

UC Irvine

UC Irvine Previously Published Works

Title

The essential dimension of congruence covers

Permalink

<https://escholarship.org/uc/item/7rp942x4>

Journal

Compositio Mathematica, 157(11)

ISSN

0010-437X

Authors

Farb, Benson

Kisin, Mark

Wolfson, Jesse

Publication Date

2021-11-01

DOI

10.1112/s0010437x21007594

Copyright Information

This work is made available under the terms of a Creative Commons Attribution-NonCommercial License, available at <https://creativecommons.org/licenses/by-nc/4.0/>

Peer reviewed

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. These results include cases where the locally symmetric variety M 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.

CONTENTS

1. Introduction	1
2. Preliminary results	5
2.1. Finite étale maps	5
2.2. Essential dimension	7
3. Essential dimension and moduli of abelian varieties	10
3.1. Ordinary finite flat group schemes	10
3.2. Monodromy of p -torsion in an abelian scheme	12
3.3. Moduli spaces of curves	16
4. Essential dimension of congruence covers	17
4.1. Forms of reductive groups	17
4.2. Shimura varieties	19
4.3. Congruence covers	21
References	24

1. INTRODUCTION

This article grew out of an attempt to answer questions first raised by Kronecker and Klein.¹ Let K be an algebraically closed field of characteristic 0, and consider

The authors are partially supported by NSF grants DMS-1811772 (BF), DMS-1601054 (MK) and DMS-1811846 (JW).

¹See [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.

the algebraic function $\Phi_{g,n}$ that assigns to a general g -dimensional (principally polarized) abelian K -variety an n -torsion point.

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 $\mathcal{A}_{g,n}^1$ be the coarse moduli space of pairs (A, z) where A is a principally polarized abelian variety of dimension g , and z is an n -torsion point on A .

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

$$\begin{array}{ccc} X' & \dashrightarrow & Y' \\ \downarrow & & \downarrow \\ X & \xrightarrow{f} & Y \end{array}$$

of a finite map $Y' \rightarrow Y$ of d -dimensional K -varieties via a rational map $f : X \dashrightarrow Y$. In this case we call f a (*rational*) *compression* of p . Question 1 can be rephrased as asking for the value of $\text{ed}_K(\mathcal{A}_{g,n}^1 \rightarrow \mathcal{A}_g)$.

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

$$\min_{E \rightarrow \mathcal{A}_g} \text{ed}_K(\mathcal{A}_{g,n}^1|_E \rightarrow E)$$

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

$$\text{ed}_K(X' \times_X E \rightarrow E) = \text{ed}_K(\tilde{X}' \times_X E \rightarrow E)$$

where \tilde{X}' denotes the composite of Galois closures of the connected components of X' (see Lemmas 2.2.2, 2.2.3, cf. [BR97, Lemma 2.3]). In particular, for any class of maps $E \rightarrow \mathcal{A}_g$ the answer to the question above does not change if we replace $\mathcal{A}_{g,n}^1$ by $\mathcal{A}_{g,n}$, the coarse moduli space of pairs (A, \mathcal{B}) where A is a principally polarized abelian variety of dimension g , and \mathcal{B} is a symplectic basis for the n -torsion $A[n]$. (Here and below we fix once and for all an isomorphism $\mu_n(K) \xrightarrow{\sim} \mathbb{Z}/n\mathbb{Z}$, so that we may speak of a symplectic basis for $A[n]$.)

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*

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

²Given maps $X' \rightarrow X$ and $E \rightarrow X$, 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, $\text{ed}_K(\mathcal{A}_{g,n}|_{\mathcal{Z}}/\mathcal{Z}) = \dim \mathcal{Z}$. More precisely, we prove the following (see Theorem 3.2.6 below).

Theorem 3. *Let p be prime, and let $N \geq 3$ be an integer prime to p . Suppose that $L = \widehat{\mathbb{Q}}_p$, 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 $\mathcal{A}_{g,N}^{\text{ord}} \subset \mathcal{A}_{g,N/k}$. Then*

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

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, proper, genus $g \geq 2$ curves over K . For any integer n , consider the *level n congruence cover* $\mathcal{M}_g[n] \rightarrow \mathcal{M}_g$, where $\mathcal{M}_g[n]$ denotes the moduli space of pairs (C, \mathcal{B}) consisting of a smooth, proper curve C of genus g , together with a symplectic basis \mathcal{B} for $J(C)[n]$, where $J(C)$ is the Jacobian of C . 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*

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

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* $\mathcal{H}_g[n] \rightarrow \mathcal{H}_g$, where $\mathcal{H}_g[n]$ denotes the moduli space of pairs (C, \mathcal{B}) consisting of a hyperelliptic curve C together with a symplectic basis \mathcal{B} for $J(C)[n]$. 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*

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

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). Attached to Γ there is a semisimple algebraic group G over \mathbb{Q} , with $X = G(\mathbb{R})/K_\infty$, for $K_\infty \subset G(\mathbb{R})$ a maximal compact subgroup. By a *principal p -level covering* $\Gamma_1 \backslash X \rightarrow \Gamma \backslash X$ 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 4.3.5 below for the most general statement).

Theorem 6. *With notation as just given, suppose that each irreducible factor of $G_{\mathbb{R}}^{\text{ad}}$ is the adjoint group of one of $U(n, n)$, $\text{SO}(n, 2)$ with $n + 2 \neq 8$, or $\text{Sp}(2n)$ for some positive integer n . If G is unramified at p , (a condition which holds for almost all p) then for any principal p -level covering $\Gamma_1 \backslash X \rightarrow \Gamma \backslash X$, we have*

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

In fact our results apply to any Hermitian symmetric domain of classical type, but in general they require a more involved condition on the \mathbb{Q} -group G giving rise to Γ ; they always apply if G splits over \mathbb{Q}_p . 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 $\{E'_i \rightarrow E_i\}$ is a collection of connected, unramified $\mathbb{Z}/p\mathbb{Z}$ covers of elliptic curves E_i , then under certain conditions, the cover $E'_1 \times \cdots \times E'_r \rightarrow E_1 \times \cdots \times E_r$ has essential dimension at p equal to r .

When $\Gamma \backslash X$ is proper, the use of fixed-point techniques is precluded by the fact that one cannot use “ramification at infinity”. This is in analogy with Margulis superrigidity for irreducible lattices Γ in higher rank semisimple Lie groups, where, for nonuniform Γ (equivalently noncompact $\Gamma \backslash X$), unipotents in Γ play a crucial role. When Γ is uniform, it contains no unipotents, and new ideas were needed (and were provided only later, also by Margulis).

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 $Y' \rightarrow Y$ such that $e := \text{ed}_K(Y'/Y; p)$ 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* $RD(X \rightarrow Y)$, which asks for the

minimum d such that an algebraic function admits a *formula*³ using only algebraic functions of d or fewer variables (see [FW17]). For example, Klein’s icosahedral formula for the quintic [Kl1884] shows that $RD(\Phi) = 1$ for any algebraic function Φ with monodromy A_5 , while the essential p -dimension can equal 2. At present, we do not know of a single example which provably has $RD(X \rightarrow Y) > 1$.

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 $N \geq 3$ be an integer coprime to p , and let \mathcal{A} denote the universal abelian scheme over $\mathcal{A}_{g,N}$ (now considered over $\mathbb{Z}[\zeta_N][1/N]$). 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 $\mathcal{A}_{g,pN} \rightarrow \mathcal{A}_{g,N}$ (in characteristic 0) onto a smaller-dimensional variety, we show that there is an ordinary mod p point x of $\mathcal{A}_{g,N}$, 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 would like to thank Aaron Landesman and Zinovy Reichstein for detailed comments on an earlier version of this paper and for extensive helpful correspondence. We also thank Maxime Bergeron, Mike Fried, Eric Rains, Alexander Polishchuk and Burt Totaro, for various helpful comments. Finally we thank the referee for many useful comments.

2. PRELIMINARY RESULTS

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

2.1.1. Let $G \rightarrow G'$ be a map of groups, and S a finite set with an action of G . We say the action of G on S *lifts* to G' if there is an action of G' on S , which induces the given action of G on S . We call such a G' -action a *lifting* of the G -action on S . We say that the action of G on S *virtually lifts* to G' if there is a finite index subgroup $G'' \subset G'$, containing the image of G , such that the action of G on S lifts to G'' .

For a positive integer n we denote by S^n the n -fold product equipped with the diagonal action of G , and by $\pi_i : S^n \rightarrow S$, $i = 1, \dots, n$ the projections.

Lemma 2.1.2. *Let $G \rightarrow G'$ be a map of groups, and S a finite set with an action of G .*

³Recall that a *formula* for an algebraic function Φ on a complex variety X is a tower of finite field extensions $\mathbb{C}(X) = K_0 \subset K_1 \subset \dots \subset K_r$, a choice of primitive element $\Psi_i \in K_i$ for K_i/K_{i-1} for each i , and an embedding $\mathbb{C}(X)(\Phi) \subset K_r$ of fields over $\mathbb{C}(X)$. One can then write $\Phi = R(\Psi_1, \dots, \Psi_r)$ for $R \in K(X)(t_1, \dots, t_r)$ a rational function, which is to say a “formula” for Φ in terms of the Ψ_i .

- (1) Suppose the action of G on S admits a lifting to an action of G' on S , and fix such a lifting. Then there exists a finite index subgroup $G'' \subset G'$ containing the image of G , such that G and G'' have the same image in $\text{Aut}(S)$.
- (2) Let $T \subset S^n$ be a G -stable subset such that $\cup_{i=1}^n \pi_i(T) = S$. Then the action of G on S virtually lifts to G' if and only if the action of G on T virtually lifts to G' .

Proof. Let $N \subset G'$ be the kernel of $G' \rightarrow \text{Aut}(S)$, and $G'' \subset G'$ the subgroup generated by N and the image of G . Since S is finite, N and hence G'' has finite index in G' , and satisfies the conditions in (1).

For (2), suppose that the action of G on S virtually lifts to G' . By (1), after replacing G' by a finite index subgroup containing the image of G , we may assume that the action of G on S lifts to G' , and that G and G' have the same image in $\text{Aut}(S)$. Then T is G' -stable, so the action of G on T lifts to G' . Conversely, if the action of G on T virtually lifts to G' , then, by (1), we may assume that the action of G on T lifts to G' , and that G and G' have the same image in $\text{Aut}(T)$. In particular, any element of G' acts on $\text{Aut}(T)$ via an element of $\text{Aut}(S)$. Since $\cup_{i=1}^n \pi_i(T) = S$ this element of $\text{Aut}(S)$ is uniquely determined. The uniqueness implies that $G' \rightarrow \text{Aut}(T)$ factors through a homomorphism $G' \rightarrow \text{Aut}(S)$, which lifts the action of G on S . \square

2.1.3. Let X be a scheme, and $f : Y \rightarrow X$ a finite étale cover. We will say that f is Galois if any connected component of Y is Galois over its image. If \bar{x} is a geometric point of X , then Y corresponds to a finite set $S(Y)$ equipped with an action of $\pi_1(X, \bar{x})$. Conversely, if X is connected and S is a finite set with an action of $\pi_1(X, \bar{x})$, we denote by $Y(S)$ the corresponding finite étale cover of X .

In the next three lemmas we consider a map of schemes $g : X \rightarrow X'$ and a finite étale cover $f' : Y' \rightarrow X'$ equipped with an isomorphism $Y \xrightarrow{\sim} Y' \times_{X'} X$. If X and X' are connected, and \bar{x} again denotes the geometric point of X' induced by \bar{x} , then such a Y' exists if and only if the action of $\pi_1(X, \bar{x})$ on $S(Y)$ lifts to $\pi_1(X', \bar{x})$.

Lemma 2.1.4. *If f is Galois, then there is a finite étale $h : X'' \rightarrow X'$ such that g factors through X'' and $Y'' = X'' \times_{X'} Y' \rightarrow X''$ is Galois.*

Proof. We may assume that X and X' are connected. We apply Lemma 2.1.2, (1), to $\pi_1(X, \bar{x}) \rightarrow \pi_1(X', \bar{x})$ and $S = S(Y) = S(Y')$. Let $h : X'' \rightarrow X'$ be the finite étale map corresponding to the $\pi_1(X', \bar{x})$ -set $\pi_1(X', \bar{x})/G''$. Since this set has a $\pi_1(X, \bar{x})$ fixed point, g factors through X'' . By construction, the images of $\pi_1(X'', \bar{x})$ and $\pi_1(X, \bar{x})$ in $\text{Aut}(S(Y')) = \text{Aut}(S(Y))$ are equal. Denote this image by H , and for $s \in S(Y)$ denote by H_s the stabilizer. Since $Y \rightarrow X$ is Galois, H_s is a normal subgroup which does not depend on s , which implies that $Y'' \rightarrow X''$ is Galois. \square

2.1.5. Let A be a finite ring. By an A -local system \mathcal{F} on X we will mean 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 $Y(\mathcal{F}) \rightarrow X$. 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 conjugacy classes of representations $\pi_1(X) \rightarrow \text{GL}_n(A)$.

For $X \rightarrow X_1$ a map of schemes, and \mathcal{G} an A -local system on X_1 , we will denote by $\mathcal{G}|_X$ the pullback of \mathcal{G} to X .

Lemma 2.1.6. *Suppose that $f : Y = Y(\mathcal{F}) \rightarrow X$ corresponds to an A -local system \mathcal{F} . Then there is a finite étale $h : X'' \rightarrow X'$ such that g factors through X'' and $Y'' = X'' \times_X Y' \rightarrow X''$ represents an A -local system \mathcal{F}'' , with $\mathcal{F}''|_X \xrightarrow{\sim} \mathcal{F}$.*

Proof. Choose X'' as in the proof of Lemma 2.1.4, using the construction in Lemma 2.1.2, (1). Then the finite set $S(Y) = S(Y')$ naturally has the structure of a finite free A -module on which $\pi_1(X, \bar{x})$ acts A -linearly. Since the images of $\pi_1(X'', \bar{x})$ and $\pi_1(X, \bar{x})$ in $\text{Aut}(S(Y))$ are equal, $\pi_1(X'', \bar{x})$ acts on $S(Y)$ A -linearly, which implies the statement of the lemma. \square

2.1.7. 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 and only if X is a $\mathbb{Z}[1/N]$ -scheme.

Suppose X is a $\mathbb{Z}[1/N]$ -scheme. For any $\mathbb{Z}/N\mathbb{Z}$ algebra A , we again denote by μ_N or $A(1)$ the étale sheaf $\mu_N \otimes_{\mathbb{Z}/N\mathbb{Z}} A$. For any non-negative integer i we write $A(i) = A(1)^{\otimes i}$. For i negative we set $A(i)$ equal to the A -linear dual of $A(-i)$.

Lemma 2.1.8. *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 $f : Y = Y(\mathcal{F}) \rightarrow X$ corresponds to an A -local system \mathcal{F} , which is an extension of $A(i)^r$ by $A(j)^s$, for some positive integers h, g .*

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

Proof. Replacing \mathcal{F} by $\mathcal{F}(-j) := \mathcal{F} \otimes_A A(-j)$, we may suppose that $j = 0$. By Lemma 2.1.6, we may assume 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 $A(j)^s$, 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 $\mathcal{F}'/A(i)^r$ by $A(j)^s$, and $g^*(\mathcal{F}') \xrightarrow{\sim} \mathcal{F}$ is an isomorphism of extensions. A similar argument, applied to $\mathcal{F}/A(j)^s \otimes A(-i)$, shows that we may assume that \mathcal{F}' is an extension of $A(i)^r$ by $A(j)^s$, with $\mathcal{F}'|_X \xrightarrow{\sim} \mathcal{F}$ as extensions. \square

2.2. Essential dimension.

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

Note that when X is irreducible, the definition does not change if we consider only coverings with E irreducible. Indeed, for any $E \rightarrow X$, as above, one of the irreducible components of E will have degree prime to p over the generic point of X .

Suppose X is connected. A *Galois closure* of $Y \rightarrow X$ is a union of Galois closures of the connected components of Y . If $Y_i \rightarrow X$ $i = 1, \dots, r$ are finite étale, Galois and connected, then a *composite* of the Y_i is a connected component of $Y_1 \times_X \dots \times_X Y_r$. Up to isomorphism, this does not depend on the choice of connected component. If we drop the assumption that X is connected, we define the Galois closure and composite by making these constructions over each connected component of X .

Lemma 2.2.2. *Let $f : Y \rightarrow X$ be finite étale cover, and \tilde{Y} a Galois closure for Y . For any map of K -schemes $E \rightarrow X$, we have*

$$\mathrm{ed}_K(Y_E/E) = \mathrm{ed}_K(\tilde{Y}_E/E).$$

In particular, we have

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

Proof. We may assume that X is connected. Let \bar{x} be a geometric point for X , and S a $\pi_1(X, \bar{x})$ -set with $Y = Y(S)$. Suppose first that Y is connected. Let $N \subset \pi_1(X, \bar{x})$ be the (normal) subgroup which fixes S pointwise. If $s \in S$, and $\pi_1(X, \bar{x})_s$ is the stabilizer of s , then $N = \bigcap_{i=1}^n g_i \pi_1(X, \bar{x})_s g_i^{-1}$ for a finite collection of elements $g_1, \dots, g_n \in \pi_1(X, \bar{x})$. Let \tilde{S} denote the $\pi_1(X, \bar{x})$ -orbit of $(g_1 \cdot s, \dots, g_n \cdot s) \in S^n$. Then the stabilizer in $\pi_1(X, \bar{x})$ of any point of \tilde{S} is N , so $\tilde{Y} = Y(\tilde{S})$ is a Galois closure of Y .

Now we drop the assumption that Y is connected, and let Y_1, \dots, Y_r denote the connected components of Y , with Y_i corresponding to a subset $S_i \subset S$ on which $\pi_1(X, \bar{x})$ acts transitively. The above construction gives subsets $\tilde{S}_i \subset S_i^n$, (we may assume without loss of generality that n does not depend on i) with $\tilde{Y}_i = Y(\tilde{S}_i)$ a Galois closure of Y_i . If $\tilde{S} = \coprod_i \tilde{S}_i \subset S^n$, then $\tilde{Y} = Y(\tilde{S}) = \coprod_i \tilde{Y}_i$ is a Galois closure for Y .

From the construction one sees that $S, T = \tilde{S}$ and $G = \pi_1(X, \bar{x})$ satisfy the conditions in Lemma 2.1.2, (2) (note that these conditions do not depend on the choice of G'). For any map of groups $H \rightarrow G$, these conditions continue to hold if we instead view S and T as H -sets.

Now let $E \rightarrow X$ be a map of K -schemes, $U \subset E$ a connected open subset, and $U \rightarrow E'$ a map of K -schemes. Suppose U admits a geometric point \bar{y} mapping to \bar{x} . Applying the above remark with $H = \pi_1(U, \bar{y})$, Lemma 2.1.2, (2) implies that the action of H on S virtually lifts to $\pi_1(E', \bar{y})$ if and only the action of H on T virtually lifts to $\pi_1(E', \bar{y})$. As in the proof of Lemma 2.1.4, this implies that $Y|_U$ arises by pullback from a cover of E' for some finite étale $E'' \rightarrow E'$, if and only if the same condition holds for $\tilde{Y}|_U$. Since \bar{x} was an arbitrary geometric point of X , this implies $\mathrm{ed}_K(Y|_E/E) = \mathrm{ed}_K(\tilde{Y}|_E/E)$. \square

Lemma 2.2.3. *Let $Y_i \rightarrow X$ $i = 1, \dots, r$ be connected Galois coverings of K -schemes, and $Y \rightarrow X$ a composite of the Y_i . Then for any map of K -schemes $E \rightarrow X$, we have*

$$\mathrm{ed}_K(Y_E/E) = \mathrm{ed}_K\left(\left(\prod_i Y_i\right)_E/E\right).$$

In particular, we have

$$\mathrm{ed}_K(Y/X; p) = \mathrm{ed}_K\left(\left(\prod_i Y_i\right)/X; p\right).$$

Proof. Let \bar{x} be a geometric point for X , and let S_i be a $\pi_1(X, \bar{x})$ -set with $Y_i = Y(S_i)$. Let $S = \coprod_i S_i$. Then Y corresponds to a transitive $\pi_1(X, \bar{x})$ set $T \subset S_1 \times \cdots \times S_r$ which surjects onto each S_i . Viewing $T \subset S^r$, we see that T satisfies the conditions of Lemma 2.1.2. The lemma now follows as in the proof of Lemma 2.2.2. \square

Lemma 2.2.4. *Let A be a finite ring, K a field, \mathcal{F} an A -local system on a connected K -scheme X equipped with a geometric point \bar{x} , and $\rho_{\mathcal{F}} : \pi_1(X, \bar{x}) \rightarrow \mathrm{GL}_n(A)$ 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 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 $\pi_1(X, \bar{x})$ on A^n corresponding to \mathcal{F} . The connected components of $Y(\mathcal{F})$ correspond to the stabilizers $\pi_1(X)_s$ for $s \in A^n$. A Galois closure of such a component corresponds to

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

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

The lemma now follows from Lemmas 2.2.2 and 2.2.3. \square

Lemma 2.2.5. *Let $K' \subset K$ be algebraically closed fields. If $Y \rightarrow X$ is a finite étale covering of finite type 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 $U_K \rightarrow W_K$ a morphism with $\dim W_K = \mathrm{ed}_K(Y_K/X_K)$ such that $Y_K|_{U_K}$ arises from a finite cover $f' : Y'_K \rightarrow W_K$. 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 $R \rightarrow K'$ produces the required data for the covering $Y \rightarrow X$. \square

2.2.6. It will be convenient to make the following definition. Suppose that $Y \rightarrow X$ is a finite étale covering of finite type R -schemes, where R is a domain of characteristic 0. Set $\mathrm{ed}(Y/X) = \mathrm{ed}_{\bar{K}}(Y/X)$ where \bar{K} is any algebraically closed field containing R , and similarly for $\mathrm{ed}(Y/X; p)$. By Lemma 2.2.5 this does not depend on the choice of \bar{K} .

Lemma 2.2.7. *Let K be an algebraically closed field, and $Y \rightarrow X$ a finite Galois covering of connected, finite type K -schemes with Galois group G . Let $H \subset G$ be a central, cyclic subgroup of order n with $\mathrm{char}(K) \nmid n$. Then for any prime p we have*

$$\mathrm{ed}(Y \rightarrow X; p) \geq \mathrm{ed}(Y/H \rightarrow X; p)$$

with equality if $p \nmid n$.

Proof. To show $\mathrm{ed}(Y/X; p) \geq \mathrm{ed}(Y/H \rightarrow X; p)$, after shrinking X , we may assume there is a map $f : X \rightarrow X'$ such that $Y = f^* Y'$ for a finite étale covering $Y' \rightarrow X'$, which may be assumed to be connected and Galois by Lemma 2.1.4. 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 when $p \nmid n$, we may assume there is a map $f : X \rightarrow X'$ such that $Y/H = f^*Y'$ for a finite étale covering $Y' \rightarrow X'$, which we may again assume is connected and Galois with group G/H . The image, c , of $Y' \rightarrow X'$ under

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

is the obstruction to lifting $Y' \rightarrow X'$ 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 an étale covering $X'_1 \rightarrow X'$ of order dividing a power n such that $c|_{X'_1}$ is trivial [FD93, Lemma 4.17]. In particular, $X'_1 \rightarrow X'$ has order prime to p . Replacing $Y \rightarrow X \rightarrow X'$ by their pullbacks to X'_1 , we may assume that $c = 0$, and that $Y' = Y''/H$ for some Galois covering $Y'' \rightarrow X'$ with group G .

The difference between the G -coverings $Y \rightarrow X$ and $f^*Y'' \rightarrow X$ 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 $\text{ed}(Y/X; p) \leq \text{ed}(Y/H \rightarrow X; p)$, \square

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, commutative, 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 $\bigoplus_{i \in I} \mathbb{Z}/p^{n_i} \mathbb{Z}$ by a group scheme of the form $\bigoplus_{j \in J} \mu_p^{m_j}$ for integers $n_i, m_j \geq 1$. In this subsection we study the classification of these extensions.

3.1.1. Now let $\tilde{X} = \text{Spec } A$ 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

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

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

$$\begin{array}{ccccccc} 1 & \longrightarrow & A^\times / (A^\times)^{p^n} & \longrightarrow & H^1(\tilde{X}, \mu_{p^n}) & \longrightarrow & H^1(\tilde{X}, \mathbb{G}_m) \\ & & \downarrow & & \downarrow & & \downarrow \\ 1 & \longrightarrow & A[1/p]^\times / (A[1/p]^\times)^{p^n} & \longrightarrow & H^1(X, \mu_{p^n}) & \longrightarrow & H^1(X, \mathbb{G}_m) \end{array}$$

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

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

Here and below, the group on the left denotes extensions as sheaves of $\mathbb{Z}/p^n \mathbb{Z}$ -modules.

Similarly, we can classify extensions of $\mathbb{Q}_p/\mathbb{Z}_p$ by $\mu_{p^\infty} = \varinjlim_n \mu_{p^n}$ as p -divisible groups. If \mathcal{E} is such an extension, then $\mathcal{E}[p^n]$ is an extension of $\mathbb{Z}/p^n\mathbb{Z}$ by μ_{p^n} and we have

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

If A is complete and local with residue field k , then the right hand side may be identified with $A^{\times,1} \subset A^\times$, the subgroup of units which map to 1 in k^\times . Thus we have

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

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, XI, Thm 3.13], and we have a commutative diagram

$$\begin{array}{ccc} A^\times / (A^\times)^{p^n} & \xrightarrow{\sim} & H^1(\tilde{X}, \mu_{p^n}) \\ \downarrow & & \downarrow \\ A[1/p]^\times / (A[1/p]^\times)^{p^n} & \xrightarrow{\sim} & H^1(X, \mu_{p^n}) \end{array}$$

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

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

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

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

$$f : \tilde{X} \rightarrow \tilde{Y} = \text{Spec } B$$

a local flat map of complete local V -algebras. Suppose that $c \in H^1(Y, \mu_{p^n})$, where $Y = \text{Spec } B[1/p]$, 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 . \square

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

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

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

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

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

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

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

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. \square

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 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 $c_{i,j} \in \text{Ext}_R^1(\mathbb{Z}/p\mathbb{Z}, \mu_p)$.

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

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

introduced in §3.1. The universal extension of p -divisible groups over R gives rise to a $g \times g$ matrix of elements $(\hat{c}_{i,j}) \in \text{Ext}_R^1(\mathbb{Q}_p/\mathbb{Z}_p, \mu_{p^\infty})$ 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 $R' = k \oplus L \subset R/(\pi, \bar{\mathfrak{m}}_R^2)$. Using the isomorphism $\hat{\theta}_{R'}$, one sees that $\mathcal{A}_R[p^\infty]|_{R/(\pi, \bar{\mathfrak{m}}_R^2)}$ is defined over R' . If $L \subsetneq \bar{\mathfrak{m}}_R/\bar{\mathfrak{m}}_R^2$, then there exists a surjective map $R/(\pi, \bar{\mathfrak{m}}_R^2) \rightarrow k[x]/x^2$ which sends L to zero. Specializing $\mathcal{A}_R[p^\infty]|_{R/(\pi, \bar{\mathfrak{m}}_R^2)}$ 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 $\text{Spec } k[x]/x^2$. 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. \square

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 $\tilde{X} = \text{Spec } A[1/p]$ and $\tilde{X} = \text{Spec } A$.

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

$$f : \tilde{X} \rightarrow \tilde{Y} = \text{Spec } B$$

be a local flat map of complete local V -algebras. Set $Y = \text{Spec } B[1/p]$. 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 $\text{Ext}_{\tilde{Y}}^1(\mathbb{Z}/p\mathbb{Z}, \mu_p)$, 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. \square

3.2.5. Fix an integer $g \geq 1$, a prime $p \geq 2$, and a positive integer $N \geq 2$ coprime to p . Consider the ring $\mathbb{Z}[\zeta_N][1/N]$, where ζ_N is a primitive N^{th} root of 1. Using the isomorphism $\mathbb{Z}/N\mathbb{Z} \xrightarrow[1 \mapsto \zeta_N]{\sim} \mu_N$, for any $\mathbb{Z}[\zeta_N][1/N]$ -scheme T , and any principally polarized abelian scheme A over T , the N -torsion scheme $A[N]$ is equipped with the (alternating) Weil pairing

$$A[N] \times A[N] \rightarrow \mathbb{Z}/N\mathbb{Z}.$$

We denote by $\mathcal{A}_{g,N}$ the $\mathbb{Z}[\zeta_N][1/N]$ -scheme which is the coarse moduli space of principally polarized abelian schemes A of dimension g equipped with a symplectic basis of $A[N]$. When $N \geq 3$, this is a fine moduli space which is smooth over $\mathbb{Z}[\zeta_N][1/N]$. For a $\mathbb{Z}[\zeta_N][1/N]$ -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 $\mathcal{A}_{g,N}$.

Suppose that $N \geq 3$, and let $\mathcal{A} \rightarrow \mathcal{A}_{g,N}$ 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 $\mathbb{Z}[\zeta_N][1/Np]$. 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 $\mathcal{A}_{g,N}^{\text{ord}} \subset \mathcal{A}_{g,N} \otimes \mathbb{F}_p$. For any N , we denote by $\mathcal{A}_{g,N}^{\text{ord}} \subset \mathcal{A}_{g,N} \otimes \mathbb{F}_p$ the image of $\mathcal{A}_{g,N,N'}$ for any $N' \geq 3$ coprime to N and 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 . We assume that K is equipped with a choice of primitive N^{th} root of 1, $\zeta_N \in K$. We remind the reader regarding the convention for the definition of ed and $\text{ed}(\cdot; p)$ introduced in 2.2.6.

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 $\mathcal{A}_{g,N}^{\text{ord}} \subset$*

$\mathcal{A}_{g,N/k}$. 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 $U_K \rightarrow \mathcal{Z}_K$ of degree prime to p at the generic points of U_K , and a map $h : U_K \rightarrow Y_K$ 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 $U_K \rightarrow Y_K$ is flat.

Let $\tilde{\mathcal{Z}}$ be the normalization of \mathcal{Z} in U_K . Let \mathfrak{p} be the generic point of \mathcal{Z}_k , and $\mathfrak{q}_1, \dots, \mathfrak{q}_m$ the primes of $\tilde{\mathcal{Z}}$ over \mathfrak{p} . Since the degree of $\tilde{\mathcal{Z}} \rightarrow \mathcal{Z}$ over \mathfrak{p} is prime to p , for some i the ramification degree $e(\mathfrak{q}_i/\mathfrak{p})$ and the degree of the residue field extension $\kappa(\mathfrak{q}_i)/\kappa(\mathfrak{p})$ are prime to p . In particular, the residue field extension is separable. By Abhyankar's Lemma, it follows that, after replacing K by a finite extension, we may assume that $e(\mathfrak{q}_i/\mathfrak{p}) = 1$ for some i , and that $\tilde{\mathcal{Z}} \rightarrow \mathcal{Z}$ is étale at \mathfrak{q}_i . Shrinking U_K further if necessary, we may assume that there is an affine open $\mathrm{Spec} B = U \subset \tilde{\mathcal{Z}}$ such that $U_k \rightarrow \mathcal{Z}_k$ has dense image, $U \otimes K = U_K$, and $U \rightarrow \mathcal{Z}$ 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 $h : U \rightarrow Y = \mathrm{Spec} C$. Let $J \supset (p)$ be an ideal of C , and $Y_J \rightarrow Y$ 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 $U_J \rightarrow Y_J$ is flat. Since U is normal, the map $U_J \rightarrow U$ is an isomorphism over the generic points of $U \otimes k$. Hence, after replacing Y by an affine open in Y_J , and shrinking U , we may assume that $U \rightarrow Y$ 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 \hat{B} and \hat{C} , denote the p -adic completions of B and C respectively, and set $\hat{U} = \mathrm{Spec} \hat{B}$ and $\hat{Y} = \mathrm{Spec} \hat{C}$.⁴ Since $\mathcal{A}[p]|_{\hat{U}}$ is ordinary, there is a finite étale covering $\hat{U}' = \mathrm{Spec} \hat{B}' \rightarrow \hat{U}$ such that $\mathcal{A}[p]|_{\hat{U}'}$ is an extension of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g . Hence by Lemmas 2.1.6 and 2.1.8, $\hat{U}'_K \rightarrow \hat{Y}'_K$ factors through a finite étale map $\hat{Y}'_K \rightarrow \hat{Y}_K$ such that $\mathcal{A}[p]|_{\hat{U}'_K}$ is the pullback of an extension \mathcal{F}' of $(\mathbb{Z}/p\mathbb{Z})^g$ by μ_p^g on \hat{Y}'_K . As \hat{U}' is normal, we may assume \hat{Y}'_K is normal.

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

$$\hat{U}' \rightarrow \hat{Y}' \rightarrow \hat{Y}.$$

As \hat{Y}' is normal, $\hat{U}' \rightarrow \hat{Y}'$ is flat over the generic points of \hat{Y}'_k . Hence, there exists $f_0 \in \hat{C}'/\pi\hat{C}'$ which is nowhere nilpotent on \hat{Y}'_k , and such that $\hat{U}'_k \rightarrow \hat{Y}'_k$ is flat

⁴Although it would in some sense be more natural to work with formal schemes here, we stay in the 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.

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 completions⁵ of $C'[1/f]$ and $B'[1/f]$. Let $\widehat{U}'' = \text{Spec } \widehat{B}''$ and $\widehat{Y}'' = \text{Spec } \widehat{C}''$. Then \widehat{U}'' is flat over \widehat{Y}'' by [Gro61, IV, 11.3.10.1]. Moreover, since $\widehat{U} \rightarrow \widehat{Y}$ 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.

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

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

are formally étale, $\mathcal{O}_{\widehat{U}''_k, x}$ is naturally isomorphic to the complete local ring at the image of x in \mathcal{Z} . Let R be the universal deformation \mathcal{O}_K -algebra of the abelian scheme \mathcal{A}_x . Then $\mathcal{O}_{\widehat{U}''_k, x}$ is naturally a quotient of R . The map $\mathcal{O}_{\widehat{Y}''_k, y} \rightarrow \mathcal{O}_{\widehat{U}''_k, x}$ 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

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

which contradicts our initial assumption. \square

Corollary 3.2.7. *Let $g \geq 1$, be an integer, p any prime, and $N \geq 1$ an integer coprime to p . 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 $\mathcal{A}_{g, N}^{\text{ord}} \subset \mathcal{A}_{g, N/k}$.*

If $N = 1, 2$ we also assume the following condition: For any generic point $\eta \in \mathcal{Z}_k$, and $\bar{\eta}$ the spectrum of an algebraic closure of $\kappa(\eta)$, the abelian variety $\mathcal{A}_{\bar{\eta}}$ over $\bar{\eta}$, has automorphism group equal to $\{\pm 1\}$. Then

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

Proof. If $N \geq 3$, the corollary follows from Theorem 3.2.6 and Lemma 2.2.4.

Suppose $N = 1$ or 2 . Let $N' \geq 3$ be an integer coprime to pN . We may assume that K is equipped with a primitive pN' th root of 1, $\zeta_{pN'}$. The map of K -schemes $\mathcal{A}_{g, pN} \rightarrow \mathcal{A}_{g, N}$, is a covering with group $\text{Sp}_{2g}(\mathbb{F}_p)/\{\pm 1\}$. Consider the maps

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

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

Let $\mathcal{Z}_{N'} = \mathcal{Z} \times_{\mathcal{A}_{g, N}} \mathcal{A}_{g, NN'}$. Our assumption on the automorphisms of $\mathcal{A}_{\bar{\eta}}$ implies that at the generic points of \mathcal{Z}_k , the map $\mathcal{Z}_{N'} \rightarrow \mathcal{Z}$ is étale. Thus, after replacing \mathcal{Z} by a fibrewise dense open, we may assume that $\mathcal{Z}_{N'}$ is smooth over \mathcal{O}_K . The observations of the previous paragraph, Lemma 2.2.7 when $p > 2$, Lemma 2.2.4 and Theorem 3.2.6 imply that we have

$$(3.2.8) \quad \begin{aligned} \text{ed}(\mathcal{A}_{g, pN} |_{\mathcal{Z}_K/\mathcal{Z}_K}; p) &\geq \text{ed}(\mathcal{A}'_{g, pNN'} |_{\mathcal{Z}_{N', K}/\mathcal{Z}_{N', K}}; p) \\ &= \text{ed}(\mathcal{A}_{g, pNN'} |_{\mathcal{Z}_{N', K}/\mathcal{Z}_{N', K}}; p) = \text{ed}(\mathcal{A}[p] |_{\mathcal{Z}_{N', K}/\mathcal{Z}_{N', K}}; p) = \dim \mathcal{Z}_K. \end{aligned}$$

\square

⁵ \widehat{C}'' corresponds to a formal affine open in the formal scheme $\text{Spf } \widehat{C}'$.

Corollary 3.2.9. *Let $g, n \geq 2$ and N a positive integer coprime to n . Consider the finite étale map of $\mathbb{Q}(\zeta_n)$ -schemes $\mathcal{A}_{g,nN} \rightarrow \mathcal{A}_{g,N}$. Then for any $p \mid n$ we have*

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

Proof. A fortiori it suffices to consider the case when $n = p$ is prime, which is a special case of 3.2.7. \square

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 smooth, proper, genus g curves. For any integer n , let $\mathcal{M}_g[n]$ denote the $\mathbb{Z}[\zeta_n][1/n]$ -scheme which is the coarse moduli space of pairs (C, \mathcal{B}) consisting of a proper smooth curve C of genus g , together with a choice \mathcal{B} of symplectic basis for $J(C)[n]$, where $J(C)$ denotes the Jacobian of C . For $n \geq 3$ this is a fine moduli space which is smooth over $\mathbb{Z}[\zeta_n][1/n]$ [DM69].

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

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

Proof. Let $N \geq 3$ be an integer. There is a natural map of $\mathbb{Z}[\zeta_N][1/N]$ -schemes $\varpi : \mathcal{M}_g[N] \rightarrow \mathcal{A}_{g,N}$ taking a curve to its Jacobian. For (C, \mathcal{B}) in $\mathcal{M}_g[N]$ the pairs $(J(C), \mathcal{B})$ and $(J(C), -\mathcal{B})$ are isomorphic via -1 on $J(C)$. Thus $(C, \mathcal{B}) \mapsto (C, -\mathcal{B})$ is an involution Σ of $\mathcal{M}_g[N]$, which is non-trivial, unless $g = 2$. We denote by $\mathcal{M}_g[N]'$ the quotient of $\mathcal{M}_g[N]$ by this involution. When $g \geq 3$, the fixed points of Σ in any fibre of $\mathcal{M}_g[N]$ over $\mathrm{Spec} \mathbb{Z}[\zeta_N][1/N]$, are contained in a proper closed subset. Thus $\mathcal{M}_g[N]'$ is generically smooth over every point of $\mathrm{Spec} \mathbb{Z}[\zeta_N][1/N]$.

By [OS80] 1.11, 2.7, 2.8, the map of $\mathbb{Z}[\zeta_N][1/N]$ -schemes $\mathcal{M}_g[N] \rightarrow \mathcal{A}_{g,N}$ induces a map $\mathcal{M}_g[N]' \rightarrow \mathcal{A}_{g,N}$ which is injective, an immersion if $g = 2$ and an immersion outside the hyperelliptic locus if $g \geq 3$.

It suffices to prove the theorem with n replaced by the prime factor p . Let $N \geq 3$ be coprime to p , and let $\mathcal{M}_g[pN]'' = \mathcal{M}_g[p] \times_{\mathcal{M}_g} \mathcal{M}_g[N]'$. It is enough to show that $\mathrm{ed}(\mathcal{M}_g[pN]''/\mathcal{M}_g[N]'; p) = 3g - 3$. If $p = 2$ then $\mathcal{M}_g[pN]'' = \mathcal{M}_g[pN]'$ as coverings of $\mathcal{M}_g[N]'$, and if $p \geq 3$ we have natural degree 2 maps of coverings of $\mathcal{M}_g[N]'$

$$\mathcal{M}_g[pN]'' \leftarrow \mathcal{M}_g[pN] \rightarrow \mathcal{M}_g[pN]'$$

Thus, using Lemma 2.2.7 when $p \geq 3$, it suffices to show that

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

Since $\mathcal{M}_g[pN]' = \mathcal{A}_{g,pN}|_{\mathcal{M}_g[N]'}$, for example by comparing the degrees of these coverings, and $\mathcal{M}_g[N]'$ meets the ordinary locus in $\mathcal{A}_{g,N} \otimes \mathbb{F}_p$ [FvdG04, 2.3], the theorem now follows from Theorem 3.2.6. \square

3.3.3. We now prove the analogue of Theorem 3.3.2 for the moduli space of hyperelliptic curves. Let S be a $\mathbb{Z}[1/2]$ -scheme. Recall that a *hyperelliptic curve* over S is a smooth proper curve C/S of genus $g \geq 1$, 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} . It is classical (and not hard to see) that over $\mathbb{Z}[1/2]$ one has

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

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 $\mathbb{Z}[\zeta_n][1/n]$ -scheme which is the coarse moduli space of pairs (C, \mathcal{B}) consisting of a hyperelliptic curve C together with a symplectic basis \mathcal{B} for $J(C)[n]$. As above, for $n \geq 3$ this is a fine moduli space which is smooth over $\mathbb{Z}[\zeta_n][1/n]$.

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. There is a natural map of $\mathbb{Z}[1/2]$ -schemes $\mathcal{H}_g \rightarrow \mathcal{M}_g$ which is generically an injective immersion on every fibre over $\mathbb{Z}[1/2]$, as a general hyperelliptic curve has only one non-trivial automorphism [Poo00], Thm 1. By the Torelli theorem and [OS80] Cor. 3.2, the map $\mathcal{M}_g \rightarrow \mathcal{A}_g$ is also generically an injective immersion on every fibre over $\mathbb{Z}[1/2]$, and thus so is $\mathcal{H}_g \rightarrow \mathcal{A}_g$.

Now the Jacobian of a hyperelliptic curve over the generic point of \mathcal{H}_g has automorphism group $\{\pm 1\}$ [Mat58] p. 790, and \mathcal{H}_g meets the ordinary locus of $\mathcal{A}_g \otimes \mathbb{F}_p$ by [GP05], Theorem 1. Hence the theorem follows from Corollary 3.2.7. \square

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 $g > 2$. To explain this, recall that for a finite group G , and a prime p , $\mathrm{ed}(G; p)$ denotes the supremum of $\mathrm{ed}(Y/X; p)$ taken over all G -covers Y/X of finite type K -schemes, for any characteristic 0, algebraically closed field K (the definition being independent of K). The covering

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

is a component of $\mathcal{H}_g[2]$; for $g > 2$, the cover is disconnected, and all components are isomorphic.⁶ 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].

The lower bound $\mathrm{ed}(\mathcal{H}_g[2]/\mathcal{H}_g; 2) \geq g + 1$ can actually be recovered using the techniques of this paper. The point is that although $\mathcal{H}_g \rightarrow \mathcal{A}_g$ is not generically an immersion in characteristic 2, one can show that the image of the map on tangent spaces at a generic point has dimension $g + 1$. We are grateful to Aaron Landesman for showing us this calculation.

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.

⁶The monodromy of $\mathcal{H}_g[2] \rightarrow \mathcal{H}_g$ was computed by Jordan [Jo1870, p. 364, §498] to factor as $SB_{2g+2} \rightarrow S_{2g+2} \hookrightarrow \mathrm{Sp}_{2g}(\mathbb{F}_2)$, where $SB_{2g+2} = \pi_1(\mathcal{H}_g)$ denotes the spherical braid group. See also [Dic08, p. 125], or for a more recent treatment, see the $q = 2$ case of [McM13, Theorem 5.2]. The connected components of the cover are in bijection with the cosets $\mathrm{Sp}_{2g}(\mathbb{F}_2)/S_{2g+2}$. The equivalence of the components follows from the monodromy computation.

4.1.1. Let F be a number field and $G = G^{\text{ad}}$ 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

$$(4.1.2) \quad 1 \rightarrow G \rightarrow \text{Aut}(G) \rightarrow \text{Out}(G) \rightarrow 1$$

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

We will also make use of the notion of the *fundamental group* $\pi_1(G)$ [Bor96]. This is a finite abelian group equipped with a $\text{Gal}(\bar{F}/F)$ -action. As an étale sheaf on $\text{Spec } F$, one has $\pi_1(G) \otimes \mu_n \xrightarrow{\sim} \ker(G^{\text{sc}} \rightarrow G)$ where G^{sc} is the simply connected cover of G^{der} , and n is the order $\ker(G^{\text{sc}} \rightarrow G)$.

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*

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

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

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

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

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

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

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

is surjective.

Next we remark that the map

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

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

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

there is an isomorphism $\tau : G \xrightarrow{\sim} H$ over \bar{F} , such for $g \in G(\bar{F})$ and $\sigma \in \text{Gal}(\bar{F}/F)$, we have $\tau(\sigma(g)) = (\sigma(\tau(g)))^{x_\sigma}$. We have a commutative diagram

$$\begin{array}{ccc} H^1(F, \text{Aut}(G)) & \longrightarrow & \prod_{v \in S} H^1(F_v, \text{Aut}(G)) \\ \tau \downarrow \sim & & \tau|_{F_v} \downarrow \sim \\ H^1(F, \text{Aut}(H)) & \longrightarrow & \prod_{v \in S} H^1(F_v, \text{Aut}(H)) \end{array}$$

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

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

is surjective, which we saw above. \square

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 $h : \mathbb{C}^\times \rightarrow G(\mathbb{R})$. 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 $G^{\text{ad}}(\mathbb{R})$ is maximal compact and $X = G(\mathbb{R})/K_\infty$ is a Hermitian symmetric domain.

Let \mathbb{A} denote the adèles over \mathbb{Q} and \mathbb{A}_f the finite adèles. 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

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

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, $\text{Sh}_K(G, X)$.

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 $\text{GSp} = \text{GSp}(V, \psi)$. We denote by S^\pm the conjugacy class of maps $h : \mathbb{C}^\times \rightarrow \text{GSp}(\mathbb{R})$ satisfying 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 (GSp, S^\pm) is a Shimura datum called the *Siegel datum*, and $\text{Sh}_K(\text{GSp}, S^\pm)$ 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 $\iota : G \hookrightarrow \text{GSp}$ of reductive groups over \mathbb{Q} which induces $X \rightarrow S^\pm$. 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 $K_p K^p$ 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_λ} [Kis10, Thm. 2.3.8], [KMP16, Thm. 1], which we will denote by $\mathcal{S}_K(G, X)$. In particular, we may apply this to $\mathrm{Sh}_{K'}(\mathrm{GSp}, S^\pm)$ if we take $K' = K'_p K'^p$ 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_λ} -schemes

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

which is locally on the source an embedding [KP, 4.1.5], [Kis10, Prop. 2.3.5]. That is, if $x \in \mathcal{S}_K(G, X)$ 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 $\mathcal{S}_K(G, X)$, whose special fibre is dense in $\mathcal{S}_K(G, X) \otimes \mathbb{F}_p$, 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 $\mathcal{S}_{K'}(\mathrm{GSp}, S^\pm)$. 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 a Galois closure of the étale local system $\mathcal{A}[p]|_{\mathrm{Sh}_K(G, X)} \rightarrow \mathrm{Sh}_K(G, X)$ is given by a congruence cover $\mathcal{S}_K(G, X)_p \rightarrow \mathcal{S}_K(G, X)$, with monodromy group isomorphic to $G^{\mathrm{der}}(\mathbb{F}_p)$ over every geometrically connected component of $\mathrm{Sh}_K(G, X)$.*

Moreover,

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

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

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

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

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

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

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

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 2.2.4 we have

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

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 $\mathcal{S}_{K'}(\mathrm{GSp}, S^\pm)$ by [Wor, Thm. 1.1]. Now using that for some N with $(N, p) = 1$, there is a surjective map $\mathcal{A}_{g, N} \rightarrow \mathrm{Sh}_{K'}(\mathrm{GSp}, S^\pm)$, and Theorem 3.2.6, we conclude

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

□

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. The group $G^{\mathrm{ad}}(\mathbb{R})$ is a product of simple groups $G_i(\mathbb{R})$, for i in some index set I . We denote by I_{nc} (resp. I_c) the set of i with G_i non-compact (resp. compact). Then X is a product of the irreducible Hermitian symmetric domains $X_i = G_i(\mathbb{R})/K_i$, for $i \in I_{nc}$, where $K_i \subset G_i(\mathbb{R})$ is maximal compact. We use Deligne's notation [Del79] for the classification of these irreducible Hermitian symmetric domains. Since we are assuming G is of classical type, for $i \in I_{nc}$, X_i is of type $A, B, C, D^{\mathbb{R}}$ or $D^{\mathbb{H}}$. The group $G_i(\mathbb{R})$ is either the adjoint group of $U(p, q)$ in case of type A , of $\mathrm{Sp}(2n)$ in the case of type C , 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_i is of type $D^{\mathbb{H}}$.

Since G is almost simple, for $i \in I_{nc}$ the X_i are all of the same type, except possibly if G is of type D , in which case it is possible that both factors of type $D^{\mathbb{R}}$ and $D^{\mathbb{H}}$ occur among the X_i . We will say that G is of *Hodge type* if all the factors X_i are of the same type $A, B, C, D^{\mathbb{R}}, D^{\mathbb{H}}$ and the following condition holds: G is simply connected, unless the X_i are of type $D^{\mathbb{H}}$, in which case $G(\mathbb{C})$ is a product of special orthogonal groups.

4.3.2. 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 $i \in I_{nc}$, $K_i \subset G_i$ 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 $h, h^{-1} : U(1) \rightarrow G_i$ 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.

4.3.3. 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 $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ leaves Σ invariant. 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.

4.3.4. 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 $i : G' \rightarrow G$ 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 $\text{Sh}_K(G, X)$ have the form $\Gamma \backslash X$, where $\Gamma \subset G^{\text{ad}}(\mathbb{Q})$ is the image of a congruence subgroup of $G^{\text{der}}(\mathbb{Q})$; this was already used in the proof of Lemma 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 $K = K^p K_p \subset G(\mathbb{A}_f)$ and $K_1 = K^p K_p^1 \subset G(\mathbb{A}_f)$ be compact open, with $K_p \subset G(\mathbb{A}_f^p)$, $K_p = G_{\mathbb{Z}_p}(\mathbb{Z}_p)$ and $K_p^1 = \ker(G_{\mathbb{Z}_p}(\mathbb{Z}_p) \rightarrow G_{\mathbb{Z}_p}(\mathbb{F}_p))$. Let $\Gamma = G(\mathbb{Q}) \cap K$ and $\Gamma_1 = G(\mathbb{Q}) \cap K_1$. We call a covering of the form $\Gamma_1 \backslash X \rightarrow \Gamma \backslash X$ a *principal p -level covering*.

Theorem 4.3.5. *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, $\Gamma_1 \backslash X \rightarrow \Gamma \backslash X$ we have*

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

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 $G^{\text{ad}}(\mathbb{R})$ -conjugacy class of cocharacters $h : U(1) \rightarrow G^{\text{ad}}$, which we denote by X^{ad} . Then $(G^{\text{ad}}, X^{\text{ad}})$ is a Shimura datum and its reflex field corresponds to the subgroup of $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ 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 $E(G^{\text{ad}}, X^{\text{ad}})$ with $\kappa(\lambda') = \mathbb{F}_p$.

Then one sees using [Del79, Prop. 2.3.10] that one can choose a Shimura datum of Hodge type (G, X) with $G^{\text{der}} = G'$ and adjoint Shimura datum $(G^{\text{ad}}, X^{\text{ad}})$, and so that all primes of $E(G^{\text{ad}}, X^{\text{ad}})$ 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. \square

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

Corollary 4.3.7. *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 $G'^{\text{ad}}(\mathbb{R})$ are all isomorphic to the adjoint group of one of $U(n, n)$, $\text{SO}(n, 2)$ with $n \neq 6$, or $\text{Sp}(2n)$ for some positive integer n .*

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

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

Proof. If G' splits over \mathbb{Q}_p then $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ 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 $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ leaves $\Sigma(G)$ stable. \square

4.3.8. 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 semisimple and H^{ad} is absolutely simple. (That is, it remains simple over an algebraic closure). We have the following result.

Proposition 4.3.9. *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*

$$e = \text{ed}(\Gamma' \backslash X \rightarrow \Gamma \backslash X; p)$$

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 $\bar{G} = \text{Res}_{\mathbb{F}_q/\mathbb{F}_p} H$. 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 semisimple 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 $SU(\frac{n}{2}, \frac{n}{2})^r$ if n is even and $SU(\frac{n-1}{2}, \frac{n+1}{2})^r$ if n is odd. If H is Sp_{2n} we take $G_{\mathbb{R}} = Sp_{2n}^r$. If H is a form of SO_{2n} we take $G_{\mathbb{R}}$ to be $SO^*(2n)^r$, the inner form of (the compact group) $SO(2n)$ which gives rise to the Hermitian symmetric domain of type D_n^{H} (cf. [Del79, 1.3.9, 1.3.10]). If H is a form of $Spin_n$ we take $G_{\mathbb{R}}$ to be $Spin(n-2, 2)^r$.

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 semisimple 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 4.3.7, except when n is odd and H is a form of SL_n or H is a form of $SO(2n)$. In these cases, we are assuming that H is a split form, so $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ permutes the components of $\Delta(G)$ simply transitively. If H is a form of SL_n or $SO(2n)$ 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 $\text{Gal}(\bar{\mathbb{Q}}_p/\mathbb{Q}_p)$ -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 -admissible. Thus, the proposition follows from Theorem 4.3.5 and the formulae for the dimensions of Hermitian symmetric domains. \square

Corollary 4.3.10. *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 $Y' \rightarrow Y$ 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 4.3.9 and Lemma 2.2.7. \square

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’algèbres 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’équation 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 fünften Grade (Lectures on the Icosahedron and the Solution of the Equation of the Fifth Degree)*, Leipzig, Tübingen, 1884.
- [Kl1887] ———, *Zur Theorie der allgemeinen Gleichungen sechsten und siebenten Grades*, Math. Ann. **28** (1887), 499–532.
- [Kl1888] ———, *Sur la résolution, par les fonctions hyperelliptiques de l’équation du vingt-septième degré, de laquelle dépend la détermination 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.
- [Mat58] T. Matsusaka, *On a theorem of Torelli*, Amer. J. Math. **80** (1958), 784–800.
- [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.
- [Poo00] Bjorn Poonen, *Varieties without extra automorphisms. II. Hyperelliptic curves*, Math. Res. Lett. **7** (2000), no. 1, 77–82.
- [OS80] F. Oort and J. Steenbrink, *The local Torelli problem for algebraic curves*, Journées de Géométrie Algébrique d’Angers, Juillet 1979/Algebraic Geometry, Angers, 1979, 1980, pp. 157–204.

- [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
E-mail address: farb@math.uchicago.edu

DEPARTMENT OF MATHEMATICS, HARVARD
E-mail address: kisin@math.harvard.edu

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA-IRVINE
E-mail address: wolfson@uci.edu