, and the result for $N' \geq 3$, we have that

$$\mathrm{ed}(\mathcal{A}_{g,pN}/\mathcal{A}_{g,N}; p) \geq \mathrm{ed}(\mathcal{A}'_{g,pNN'}/\mathcal{A}_{g,NN'}; p) = \mathrm{ed}(\mathcal{A}_{g,pNN'}/\mathcal{A}_{g,NN'}; p) = \mathrm{dim}\mathcal{A}_g.$$

□

3.3. **Moduli spaces of curves.** Using the Torelli theorem one can use Theorem 3.2.6 to deduce the essential p-dimension of certain coverings of families of curves.

3.3.1. Let $g \geq 2$, and let $\mathcal{M}_g$ denote the coarse moduli space of genus g curves, which we view over $\mathbb{Q}$. For any integer n, let $\mathcal{M}_g[n]$ denote the $\mathbb{Z}[1/n]$-scheme which is the coarse moduli space of pairs $(C, \mathcal{B})$ consisting of a curve $C \in \mathcal{M}_g$ together with a choice $\mathcal{B}$ of basis for $H_1(C; \mathbb{Z}/n\mathbb{Z})$. For $n \geq 3$ this is a fine moduli space which is smooth over $\mathbb{Z}[1/n]$ [DM69].

Theorem 3.3.2. *Let $g, n \geq 2$, and let p be any prime dividing n. Then*

$$\mathrm{ed}(\mathcal{M}_g[n]/\mathcal{M}_g; p) = \mathrm{dim}\mathcal{M}_g = 3g - 3.$$

Proof. It suffices to prove the theorem with n replaced by the prime factor p. Choose $N \geq 3$ an integer coprime to p. Consider the natural map of $\mathbb{Q}$-schemes

$$\psi : \mathcal{M}_g[pN] \to \mathcal{M}_g[p] \times_{\mathcal{M}_g} \mathcal{M}_g[N]$$

If $g \geq 3$, there is a non-empty subset of $\mathcal{M}_g$ which admits a universal curve having no nontrivial automorphisms, and ψ is an isomorphism over a dense open subset of $\mathcal{M}_g[N]$. Hence in this case it suffices to show that $\mathrm{ed}(\mathcal{M}_g[pN]/\mathcal{M}_g[N]; p) = 3g - 3$. If $g = 2$ then, as in the proof of Corollary 3.2.7, one sees that ψ is an isomorphism if $p = 2$, and has degree 2 otherwise (all genus g curves are hyperelliptic and the hyperelliptic involution induces multiplication by -1 on the Jacobian), so that using Lemma 2.2.5 it also suffices in this case to show that $\mathrm{ed}(\mathcal{M}_g[pN]/\mathcal{M}_g[N]; p) = 3g - 3$.

The period map $\varpi : \mathcal{M}_g[N] \to \mathcal{A}_{g,N}$, which associates to a curve its Jacobian, is a locally closed embedding of smooth $\mathbb{Z}[1/N]$-schemes by the Torelli theorem. By [FvdG04, 2.3] the image of ϖ meets the ordinary locus in $\mathcal{A}_{g,N} \otimes \mathbb{F}_p$. The theorem now follows from Theorem 3.2.6. □

3.3.3. We now prove the analogue of Theorem 3.3.2 for hyperelliptic curves. Let S be a $\mathbb{Z}[1/2]$-scheme. Recall that a *hyperelliptic curve* of genus g over S is a smooth curve C/S equipped with an involution σ such that $P = C/\langle\sigma\rangle$ has genus 0. Let $\mathcal{H}_g$ denote the coarse moduli space of genus g hyperelliptic curves over $\mathbb{Z}[1/2]$. It is classical (and not hard to see) that

$$\mathcal{H}_g \cong \mathcal{M}_{0,2g+2}/S_{2g+2}$$

where $\mathcal{M}_{0,2g+2}$ is the moduli space of genus 0 curves with $2g+2$ ordered marked points, and S_{2g+2} is the symmetric group on $2g+2$ letters.

For any integer n, let $\mathcal{H}_g[n]$ denote the $\mathbb{Z}[1/2n]$-scheme which is the coarse moduli space of pairs $(C, \mathcal{B})$ consisting of a hyperelliptic curve C together with a choice $\mathcal{B}$ of basis for $H_1(C; \mathbb{Z}/n\mathbb{Z})$. As above, for $n \geq 3$ this is a fine moduli space which is smooth over $\mathbb{Z}[1/2n]$.

Theorem 3.3.4. *Let $g, n \geq 2$, and let p be any odd prime dividing n. Then*

$$\mathrm{ed}(\mathcal{H}_g[n]/\mathcal{H}_g; p) = \dim \mathcal{H}_g = 2g - 1.$$

Proof. Using Lemma 2.2.5 as in the proof of Corollary 3.2.7, one sees that it suffices to show $\mathrm{ed}(\mathcal{H}_g[pN]/\mathcal{H}_g[N]; p) = 2g - 1$ for any integer $N \geq 3$ which is coprime to p. This follows from Theorem 3.2.6, and the Torelli theorem, once we note that $\mathcal{H}_g[N]$ meets the ordinary locus of $\mathcal{A}_{g,N} \otimes \mathbb{F}_p$ ([GP05], Theorem 1). □

3.3.5. We remark that when $g = 2$, Theorem 3.3.4 extends to $p = 2$, as this is a special case of Theorem 3.3.2. However, an extension to $p = 2$ is not possible when $g > 2$. Indeed, the covering $\mathcal{M}_{0,2g+2} \to \mathcal{M}_{0,2g+2}/S_{2g+2} \xrightarrow{\sim} \mathcal{H}_g$ is a component of the coarse moduli space $\mathcal{H}_g[2]$ for hyperelliptic curves equipped with a 2-torsion point; for $g > 2$, the cover is disconnected, and all components are isomorphic.[5] We conclude that

$$\begin{aligned}\mathrm{ed}(\mathcal{H}_g[2]/\mathcal{H}_g; 2) &= \mathrm{ed}(\mathcal{M}_{0,2g+2}/\mathcal{H}_g; 2)\\ &= \mathrm{ed}(S_{2g+2}; 2)\\ &= g + 1 < 2g - 1\end{aligned}$$

where the second equality follows from the versality of $\mathcal{M}_{0,2g+2}$ for S_{2g+2}, and the third follows from [MR09, Corollary 4.2].

4. Essential dimension of congruence covers

4.1. **Forms of reductive groups.** In this subsection we prove a (presumably well known) lemma showing that for a reductive group over a number field one can always find a form with given specializations at finitely many places.

4.1.1. Let F be a number field and $G = G^{\mathrm{ad}}$ an adjoint connected reductive group over F. We fix algebraic closures $\bar{F}$ and $\bar{F}_v$ of F and F_v respectively, for every finite place v of F, as well as embeddings $\bar{F} \hookrightarrow \bar{F}_v$.

Recall [DG65, XXIV, Thm. 1.3] that the *automorphism group scheme* of G is an extension

$$1 \to G \to \mathrm{Aut}(G) \to \mathrm{Out}(G) \to 1 \qquad (4.1.2)$$

where $\mathrm{Out}(G)$ is a finite group scheme. If G is split, then this extension is split and $\mathrm{Out}(G)$ is a constant group scheme which can be identified with the group of automorphisms of the Dynkin diagram of G.

[5] The monodromy of $\mathcal{H}_g[2] \to \mathcal{H}_g$ was computed by Jordan [Jo1870, p. 364, §498] to factor as $SB_{2g+2} \twoheadrightarrow S_{2g+2} \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{F}_2)$, where $SB_{2g+2} = \pi_1(\mathcal{H}_g)$ denotes the spherical braid group. See also [Dic08, p. 125], or for more recent treatment, see the $q = 2$ case of [McM13, Theorem 5.2]. That the cover is disconnected follows from a straightforward computation: given the representation $S_{2g+2} \to \mathrm{Sp}_{2g}(\mathbb{F}_2)$, one easily exhibits vectors in $\mathbb{F}_2^{2g}$ with orbit of cardinality $(g+1)(2g+1) < 2^{2g} - 1$. The equivalence of the components follows from the monodromy computation.

We will also make use of the notion of the *fundamental group* $\pi_1(G)$ [Bor96]. This is a finite group equipped with a $\mathrm{Gal}(\bar{F}/F)$-action.

Lemma 4.1.3. *Let G be a split, adjoint connected reductive group over F, and S a finite set of places of F. The natural map of pointed sets*

$$H^1(F, \mathrm{Aut}(G)) \to \prod_{v \in S} H^1(F_v, \mathrm{Aut}(G))$$

is surjective.

Proof. Recall the following facts about the cohomology of reductive groups over global and local fields [Kot86]: Let H be an adjoint connected reductive group over F. For any place v of F, there is a map

$$H^1(F_v, H) \to \pi_1(H)_{\mathrm{Gal}(\bar{F}_v/F_v)},$$

which is an isomorphism if v is finite. For any finite set of places T of F, consider the composite map

$$\xi : \prod_{v \in T} H^1(F_v, H) \to \prod_{v \in T} \pi_1(H)_{\mathrm{Gal}(\bar{F}_v/F_v)} \to \pi_1(H)_{\mathrm{Gal}(\bar{F}/F)}.$$

Then by [Kot86, §2.2] $(x_v)_{v \in T} \in \prod_{v \in T} H^1(F_v, H)$ is in the image of $H^1(F, H)$ if $\xi((x_v)) = 0$. Applying this to $T = S \cup \{v_0\}$ for some finite place $v_0 \notin S$, we see that

$$H^1(F, H) \to \prod_{v \in S} H^1(F_v, H) \tag{4.1.4}$$

is surjective.

Next we remark that the map

$$H^1(F, \mathrm{Out}(G)) \to \prod_{v \in S} H^1(F_v, \mathrm{Out}(G))$$

is surjective. Indeed, since G is split a class in $H^1(F, \mathrm{Out}(G))$ is simply a conjugacy class of maps $\mathrm{Gal}(\bar{F}/F) \to \mathrm{Out}(G)$, and similarly for the local classes, so this follows from [Cal12, Prop. 3.2].

Now let $(x_v) \in \prod_{v \in S} H^1(F_v, \mathrm{Aut}(G))$ and let $(\bar{x}_v) \in \prod_{v \in S} H^1(F_v, \mathrm{Out}(G))$ be the image of (x_v). By what we have seen above, there exists $\bar{x} \in H^1(F, \mathrm{Out}(G))$ mapping to $(\bar{x}_v)$. Since we are assuming G is split, (4.1.2) is a split extension, so there is a $x \in H^1(F, \mathrm{Aut}(G))$ mapping to $\bar{x}$. Let H be the twist of G by x. Recall that this means that, if we choose a cocycle $x = (x_\sigma)_{\sigma \in \mathrm{Gal}(\bar{F}/F)}$ representing x, then there is an isomorphism $\tau : G \xrightarrow{\sim} H$ over $\bar{F}$, such for $g \in G(\bar{F})$ and $\sigma \in \mathrm{Gal}(\bar{F}/F)$, we have $\tau(\sigma(g)) = (\sigma(\tau(g)))^{x_\sigma}$. We have a commutative diagram

$$\begin{tikzcd}
H^1(F, \mathrm{Aut}(G)) \arrow[r] \arrow[d, "\tau"', "\sim"] & \prod_{v \in S} H^1(F_v, \mathrm{Aut}(G)) \arrow[d, "\tau|F_v"', "\sim"] \\
H^1(F, \mathrm{Aut}(H)) \arrow[r] & \prod_{v \in S} H^1(F_v, \mathrm{Aut}(H))
\end{tikzcd}$$

such that the vertical maps send x and $(x|_{F_v})_v$ to the trivial classes in the bottom line. Thus it suffices to show that

$$H^1(F, H) \to \prod_{v \in S} H^1(F_v, H)$$

is surjective, which we saw above. □

4.2. **Shimura varieties.** In this subsection we apply the results of Section 3 to compute the essential dimension for congruence covers of Shimura varieties. This will be applied in the next subsection to give examples of congruence covers of locally symmetric varieties where our techniques give a lower bound on the essential dimension. Since our aim is to give lower bounds on essential dimension, it may seem odd that we work with the formalism of Shimura varieties, rather than the locally symmetric varieties which are their geometrically connected components. However, many of the results we need are in the literature only in the former language, and it would take more effort to make the (routine) translation.

4.2.1. Recall [Del79, §1.2] that a *Shimura datum* is a pair (G, X) consisting of a connected reductive group G over $\mathbb{Q}$, and a $G(\mathbb{R})$ conjugacy class of maps $h : \mathbb{C}^\times \to G(\mathbb{R})$. This data is required to satisfy certain properties which imply that the commutant of $h(\mathbb{C}^\times)$ is a subgroup $K_\infty \subset G(\mathbb{R})$ whose image in $G^{\mathrm{ad}}(\mathbb{R})$ is maximal compact and $X = G(\mathbb{R})/K_\infty$ is a Hermitian symmetric domain.

Let $\mathbb{A}$ denote the adeles over $\mathbb{Q}$ and $\mathbb{A}_f$ the finite adeles. Let $K \subset G(\mathbb{A}_f)$ be a compact open subgroup. The conditions on (G, X) imply that for K sufficiently small, the quotient

$$\mathrm{Sh}_K(G, X) = G(\mathbb{Q})\backslash X \times G(\mathbb{A}_f)/K$$

has a natural structure of (the complex points of) an algebraic variety over a number field $E = E(G, X) \subset \mathbb{C}$, called the reflex field of (G, X), which does not depend on K. We denote this algebraic variety by the same symbol, $\mathrm{Sh}_K(G, X)$.

Now let $V_\mathbb{Z} = \mathbb{Z}^{2g}$ equipped with a perfect symplectic form ψ. Set $V = V_\mathbb{Z} \otimes_\mathbb{Z} \mathbb{Q}$ and $\mathrm{GSp} = \mathrm{GSp}(V, \psi)$. We denote by $S^\pm$ the conjugacy class of maps $h : \mathbb{C}^\times \to \mathrm{GSp}(\mathbb{R})$ satisying the following two properties

(1) The action of the real Lie group $\mathbb{C}^\times$ on $V_\mathbb{C}$ gives rise to a Hodge structure of type $(-1, 0)$ $(0, -1)$:

$$V_\mathbb{C} \xrightarrow{\sim} V^{-1,0} \oplus V^{0,-1}.$$

(2) The pairing $(x, y) \mapsto \psi(x, h(i)y)$ on $V_\mathbb{R}$ is positive or negative definite.

Then $(\mathrm{GSp}, S^\pm)$ is a Shimura datum called the *Siegel datum*, and $\mathrm{Sh}_K(\mathrm{GSp}, S^\pm)$ has an interpretation as the moduli space of principally polarized abelian varieties with suitable level structure.

We say that (G, X) is of Hodge type if there is a map $\iota : G \hookrightarrow \mathrm{GSp}$ of reductive groups over $\mathbb{Q}$ which induces $X \to S^\pm$. Given any compact open subgroup $K \subset G(\mathbb{A}_f)$ there exists a $K' \subset \mathrm{GSp}(\mathbb{A}_f)$ such that the above maps induce an embedding of Shimura varieties [Del71, Prop. 1.15]

$$\mathrm{Sh}_K(G, X) \hookrightarrow \mathrm{Sh}_{K'}(\mathrm{GSp}, S^\pm).$$

4.2.2. Now fix a prime p, and suppose that G is the generic fibre of a reductive group $G_{\mathbb{Z}_{(p)}}$ over $\mathbb{Z}_{(p)}$. If no confusion is likely to result we will sometimes write simply G for $G_{\mathbb{Z}_{(p)}}$. We take K to be of the form K_pK^p where $K_p = G(\mathbb{Z}_p)$ and $K^p \subset G(\mathbb{A}_f^p)$, where $\mathbb{A}_f^p$ denotes the finite adeles with trivial p-component. Under these conditions, p is unramified in E, and for any prime $\lambda|p$ of E, $\mathrm{Sh}_K(G, X)$ has a canonical smooth model over $\mathcal{O}_{E_\lambda}$ [Kis10, Thm. 2.3.8], [KMP16, Thm. 1], which we will denote by $\mathscr{S}_K(G, X)$. In particular, we may apply this to $\mathrm{Sh}_{K'}(\mathrm{GSp}, S^\pm)$ if we take $K' = K'_pK'^p$ with $K'_p = \mathrm{GSp}(V_\mathbb{Z}, \psi)(\mathbb{Z}_p)$.

Given $G_{\mathbb{Z}_{(p)}}$ and (G,X) of Hodge type, we may always choose (V,ψ), ι and K' with $K'_p = \mathrm{GSp}(V_{\mathbb{Z}},\psi)(\mathbb{Z}_p)$ such that ι induces a map of smooth $\mathcal{O}_{E_\lambda}$-schemes

$$\iota : \mathscr{S}_K(G,X) \hookrightarrow \mathscr{S}_{K'}(\mathrm{GSp}, S^{\pm})$$

which is locally on the source an embedding [KP, 4.1.5], [Kis10, Prop. 2.3.5]. That is, if $x \in \mathscr{S}_K(G,X)$ is a closed point, and $y = \iota(x)$, then the complete local ring at x is a quotient of the complete local ring at y. In particular, there is an open subscheme of $\mathscr{S}_K(G,X)$, whose special fibre is dense in $\mathscr{S}_K(G,X)\otimes\mathbb{F}_p$, such that the restriction of ι to this open subscheme is a locally closed embedding. Fix such choices. As in §3, we denote by $\mathcal{A}$ the universal abelian scheme over $\mathscr{S}_{K'}(\mathrm{GSp}, S^{\pm})$. Then we have

Lemma 4.2.3. *Suppose that the reflex field E, admits a prime $\lambda|p$ with residue field $\mathbb{F}_p$. Then the Galois closure of the étale local system $\mathcal{A}[p]|_{\mathrm{Sh}_K(G,X)} \to \mathrm{Sh}_K(G,X)$ is a congruence cover $\mathscr{S}_K(G,X)_p \to \mathscr{S}_K(G,X)$, with monodromy group isomorphic to $G^{\mathrm{der}}(\mathbb{F}_p)$ over every geometrically connected component of $\mathrm{Sh}_K(G,X)$.*

Moreover,

$$\mathrm{ed}(\mathrm{Sh}_K(G,X)_p \to \mathrm{Sh}_K(G,X);p) = \mathrm{dim}_{\mathbb{C}}X.$$

Proof. Let S and S' denote geometrically connected components of $\mathrm{Sh}_K(G,X)$ and $\mathrm{Sh}_{K'}(\mathrm{GSp}, S^{\pm})$ respectively with $S \subset S'$. The étale local system $\mathcal{A}[p]|_{S_{\bar{\mathbb{Q}}}}$ corresponds to a representation

$$\rho_G : \pi_1(S_{\bar{\mathbb{Q}}}) \to \pi_1(S'_{\bar{\mathbb{Q}}}) \to \mathrm{GSp}(\mathbb{F}_p)$$

where $\mathrm{GSp} = \mathrm{GSp}(V_{\mathbb{Z}},\psi)$, as above, and ρ_G has image $G^{\mathrm{der}}(\mathbb{F}_p)$: By the smooth base change theorem and the comparison between the algebraic étale and topological fundamental groups for varieties over $\mathbb{C}$, it suffices to check that the composite of the maps of topological fundamental groups

$$\pi_1^{\mathrm{top}}(S(\mathbb{C})) \to \pi_1^{\mathrm{top}}(S'(\mathbb{C})) \to \mathrm{GSp}(\mathbb{F}_p)$$

has image $G^{\mathrm{der}}(\mathbb{F}_p)$. This sequence of maps may be identified with [Del79, 2.1.2, 2.0.13]

$$\Gamma \to \Gamma' \to \mathrm{GSp}(\mathbb{F}_p)$$

where Γ and Γ' are T-congruence subgroups of $G^{\mathrm{der}}(\mathbb{Q})$ and $\mathrm{Sp}(\mathbb{Q})$-respectively, for some finite set of finite places T not containing p. In particular, the image of the composite map is $G^{\mathrm{der}}(\mathbb{F}_p)$.

By Lemma 2.2.2 we have

$$\mathrm{ed}(\mathrm{Sh}_K(G,X)_p \to \mathrm{Sh}_K(G,X);p) = \mathrm{ed}(\mathcal{A}[p]|_{S_{\bar{\mathbb{Q}}}}/S_{\bar{\mathbb{Q}}};p).$$

We now consider the map of integral models ι, corresponding to the prime $\lambda|p$ of the lemma. Since λ has residue field $\mathbb{F}_p$, every component of the image ι meets the ordinary locus of $\mathscr{S}_{K'}(\mathrm{GSp}, S^{\pm})$ by [Wor, Thm. 1.1]. Now using that for some N with $(N,p)=1$, there is a surjective map $\mathcal{A}_{g,N} \to \mathrm{Sh}_{K'}(\mathrm{GSp}, S^{\pm})$, and Theorem 3.2.6, we conclude

$$\mathrm{ed}(\mathcal{A}[p]|_{S_{\bar{\mathbb{Q}}}}/S_{\bar{\mathbb{Q}}};p) = \mathrm{dim}S = \mathrm{dim}X.$$

□

4.3. **Congruence covers.** It will be more convenient to state the results of this subsection in terms of locally symmetric varieties. These are geometrically connected components of the Shimura varieties discussed in the previous subsection.

4.3.1. Let G be a semisimple, almost simple group over $\mathbb{Q}$. We will assume that G is of classical type, so that (the connected components of) its Dynkin diagram are of type A, B, C or D.

Let $K_\infty \subset G(\mathbb{R})$ be a maximal compact subgroup. We will assume that $X = G(\mathbb{R})/K_\infty$ is a Hermitian symmetric domain. We use Deligne's notation [Del79] for the classification of these spaces. Since we are assuming G is of classical type, these are of type A_n, B_n, C_n and $D_n^{\mathbb{R}}$ and $D_n^{\mathbb{H}}$. The group $G^{\mathrm{ad}}(\mathbb{R})$ is a product of simple groups $G_i(\mathbb{R})$, for i in some index set I.

Each $G_i(\mathbb{R})$ is either compact or the adjoint group of $U(p,q)$ with $p+q = n-1$ in case of type A, of $\mathrm{SO}(n,2)$ in case of type B or $D^{\mathbb{R}}$, and of $\mathrm{SO}^*(2n)$, an inner form of $\mathrm{SO}(2n)$ if G is of type $D^{\mathbb{H}}$. We denote by I_{nc} (resp. I_c) the set of i with G_i non-compact (resp. compact).

The Dynkin diagram $\Delta(G)$ is equipped with a set of vertices $\Sigma(G)$ which is described as follows (cf. [Del79] §1.2, 1.3). For $i \in I_{nc}$, the maximal compact subgroup $K_i \subset G_i$ is the centralizer of a rank 1 compact torus $U(1) \subset G_i$, which is the center of K_i. Thus there are two cocharacters $h, h^{-1} : U(1) \to G_i$ which identify $U(1)$ with this compact torus. These cocharacters are miniscule, and each corresponds to a vertex of $\Delta(G_i)$. The two vertices are distinct exactly when h, h^{-1} are not conjugate cocharacters. In this case, they are exchanged by the *opposition involution* of $\Delta(G_i)$, which also gives the action of complex conjugation on $\Delta(G_i)$. We set $\Sigma(G)$ to be the union of all the vertices above. Thus $\Sigma(G) \cap \Delta(G_i)$ is empty if $i \in I_c$, and consists of one or two vertices if $i \in I_{nc}$. In the latter case it consists of two vertices if and only if $G_i(\mathbb{R})$ is either the adjoint group of $U(p,q)$ with $p \neq q$, or of $\mathrm{SO}^*(2n)$ with n odd.

4.3.2. Fix an embedding $\bar{\mathbb{Q}} \hookrightarrow \mathbb{C}$. The Galois group $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ acts on $\Delta(G)$. We consider a subset $\Sigma \subset \Sigma(G)$ such that $\Delta(G_i) \cap \Sigma$ consists of one element for $i \in I_{nc}$..

We call G p-admissible if G splits over an unramified extension of $\mathbb{Q}_p$, and for some embedding $\bar{\mathbb{Q}} \hookrightarrow \bar{\mathbb{Q}}_p$, and some choice of Σ, the action of $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ leaves Σ stable. This definition may look slightly odd; it will be used to guarantee that the reflex field of a Shimura variety built out of G has at least one prime where the Shimura variety has a non-empty ordinary locus.

We will say that G is of Hodge type, if G is of type A, B, C, D with $G(\mathbb{R})/K_\infty$, a Hermitian symmetric domain, as we are assuming, and if the following condition holds: If G is not of type $D^{\mathbb{H}}$ we require that G is simply connected. If G is of type $D^{\mathbb{H}}$ we require that $G(\mathbb{C})$ is a product of special orthogonal groups.

4.3.3. For any reductive group H over $\mathbb{Q}$ a *congruence subgroup* $\Gamma \subset H(\mathbb{Q})$ is a group of the form $H(\mathbb{Q}) \cap K$ for some compact open subgroup $K \subset H(\mathbb{A}_f)$. An *arithmetic lattice* $\Gamma \subset H(\mathbb{Q})$ is a finite index subgroup of a congruence subgroup. If $i : G' \to G$ is a map of reductive groups whose kernel is in the center of G', and $\Gamma' \subset G'(\mathbb{Q})$ is an arithmetic lattice then $i(\Gamma') \subset G(\mathbb{Q})$ is an arithmetic lattice.

If $\Gamma \subset G(\mathbb{Q})$ is an arithmetic lattice which acts freely on X then $M_\Gamma := \Gamma\backslash X$ has a natural structure of algebraic variety over $\bar{\mathbb{Q}}$ [Del79, §2]. For any arithmetic lattice Γ there is a finite index subgroup which acts freely on X. For a Shimura datum (G, X) the geometrically connected components of $\mathrm{Sh}_K(G, X)$ have the form

$\Gamma\backslash X$, where $\Gamma \subset G^{\mathrm{ad}}(\mathbb{Q})$ is the image of a congruence subgroup of $G^{\mathrm{der}}(\mathbb{Q})$; this was already used in the proof of 4.2.3.

Now suppose that G is almost simple and G splits over an unramified extension of $\mathbb{Q}_p$. Then G extends to a reductive group $G_{\mathbb{Z}_p}$ over $\mathbb{Z}_p$. Let $K = K^pK_p \subset G(\mathbb{A}_f)$ and $K_1 = K^pK_p^1 \subset G(\mathbb{A}_f)$ be compact open, with $K_p \subset G(\mathbb{A}_f^p)$, $K_p = G_{\mathbb{Z}_p}(\mathbb{Z}_p)$ and $K_p^1 = \ker(G_{\mathbb{Z}_p}(\mathbb{Z}_p) \to G_{\mathbb{Z}_p}(\mathbb{F}_p))$. Let $\Gamma = G(\mathbb{Q}) \cap K$ and $\Gamma_1 = G(\mathbb{Q}) \cap K_1$. We call a covering of the form $\Gamma_1\backslash X \to \Gamma\backslash X$ a principal p-level covering.

Theorem 4.3.4. *Let G' be an almost simple group of Hodge type which is p-admissible, and let $X = G'(\mathbb{R})/K_\infty$. Then for any principal p-level covering. $\Gamma_1\backslash X \to \Gamma\backslash X$ we have*

$$\mathrm{ed}(\Gamma_1\backslash X \to \Gamma\backslash X; p) = \dim X.$$

Proof. We slightly abuse notation and write G^{ad} for G'^{ad}. Let $\Sigma \subset \Sigma(G')$ be a subset of the form described above. This corresponds to a $G^{\mathrm{ad}}(\mathbb{R})$-conjugacy class of cocharacters $h : U(1) \to G^{\mathrm{ad}}$, which we denote by X^{ad}. Then $(G^{\mathrm{ad}}, X^{\mathrm{ad}})$ is a Shimura datum and its reflex field corresponds to the subgroup of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ which takes Σ to itself [Del79, Prop. 2.3.6]. Since G' is p-admissible, there is a choice of Σ, and a prime $\lambda'|p$ of $E(G^{\mathrm{ad}}, X^{\mathrm{ad}})$ with $\kappa(\lambda') = \mathbb{F}_p$.

Then one sees using [Del79, Prop. 2.3.10] that one can choose a Shimura datum (G, X) with $G^{\mathrm{der}} = G'$ and adjoint Shimura datum $(G^{\mathrm{ad}}, X^{\mathrm{ad}})$, and so that all primes of $E(G^{\mathrm{ad}}, X^{\mathrm{ad}})$ above p split completely in $E(G, X)$. In particular, any prime $\lambda|\lambda'$ of $E(G, X)$ has residue field $\mathbb{F}_p$. We have verified that (G, X) satisfies the hypotheses of Lemma 4.2.3. The theorem follows by restricting the map of that lemma to geometrically connected components. □

4.3.5. We can make the condition of p-admissibility of G' in the proposition somewhat more explicit, if we assume that $G'^{\mathrm{ad}}(\mathbb{R})$ has no compact factors.

Corollary 4.3.6. *Let G' be an almost simple group which splits over an unramified extension of $\mathbb{Q}_p$. Suppose either that*

(1) G' splits over $\mathbb{Q}_p$, or

(2) The irreducible factors of $G'^{\mathrm{ad}}(\mathbb{R})$ are all isomorphic to the adjoint group of one of $U(n,n)$, $\mathrm{SO}(n,2)$ with $n \neq 6$, or $\mathrm{Sp}(2n)$ for some positive integer n.

Then G' is p-admissible, and for any principal p-level covering $\Gamma_1\backslash X \to \Gamma\backslash X$ we have

$$\mathrm{ed}(\Gamma_1\backslash X \to \Gamma\backslash X; p) = \dim X.$$

Proof. If G' splits over $\mathbb{Q}_p$ then $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ acts trivially on $\Delta(G)$, and so leaves any choice of Σ stable. For (2), one checks using the classification of [Del79] that in each of these cases, $\Sigma = \Sigma(G)$, and a vertex $v \in \Sigma(G)$ is stable by any automorphism of the connected component of $\Delta(G)$ containing v. It follows that $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ leaves $\Sigma(G)$ stable. □

4.3.7. The above results give examples of coverings for which one can compute the essential p-dimension. It may be of interest to compare these numbers with the essential p-dimension of the corresponding group, which can in principle be computed using the Karpenko-Merkjurev theorem [KM08].

We call a reductive group H almost absolutely simple if H is semi-simple and H^{ad} is absolutely simple. (That is, it remains simple over an algebraic closure).We have the following result

Proposition 4.3.8. *Let H be a classical, almost absolutely simple group over $\mathbb{F}_q$, with $q = p^r$. Then there exists a Hermitian symmetric domain X attached to an adjoint $\mathbb{Q}$-group G, and arithmetic lattices $\Gamma' \subset \Gamma \subset G(\mathbb{Q})$ corresponding to a principal p-covering, with $\Gamma/\Gamma' \xrightarrow{\sim} H(\mathbb{F}_q)$, such that*

$$e = \mathrm{ed}(\Gamma'\backslash X \to \Gamma\backslash X; p)$$

satisfies

- *If H is a form of SL_n which is split if n is odd, then $e = r\lfloor \frac{n^2}{4} \rfloor$.*
- *If H is Sp_{2n} then $e = r(\frac{n^2+n}{2})$.*
- *If H is a split form of SO_{2n} then $e = r(\frac{n^2-n}{2})$.*
- *If H is a form of Spin_n and H is not of type D_4, then $e(H(\mathbb{F}_q)) = r(n-2)$.*

Proof. Let $\bar{G} = \mathrm{Res}_{\mathbb{F}_q/\mathbb{F}_p} H$. There is a unique (up to canonical isomorphism) connected reductive group $G_{\mathbb{Z}_p}$ over $\mathbb{Z}_p$ with $G_{\mathbb{Z}_p} \otimes \mathbb{F}_p = \bar{G}$.

We (may) now assume that H is one of the four types listed, and in each of these cases we define a semi-simple Lie group $G_{\mathbb{R}}$ over $\mathbb{R}$ as follows. If H is a form of SL_n, we take $G_{\mathbb{R}}$ to be $\mathrm{SU}(\frac{n}{2}, \frac{n}{2})^r$ if n is even and $\mathrm{SU}(\frac{n-1}{2}, \frac{n+1}{2})^r$ if n is odd. If H is Sp_{2n} we take $G_{\mathbb{R}} = \mathrm{Sp}_{2n}^r$. If H is a form of SO_{2n} we take $G_{\mathbb{R}}$ to be $\mathrm{SO}^*(2n)^r$, the inner form of (the compact group) $\mathrm{SO}(2n)$ which gives rise to the Hermitian symmetric domain of type $D_n^{\mathbb{H}}$ (cf. [Del79, 1.3.9,1.3.10]). If H is a form of Spin_n we take $G_{\mathbb{R}}$ to be $\mathrm{Spin}(n-2,2)^r$.

In all cases $G_{\mathbb{R}}$ and $G_{\mathbb{Z}_p}$ are forms of the same split group. Thus by Lemma 4.1.3 there exists a semi-simple reductive group G over $\mathbb{Q}$, which gives rise to $G_{\mathbb{R}}$ and $G_{\mathbb{Z}_p}$ over $\mathbb{R}$ and $\mathbb{Z}_p$ respectively. By assumption G' is of Hodge type, and we now check that it can be chosen to be p-admissible. This is necessarily the case by Corollary 4.3.6, except when n is odd and H is a form of SL_n or H is a form of $\mathrm{SO}(2n)$. In these cases, we are assuming that H is a split form, so $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ permutes the components of $\Delta(G)$ simply transitively. If H is a form of SL_n or $\mathrm{SO}(2n)$ with n odd, then $\Delta(G_i)$ contains two points in $\Sigma(G)$ (the opposition involution is nontrivial on $\Delta(G_i)$ in these cases), and we can take $\Sigma \subset \Sigma(G)$ to be a $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit of any point $v \in \Sigma(G)$.

When H is a form of $\mathrm{SO}(2n)$ with n even, then the opposition involution is trivial on $\Delta(G_i)$, and hence so is the action of complex conjugation. The set $\Sigma(G)$ meets each component of $\Delta(G)$ in one vertex. Let Σ_1 be the $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$-orbit of any vertex in $\Sigma(G)$. There is an inner form $G_{1,\mathbb{R}}$ of G over $\mathbb{R}$ such that $\Sigma(G_{1,\mathbb{R}}) = \Sigma_1$. (Note that the Dynkin diagrams of inner forms are identified so this makes sense.) Explicitly, let $a \in \mathrm{Out}(G)$ be an automorphism which preserves the connected components of $\Delta(G)$ and such that $a(\Sigma(G)) = \Sigma_1$. (Such an a is unique except if H is of type D_4.) Then $G_{1,\mathbb{R}}$ is given by twisting G by the cocycle $\tilde{a}\sigma(\tilde{a})^{-1}$ where $\tilde{a} \in \mathrm{Aut}(G)(\mathbb{C})$ lifts a. Using the surjection (4.1.4), we see that there is an inner twisting G_1 of G over $\mathbb{Q}$ which is isomorphic to $G_{1,\mathbb{R}}$ over $\mathbb{R}$ and to G over $\mathbb{Q}_p$, as an inner twist. As $\Sigma(G_1) = \Sigma_1$ is stable by $\mathrm{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$, G_1 is p-adimissible. Thus, the proposition follows from Theorem 4.3.4 and the formulae for the dimensions of Hermitian symmetric domains. □

Corollary 4.3.9. *Let H be a classical, absolutely simple group over $\mathbb{F}_q$, with $q = p^r$. Then there is a congruence $H(\mathbb{F}_q)$-cover of locally symmetric varieties $Y' \to Y$ such that $e := \mathrm{ed}_K(Y'/Y; p)$ satisfies :*

- *If H is a form of PGL_n which is split if n is odd, then $e = r\lfloor \frac{n^2}{4} \rfloor$.*

- *If H is* PSp_{2n} *then* $e = r(\frac{n^2+n}{2})$.
- *If H is a split form of* PO_{2n} *then* $e = r(\frac{n^2-n}{2})$.
- *If H is a form of* PO_n *and H is not of type* D_4, *then* $e = r(n-2)$.

Proof. This follows immediately from Proposition 4.3.8 and Lemma 2.2.5. □

References

[Bor96] Mikhail Borovoi, *Abelianization of the first Galois cohomology of reductive groups*, Internat. Math. Res. Notices **8** (1996), 401–407.

[BR97] J. Buhler and Z. Reichstein, *On the essential dimension of a finite group*, Compositio Math. **106** (1997), no. 2, 159–179.

[Bu1890] Heinrich Burkhardt, *Grundzüge einer allgemeinen Systematik der hyperelliptischen Functionen I. Ordnung*, Math. Ann. **35** (1890), 198-296.

[Bu1891] ———, *Untersuchungen aus dem Gebiete der hyperelliptischen Modulfunctionen. Zweiter Teil.*, Math. Ann. **38** (1891), 161-224.

[Bu1893] ———, *Untersuchungen aus dem Gebiete der hyperelliptischen Modulfunctionen. III.*, Math. Ann. **41** (1893), 313-343.

[Cal12] Frank Calegari, *Even Galois representations and the Fontaine–Mazur conjecture. II*, J. Amer. Math. Soc. **25** (2012), no. 2, 533–554.

[CT02] J.L. Colliot-Thélène, *Exposant et indice d'algbres simples centrales non ramifiées. (With an appendix by Ofer Gabber.)*, Enseigne. Math. **48** (2002), no. 1–2, 127-146.

[Del71] Pierre Deligne, *Travaux de Shimura*, Séminaire Bourbaki, 23ème année (1970/71), Exp. No. 389, 1971, pp. 123–165. Lecture Notes in Math., Vol. 244.

[Del79] ———, *Variétés de Shimura: interprétation modulaire, et techniques de construction de modèles canoniques*, Automorphic forms, representations and L-functions (Proc. Sympos. Pure Math., Oregon State Univ., Corvallis, Ore., 1977), Part 2, 1979, pp. 247–289.

[DM69] P. Deligne and D. Mumford, *The irreducibility of the space of curves of given genus*, Inst. Hautes Études Sci. Publ. Math. **36** (1969), 75–109.

[DG65] M. Demazure and A. Grothendieck, *Schémas en groupes. Fasc. 7: Exposés 23 à 26*, Séminaire de Géométrie Algébrique de l'Institut des Hautes Études Scientifiques, vol. 1963/64, Institut des Hautes Études Scientifiques, Paris, 1965/1966.

[Dic08] L.E. Dickson, *Representations of the General Symmetric Group as Linear Groups in Finite and Infinite Fields*, Trans. AMS **9** (1908), no. 2, 121–148.

[DR15] Alexander Duncan and Zinovy Reichstein, *Versality of algebraic group actions and rational points on twisted varieties*, J. Algebraic Geom. **24** (2015), no. 3, 499–530.

[FvdG04] Carel Faber and Gerard van der Geer, *Complete subvarieties of moduli spaces and the Prym map*, J. Reine Angew. Math. **573** (2004), 117–137.

[FW17] Benson Farb and Jesse Wolfson, *Resolvent degree, Hilbert's 13th Problem and Geometry*, arXiv:1803.04063 (2017).

[Gro68] Alexander Grothendieck, *Cohomologie locale des faisceaux cohérents et théorèmes de Lefschetz locaux et globaux* (*SGA* 2), North-Holland Publishing Co., Amsterdam; Masson & Cie, Éditeur, Paris, 1968. Séminaire de Géométrie Algébrique du Bois-Marie, 1962, Advanced Studies in Pure Mathematics, Vol. 2.

[Gro61] A. Grothendieck, *Éléments de géométrie algébrique.*, Inst. Hautes Études Sci. Publ. Math. **4,8,11,17,20,24,32** (1961,1962,1964).

[FD93] Benson Farb and R. Keith Dennis, *Noncommutative algebra*, Graduate Texts in Mathematics, vol. 144, Springer-Verlag, New York, 1993.

[GP05] Darren Glass and Rachel Pries, *Hyperelliptic curves with prescribed p-torsion*, Manuscripta Math. **117** (2005), no. 3, 299–317.

[He1858] C. Hermite, *Sur la résolution de l'equation du cinquième degré*, Comptes rendus de l'Académie des Sciences **46** (1858), 508–515.

[HS02] K Hulek and G.K. Sankaran, *The geometry of Siegel modular varieties*, Higher dimensional birational geometry (Kyoto, 1997), 2002, pp. 89–156.

[Jo1870] Camille Jordan, *Traité des Substitutions*, Gauthier–Villars, Paris, 1870.

[KM08] Nikita A. Karpenko and Alexander S. Merkurjev, *Essential dimension of finite p-groups*, Invent. Math. **172** (2008), no. 3, 491–508.

[Kat81] N. Katz, *Serre-Tate local moduli*, Algebraic surfaces (Orsay, 1976–78), 1981, pp. 138–202.

[KMP16] Wansu Kim and Keerthi Madapusi Pera, *2-adic integral canonical models*, Forum Math. Sigma **4** (2016), e28, 34.

[Kis10] Mark Kisin, *Integral models for Shimura varieties of abelian type*, J. Amer. Math. Soc. **23** (2010), no. 4, 967–1012.

[KP] Mark Kisin and George Pappas, *Integral models of Shimura varieties with parahoric level structure*, Publ. IHES, to appear, arXiv:1512.01149.

[Kl1884] Felix Klein, *Vorlesungen über das Ikosaeder und die Auflösung der Gleichungen vom fnften Grade (Lectures on the Icosahedron and the Solution of the Equation of the Fifth Degree)*, Leipzig, Tübner, 1884.

[Kl1887] ———, *Zur Theorie der allgemeinen Gleichungen sechsten und siebenten Grades*, Math. Ann. **28** (1887), 499-532.

[Kl1888] ———, *Sur la resolution, par les fonctions hyperelliptiques de l'equation du vingt-septieme degre, de laquelle depend la determination des vingt-sept droites d'une surface cubique*, Journal de Mathématiques pures et appliquées **4** (1888), 169-176.

[Kl1893] ———, *Lectures on Mathematics*, MacMillan and Co., 1894.

[Kle05] ———, *Über die Auflösung der allgemeinen Gleichungen fünften und sechsten Grades*, Journal für die reine und angewandte Mathematik **129** (1905), 150-174.

[Kle22] ———, *Gesammelte Mathematische Abhandlungen*, Vol. 2, Berlin, 1922.

[Kot86] Robert E. Kottwitz, *Stable trace formula: elliptic singular terms*, Math. Ann. **275** (1986), no. 3, 365–399.

[Kr1861] Leopold Kronecker, *Ueber die Gleichungen fünften Grades*, Journal für die reine und angewandte Mathematik **59** (1861), 306–310.

[McM13] Curtis McMullen, *Braids and Hodge Theory*, Math. Ann. **355** (2013), 893–946.

[Mer17] Alexander Merkurjev, *Essential dimension*, Bull. AMS **54** (2017), no. 4, 635–661.

[MR09] A. Meyer and Z. Reichstein, *The essential dimension of the normalizer of a maximal torus in the projective linear group*, Algebra & Number Theory **3** (2009), no. 4, 467–487.

[RG71] M. Raynaud and L. Gruson, *Critères de platitude et de projectivité. Techniques de "platification" d'un module*, Invent. Math. **13** (1971), 1–89.

[Rei10] Zinovy Reichstein, *Essential Dimension*, Proceedings of the International Congress of Mathematicians, 2010.

[RY00] Zinovy Reichstein and Boris Youssin, *Essential dimensions of algebraic groups and a resolution theorem for G-varieties*, Canad. J. Math. **52** (2000), no. 5, 1018–1056. With an appendix by János Kollár and Endre Szabó.

[Tsc43] N.G. Tschebotaröw, *The problem of resolvents and critical manifolds*, Izvestia Akad. Nauk SSSR **7** (1943), 123–146.

[Wor] Daniel Wortmann, *The μ-ordinary locus for Shimura varieties of Hodge type*, arXiv:1310.6444.

Department of Mathematics, University of Chicago
Email address: farb@math.uchicago.edu

Department of Mathematics, Harvard
Email address: kisin@math.harvard.edu

Department of Mathematics, University of California-Irvine
Email address: wolfson@uci.edu