

EXPANDER GRAPHS, GONALITY AND VARIATION OF GALOIS REPRESENTATIONS

JORDAN S. ELLENBERG, CHRIS HALL, AND EMMANUEL KOWALSKI

ABSTRACT. We show that families of coverings of an algebraic curve where the associated Cayley-Schreier graphs form an expander family exhibit strong forms of geometric growth. We then give many arithmetic applications of this general result, obtained by combining it with finiteness statements for rational points of curves with large gonality. In particular, we derive a number of results concerning the variation of Galois representations in one-parameter families of abelian varieties.

1. INTRODUCTION

When $A \rightarrow B$ is a family of abelian varieties over a base B , there is a general philosophy that "most" fibers A_b , where b ranges over closed points of B , should have properties similar to that of the generic fiber A_η . In the present paper we develop a very general method to prove statements of this kind, where the properties of abelian varieties we study pertain to the images of their ℓ -adic Galois representation, or to the presence of "extra" algebraic cycles, and where the base B is a curve over a number field. Notably, a key role is played by recent results about expansion in Cayley graphs of linear groups over finite fields.

Our motivation for this work comes from our previous paper [23], joint with C. Elsholtz, in which we studied the geometrically non-simple specializations in a family of abelian varieties whose generic fiber is geometrically simple. As pointed out by J. Achter (and indicated in a note of [23]), D. Masser previously studied questions of a similar nature in [45] using methods arising from transcendence theory.

A particular case of our results and of those of Masser is the following: let $g \geq 2$, let $f \in \mathbb{Z}[X]$ be a squarefree polynomial of degree $2g$, and consider the family of hyperelliptic curves

$$(1) \quad \mathcal{C}_t : y^2 = f(x)(x - t), \quad t \in U = \mathbb{A}^1 - \{\text{zeros of } f\}.$$

The jacobian $J_t = \text{Jac}(\mathcal{C}_t)$ is an abelian variety of dimension g . In fact, the jacobian of the generic fiber, $\text{Jac}(\mathcal{C}_\eta)$, is an absolutely simple abelian variety with geometric endomorphism ring equal to \mathbb{Z} . Masser's methods, as well as ours, can be interpreted as stating that, for "most" t , the specialization J_t is absolutely simple with geometric endomorphism ring \mathbb{Z} . In [23], the parameter t varies over \mathbb{Q} ; by contrast, Masser's methods provide similar results where t is allowed to range over the union of all extensions of degree d of \mathbb{Q} , for any fixed $d \geq 1$.

2000 *Mathematics Subject Classification*. Primary 14G05, 14D10, 05C40, 05C50; Secondary 14K15, 14D05, 35P15.

Key words and phrases. Expanders, Galois representations, rational points, gonality, families of abelian varieties, spectral gap, monodromy.

The prototype of a statement that involves all number fields of degree d is the deep fact that there exist only finitely many j -invariants of CM elliptic curves with bounded degree (or equivalently, in view of the theory of complex multiplication, the class number of imaginary quadratic orders tends to infinity with the absolute value of the discriminant). Our method allows us to prove many new finiteness statements of this nature.

1.1. Statements of results. The new method is quite general. It is based, rather surprisingly, on expansion properties of some families of graphs. We encapsulate a sufficiently strong form of expansion in the following definition:

Definition 1 (Esperantist graphs). Let (Γ_i) be a family of connected r -regular graphs,¹ with adjacency matrices $A(\Gamma_i)$. Let

$$\Delta_i = r\text{Id} - A(\Gamma_i)$$

denote the combinatorial Laplace operator of Γ_i , and let

$$0 = \lambda_0(\Gamma_i) < \lambda_1(\Gamma_i) \leq \lambda_2(\Gamma_i) \leq \dots$$

denote the spectrum of Δ_i . We say that (Γ_i) is an *esperantist family* if it satisfies²

$$(2) \quad \lim_{i \rightarrow +\infty} |\Gamma_i| = +\infty,$$

and if there exist constants $c > 0$ and $A \geq 0$, such that

$$(3) \quad \lambda_1(\Gamma_i) \geq \frac{c}{(\log 2|\Gamma_i|)^A}$$

for all i .

Example 2. In the special case where we can take $A = 0$, we obtain the well-known notion of an *expander family* of graphs, namely

$$(4) \quad \lambda_1(\Gamma_i) \geq c > 0$$

for all i and some constant c independent of i . We refer readers to the survey paper of Hoory, Linial and Wigderson [35] for extensive background information on expansion in graphs, in particular on expanders. In Section 6.1, we will comment on the distinction we make between expander graphs and esperantist graphs.

The following theorem is our main diophantine statement:

Theorem 3. *Let k be a number field. Let U/k be a smooth geometrically connected algebraic curve over k and $(U_i)_{i \in I}$ an infinite family of étale covers of U defined over k . Fix an embedding of k in \mathbb{C} to define the complex Riemann surfaces $U_{\mathbb{C}}$ and $U_{i,\mathbb{C}}$. Let S be a fixed finite symmetric³ generating set of the topological fundamental group $\pi_1(U_{\mathbb{C}}, x_0)$ for some fixed $x_0 \in U$ and assume that the family of Cayley-Schreier graphs $C(N_i, S)$ associated to the finite quotient sets*

$$N_i = \pi_1(U_{\mathbb{C}}, x_0) / \pi_1(U_{i,\mathbb{C}}, x_i), \quad x_i \in U_i \text{ some point over } x_0,$$

¹ We allow our graphs to have self-loops and multiple edges between vertices; see, e.g., [44, §4.2] for references.

² This limit means that for any $N \geq 1$, there are only finitely many $i \in I$ such that $|\Gamma_i| \leq N$; similar limits below have analogue meaning.

³ This means that $s^{-1} \in S$ for all $s \in S$.

is an esperantist family.

Then, for any fixed $d \geq 1$, the set

$$\bigcup_{[k_1:k]=d} U_i(k_1)$$

is finite for all but finitely many i .

Remark 1. We recall the definition of a Cayley-Schreier graph: given a group G with symmetric generating set $S \subset G$ and a subgroup H , the graph $C(G/H, S)$ is defined as the $|S|$ -regular (undirected) graph with vertex set G/H and with (possibly multiple) edges from xH to sxH for all $s \in S$. If $H = 1$, this is the Cayley graph of G with respect to S .

Theorem 3 applies, in particular, when the family is an expander family, which is the case in many of the applications in this paper.

As far as we know, Theorem 3 (and its variants and applications) are the first explicit use of general theorems about spectral gaps in graphs to obtain finiteness statements in arithmetic geometry. However the idea descends from a result of Zograf [62] (and, independently, Abramovich [2]), who proved lower bounds for gonality of modular curves via spectral gaps for the Laplacian on the underlying Riemann surfaces (given by Selberg's 3/16 bound).

We believe that there should exist other arithmetic consequences of the following philosophy: in any category where the notion of finite (Galois) covering makes sense, any family of finite coverings with a similar expansion property should be "extremely complicated". In Section 6, we present some concrete questions along these lines.

In the remainder of the introduction, we present some applications of this theorem. The reader may note that these do not mention explicitly a family of coverings of a fixed curve: those appear only as auxiliary tools in the proofs. The finiteness statements are therefore of a different nature than the finiteness of the set of rational points on some fixed algebraic variety. We focus on abelian varieties, but this is by no means the only area where applications are possible.

First, we will give a strong uniform version of "large Galois image" for certain one-parameter families of abelian varieties:

Theorem 4. *Let k be a number field and U/k a smooth geometrically connected algebraic curve over k . Let $\mathcal{A} \rightarrow U$ be a principally polarized abelian scheme of dimension $g \geq 1$, defined over k , and let*

$$\rho : \pi_1(U_{\mathbb{C}}, x_0) \rightarrow \mathrm{Sp}_{2g}(\mathbb{Z})$$

be the associated monodromy representation. For k_1/k a finite extension and $t \in U(k_1)$, let $\bar{\rho}_{t,\ell}$ be the Galois representation

$$\bar{\rho}_{t,\ell} : \mathrm{Gal}(\bar{k}/k_1) \rightarrow \mathrm{GSp}_{2g}(\mathbb{F}_{\ell})$$

associated to the action on the ℓ -torsion points of \mathcal{A}_t .

If the image of ρ is Zariski-dense in Sp_{2g} , then for any $d \geq 1$ and all but finitely many ℓ , depending on d , the set

$$\bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \text{the image of } \bar{\rho}_{t,\ell} \text{ does not contain } \mathrm{Sp}_{2g}(\mathbb{F}_{\ell})\}$$

is finite.

We proved the case $d = 1$ in our earlier paper [23, Prop. 8].

Corollary 5. *Let k be a number field, and let $f \in k[X]$ be a squarefree polynomial of degree $2g$ with $g \geq 1$. Let U_f be the complement of the zeros of f in \mathbb{A}^1 , and let \mathcal{C}/U be the family of hyperelliptic curves given by*

$$\mathcal{C} : y^2 = f(x)(x - t),$$

with Jacobians $J_t = \text{Jac}(\mathcal{C}_t)$. Then for any $d \geq 1$, the set

$$\bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \text{End}_{\mathbb{C}}(J_t) \neq \mathbb{Z}\}$$

is finite.

Remark 2. This set was also considered by Masser, who gave an explicit upper bound for the cardinality of its subsets of bounded height (see [45, Theorem, p. 459]), namely we have

$$\left| \bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \text{End}_{\mathbb{C}}(J_t) \neq \mathbb{Z} \text{ and } h(t) \leq h\} \right| \ll \max(g, h)^\beta$$

for $h \geq 1$, where $h(x)$ denotes the absolute logarithmic Weil height on \bar{k} and $\beta > 0$ is some (explicit) constant depending only on g . Then, based on concrete examples and other results of André, Masser raised the following question (see [45, middle of p. 460]): is it true, or not, that there are only finitely many t of degree at most d over k such that the geometric endomorphism ring of J_t is larger than \mathbb{Z} ? This corollary gives an affirmative answer.

That being said, contrary to Masser's method, ours does not give explicit or effective bounds on the cardinality of the sets we consider, and hence the two are complementary. (We discussed a similar dialectic in [23].) In particular, Masser's methods can be used to get some control of exceptional fibers in families of abelian varieties over higher-dimensional bases, whereas Theorem 3 does not provide anything interesting in such a situation.

We will next prove that Theorem 3 implies that two families of elliptic curves which are not generically isogenous have few fibers with isomorphic mod- ℓ Galois representations:

Theorem 6. *Let k be a number field and let \mathcal{E}_1 and \mathcal{E}_2 be elliptic curves over the function field $k(T)$. Assume furthermore that \mathcal{E}_1 and \mathcal{E}_2 are not geometrically isogenous. Then, for $d \geq 1$, the set*

$$\bigcup_{[k_1:k]=d} \{t \in k_1 \mid \mathcal{E}_{1,t}[\ell] \text{ and } \mathcal{E}_{2,t}[\ell] \text{ are isomorphic as } G_{k_1}\text{-modules}\}$$

is finite for all but finitely many ℓ .

Our method has also some applications to *arbitrary* one-parameter families of abelian varieties. Using a general “semisimple approximation” of the Galois groups of ℓ -torsion fields (which builds on work of Serre [57]), we will prove the following result on existence, which also exhibits some level of quantitative information on the field of definition (the interest of the latter was suggested by J. Pila):

Theorem 7. *Let k be a number field and let U/k a smooth geometrically connected algebraic curve over k . Let $\mathcal{A} \rightarrow U$ be an abelian scheme of dimension $g \geq 1$, defined over k . Then*

for every $d \geq 1$ there exists an $\ell(d)$ such that, for all primes $\ell > \ell(d)$, the set

$$(5) \quad \bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \mathcal{A}_t[\ell](k_1) \text{ is non-zero}\}$$

is finite, and more precisely there exist $c > 0$ and $A \geq 0$ such that for $\ell > \ell(d)$, the set

$$(6) \quad \bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \text{there exists } e \neq 0 \text{ in } \mathcal{A}_t[\ell] \text{ with } [k_1(e) : k_1] \leq c\ell/(\log \ell)^A\}$$

is finite, where $k_1(e)$ is the field generated by coordinates of e .

Remark 3. The ‘‘Strong Uniform Boundedness Conjecture’’ (which is a theorem due to Merel [47] in the case $g = 1$) makes the much stronger prediction that the set

$$\bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \mathcal{A}_t[\ell](k_1) \text{ is non-zero}\}$$

is empty for ℓ large enough (depending on d), and indeed that this holds even when U is replaced by the entire moduli space of abelian g -folds!

1.2. Outline of the proofs and of the paper. We now briefly summarize the basic ideas in the proofs. For Theorem 3, the argument is quite short but involves a rather disparate combination of ideas. We proceed in four steps, whose combination is rather surprising. First, using the esperantist property and a result of Kelner [39], we show that the genus of the smooth projective models C_i of the U_i goes to infinity; second, we invoke comparison principle between the first eigenvalue of the Cayley-Schreier graphs attached to the covers U_i and the first Laplace eigenvalue on the Riemann surface $U_{i,\mathbb{C}}$ (this goes back to Brooks [12, 11] and Burger [13]); next, we combine these facts to infer, by means of a theorem of Li and Yau [43], that the gonality of U_i tends to infinity; finally, a result of Abramovich and Voloch [4] or Frey [27] (which involve Faltings’ Theorem [25] on rational points on subvarieties of abelian varieties) gives the desired uniformity for points of bounded degree.

For Theorems 4 and 6, it is easy to describe a suitable family of covers for which the conclusion of Theorem 3 leads to the desired conclusion: they are constructed from congruence quotients of the image Γ of the relevant monodromy representation. The main difficulty is to prove that these covers satisfy the esperantist property. In Section 3, we explain different results which provide this property. The easiest case is when Γ has Property (T) of Kazhdan (see [5]), which turns out to happen in the special case of Corollary 5 when $g \geq 2$ (because of a result of J-K Yu [61]). However, most of the time this property is either not known, or not true. When Γ is of infinite index in a lattice in its Zariski-closure, which is a crucial case, we derive the esperantist property by an appeal to the remarkable recent results concerning expansion in linear groups over finite fields. These begin with Helfgott’s breakthrough treatment of SL_2 (see [34]), and further cases are due to Gill and Helfgott [29], Breuillard-Green-Tao [10] and particularly Pyber-Szabó [53]. In the case of Theorem 6, there are very simple concrete examples (due to Nori [49]) where the image of the relevant representation ρ is not a lattice (see Example 15), so that these new developments are absolutely essential.

In the case of Theorem 7, we also require a general result that states, roughly speaking, that the image of the monodromy representation modulo ℓ are ‘‘almost’’ perfect groups generated by elements of order ℓ , which we prove in Section 5. The esperantist property in such a case is also obtained from the work of Pyber and Szabó.

We think that this paper raises a number of interesting questions. In the final Section, we raise a few of them, and also make a few additional comments. Finally, in two appendices, we record some necessary facts about comparison between combinatorial and analytic Laplacians (Appendix A) and semisimple approximation of linear groups over finite fields (Appendix B) which are either difficult to find in the form we need, or not fully spelled out, in the published literature.

Notation. As usual, $|X|$ denotes the cardinality of a set, or, if X is a graph, the cardinality of its vertex set.

By $f \ll g$ for $x \in X$, or $f = O(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geq 0$ such that $|f(x)| \leq Cg(x)$ for all $x \in X$. The “implied constant” refers to any value of C for which this holds. It may depend on the set X , which is usually specified explicitly, or clearly determined by the context.

If U/k is an algebraic curve over a number field, we denote by $U_{\mathbb{C}}$, or sometimes $U(\mathbb{C})$, the associated Riemann surface, with its complex topology. If k is a number field, we write \mathbb{Z}_k for its ring of integers, and

$$\bigcup_{[k_1:k]=d} (\dots)$$

denotes a union over all extensions k_1/k of degree d . When considering étale or topological fundamental groups, we often omit explicit mention of a basepoint.

Acknowledgments. We warmly thank J. Achter for sending us the paper [45] of D. Masser, which motivated us to extend the results of [23] to points of bounded degree. Thanks also to M. Burger for discussions and clarifications concerning the links between expanders and Laplace eigenvalues, and to A. Gamburd for useful discussions at an earlier stage of this project. We also thank P. Sarnak for pointing out to us the paper [62] of P. Zograf and for other enlightening remarks, and J. Bourgain for pointing out that the results of E. Hrushovski [36] are also applicable to obtain gonality growth.

The first-named author’s work was partially supported by NSF-CAREER Grant DMS-0448750 and a Sloan Research Fellowship.

2. GROWTH OF GONALITY IN EXPANDING FAMILIES OF COVERINGS

Theorem 3 is obtained by combining known finiteness statements from arithmetic geometry and a “geometric growth” theorem of independent interest, which we state first. For a smooth curve X/k , where k is a number field, we recall that the *gonality* $\gamma(X)$ is the minimal degree of a dominant morphism from $X_{\mathbb{C}}$ to $\mathbb{P}_{\mathbb{C}}^1$.

Theorem 8 (Growth of genus and gonality). *Let U/\mathbb{C} be a smooth connected algebraic curve over \mathbb{C} . Let $(U_i)_{i \in I}$ be an infinite family of étale covers of U , and let C_i be the smooth projective model of U_i . Let S be a fixed finite symmetric generating set of the topological fundamental group $\pi_1(U, x_0)$ for some fixed $x_0 \in U$. Assume that the family of Cayley-Schreier graphs $C(N_i, S)$ associated to the finite quotient sets*

$$N_i = \pi_1(U, x_0)/\pi_1(U_i, x_i), \quad x_i \in U_i \text{ some point over } x_0,$$

is an esperantist family with constants $c > 0$ and $A \geq 0$.

(a) The genus $g(C_i)$ tends to infinity, i.e., for any $g \geq 0$, there are only finitely many i for which the genus $g(C_i)$ of C_i is $\leq g$.

(b) The gonality $\gamma(U_i)$ also tends to infinity. In fact, there exists a constant $c' > 0$ such that

$$(7) \quad \gamma(U_i) \geq c'|N_i|/(\log 2|N_i|)^{2A}$$

for all i .

Note that (a) is certainly a necessary condition for (b) to be true. However, for the proof of (b), we will need a form of (a), so we have included the statement separately. One may already see that, by applying the Mordell Conjecture (proved by Faltings [24]), one deduces from (a) the case $d = 1$ of Theorem 3. In the setting of Theorem 4, this argument provides a new proof of some of our results in [23].

In order to deduce the full force of Theorem 3 from Theorem 8, we use a well-known and very deep result of Faltings and Frey, which roughly states that curves over number fields only have infinitely many points of bounded degree for “obvious” reasons:

Theorem 9 (Faltings, Frey). *Let k be a number field, and let X/k be a smooth geometrically connected algebraic curve. For any positive integer d such that $\gamma(X) > 2d$, the set*

$$\bigcup_{[k_1:k]=d} X(k_1)$$

is finite, i.e., there are only finitely many points of X defined over an extension of k of degree at most d .

This is Proposition 2 in [27]: Frey shows that the existence of infinitely many points over extensions of k of degree d implies the existence of a non-trivial k -rational map of degree $\leq 2d$ to \mathbb{P}_k^1 , using the main theorem of Faltings on rational points of abelian varieties [24]. (Alternatively, it was observed by Abramovich and Voloch [4] that this follows from a result of Abramovich and Harris [3, Lemma 1] and the theorem of Faltings.)

We now begin the proof of Theorem 8. First, we obtain (a) quite quickly. The basic intuition here is that a graph embedded in a surface of bounded genus can not have a large Cheeger constant. Precisely:

Lemma 10. *Under the condition of Theorem 8, we have*

$$g(C_i) \gg \frac{|N_i|}{(\log 2|N_i|)^A}$$

for all i , where A is the constant appearing in Definition 1.

Proof. Following the ideas of Brooks [12, §1] and of Burger [13] (see also [44, p. 50], and Appendix A), it is known that there is a suitable symmetric set of generators S_0 of $\pi_1(U, x_0)$ such that the Cayley-Schreier graph $\Gamma_i = C(N_i, S_0)$ with respect to S_0 may be embedded in the Riemann surface $U_i(\mathbb{C})$, hence in $C_i(\mathbb{C})$, for all $i \in I$. Moreover, this family (Γ_i) is still an esperantist family (see for instance [44, Th. 4.3.2] for this standard fact).

Now, a beautiful result of Kelner [39, Th. 2.3] shows that the first non-zero eigenvalue $\lambda_1(\Gamma_i)$ satisfies

$$(8) \quad \lambda_1(\Gamma_i) \ll \frac{\max(g(C_i), 1)}{|\Gamma_i|}$$

where the implied constant depends only on the degree of the graph, and the result follows from Definition 1. \square

Using this, we now go to the second part of Theorem 8, the lower bound on the gonality.

Proof of (b). In a slight abuse of notation, we use U_i (resp. C_i) here to refer to the Riemann surfaces $U_i(\mathbb{C})$, $C_i(\mathbb{C})$. Following ideas of Zograf [62] and Abramovich [2, §1], we first use a result of Li and Yau to connect the gonality of U_i to its genus and its first Laplace eigenvalue.

By (a), the universal cover of the (possibly open) curve U_i is the hyperbolic plane \mathbb{H} for all but finitely many i , and we can exclude these exceptions from consideration. We can therefore represent U_i as a quotient

$$U_i \simeq G_i \backslash \mathbb{H},$$

where G_i is a discrete subgroup of $\mathrm{PSL}_2(\mathbb{R})$. From \mathbb{H} , the Riemann surface U_i also inherits the hyperbolic metric and its associated area-element $d\mu = y^{-2}dx dy$. The hyperbolic area of U_i is finite (since U_i differs from the compact curve C_i by finitely many points, i.e., it is a Riemann surface of finite type). Moreover, the Poincaré metric also induces the Laplace operator Δ on the space $L^2(U_i, d\mu)$. Thus one can define the invariant

$$\begin{aligned} \lambda_1(U_i) &= \inf \left\{ \frac{\langle \Delta \varphi, \varphi \rangle}{\|\varphi\|^2} \mid \varphi \text{ smooth and } \int_{U_i} \varphi(x) d\mu(x) = 0 \right\} \\ (9) \quad &= \inf \left\{ \frac{\int_{U_i} \|\nabla \varphi\|^2 d\mu}{\|\varphi\|^2} \mid \varphi \text{ smooth and } \int_{U_i} \varphi(x) d\mu(x) = 0 \right\}, \end{aligned}$$

where

$$\nabla \varphi = y^2(\partial_x \varphi, \partial_y \varphi) : U_i \rightarrow \mathbb{C}^2$$

is the gradient of φ , computed with respect to the hyperbolic metric. It is known that $\lambda_1(U_i)$ is either equal to $1/4$ or to the first non-zero eigenvalue of the laplacian Δ acting on L^2 -functions on U_i .

It follows from the results of Li and Yau that

$$(10) \quad \gamma(U_i) \geq \frac{1}{8\pi} \lambda_1(U_i) \mu(U_i).$$

More precisely, writing $V_c(2, U_i)$ for the conformal area of U_i (as defined in [43, §1]) the easy bound [43, Fact 1, Fact 2]

$$V_c(2, U_i) \leq \gamma(U_i) V_c(2, \mathbb{S}^2) = 4\pi \gamma(U_i)$$

and the key inequality [43, Th. 1]

$$\lambda_1(U_i) \mu(U_i) \leq 2V_c(2, U_i)$$

combine to give (10). Note that, although Li and Yau assume that the surfaces involved are compact, Abramovich [2] explains how the inequality (10) extends immediately to finite area hyperbolic surfaces.

By the Gauss-Bonnet theorem (for finite-area hyperbolic surfaces, see, e.g., [54, Th. B]) we have

$$\mu(U_i) = -2\pi\chi(U_i) = -2\pi(\chi(C_i) - |C_i - U_i|) \geq 4\pi(g(C_i) - 1)$$

where $\chi(\cdot)$ denotes the Euler-Poincaré characteristic, hence (10) leads to

$$(11) \quad \gamma(U_i) \geq \frac{1}{8\pi} \lambda_1(U_i) (-2\pi\chi(C_i)) \geq 2\lambda_1(U_i)(g(C_i) - 1).$$

In turn, Lemma 10 now gives

$$\gamma(U_i) \gg \lambda_1(U_i) \frac{|N_i|}{(\log 2|N_i|)^A}$$

using the esperantist condition (for all but finitely many i).

Finally, the comparison principle of Brooks [11] and Burger [13, 14] relates $\lambda_1(U_i)$ to the combinatorial laplacian of the Cayley-Schreier graphs: by [14, §3, Cor. 1], there exists a constant $c > 0$, depending only on U and on S , such that

$$(12) \quad \lambda_1(U_i) \geq c\lambda_1(\Gamma_i)$$

for all i (Brooks and Burger state their result for *compact* Riemannian manifolds, but they also both mention that they remain valid for finite-area Riemann surfaces; in Theorem 20 in Appendix A, we sketch the extension using Burger's method; see also the recent extension to include infinite-covolume situations by Bourgain, Gamburd and Sarnak [9, Th. 1.2], although the latter does not state precisely this inequality). Using once more the esperantist property, we obtain

$$\gamma(U_i) \gg \frac{|N_i|}{(\log 2|N_i|)^{2A}}$$

for all i (we can adjust the implied constant to make the inequality valid for any finite exceptional set), which is the conclusion (7). \square

Remark 4. Zograf [62, Th. 5] first showed the relevance of arguments of differential geometry of Yang and Yau [60] to prove gonality bounds for modular curves. The result of Li and Yau is similar to that of [60] and both are remarkable in that they prove a lower bound for the degree of any conformal map $C_i \rightarrow \mathbb{S}^2$, in terms of the hyperbolic area of C_i and the first Laplace eigenvalue. These arguments are highly ingenious, involving an application of a topological fixed-point theorem to find a suitable test function in order to estimate λ_1 . Abramovich [2], independently, also applied [43] to modular curves.

Remark 5. There is an intriguing similarity between the proof of Theorem 8 and a beautiful recent result of Gromov and Guth [30, Th. 4.1, 4.2]. Roughly speaking, their result implies that for any family $(M_i \rightarrow M)$ of Galois coverings of hyperbolic 3-manifolds, and for any knot K_i such that K_i is the ramification locus of a map $M_i \rightarrow \mathbb{S}^3$ of degree 3 (which exists by results of Hilden and Montesinos in 3-dimensional topology), the *distortion* of K_i (see [30, §4] for the definition) goes to infinity if the Cayley graphs of $\pi_1(M)/\pi_1(M_i)$ (with respect to a fixed symmetric generating set of $\pi_1(M)$) form an expander family. However, their quantitative lower bound shows that it is enough to consider an *esperantist* family.

3. SOURCES OF EXPANSION

We explain in this section some results which ensure that various families of Cayley-Schreier graphs are esperantist families. Some are quite classical, while others are very recent developments. We try to present these in an understandable manner for non-specialists.

– If G is a finite-index subgroup in $\mathbf{G}(\mathbb{Q}) \cap \mathrm{GL}_m(\mathbb{Z})$, where $\mathbf{G} \hookrightarrow \mathrm{GL}_m$ is a semisimple algebraic subgroup, defined over \mathbb{Q} , and \mathbf{G} has real rank at least 2 (examples include GL_n , $n \geq 3$, or Sp_{2g} , $g \geq 2$, so that G can be a finite-index subgroup of $\mathrm{SL}_n(\mathbb{Z})$, $n \geq 3$, or of $\mathrm{Sp}_{2g}(\mathbb{Z})$, $g \geq 2$) and S is an arbitrary finite set of generators of G , then the family of Cayley graphs $C(\Gamma_i, S)$ of *all* finite quotients Γ_i of G is an expander family, and hence an esperantist family. This is because G has Property (T) of Kazhdan (see [5] for a full treatment of Property (T)).

– Our families of graphs will most often be of the following type: we have a finitely-generated discrete group $G \subset \mathbf{G}(\mathbb{Q}) \cap \mathrm{GL}_m(\mathbb{Z})$ which is *Zariski-dense* subgroup of a semisimple algebraic group $\mathbf{G} \hookrightarrow \mathrm{GL}_m$ (defined over \mathbb{Q}), and we consider the Cayley graphs, with respect to a fixed symmetric set of generators S , of the congruence quotients

$$G_\ell = G / \ker(G \rightarrow \mathbf{G}(\mathbb{F}_\ell)) \subset \mathbf{G}(\mathbb{F}_\ell)$$

(which are well-defined for almost all ℓ after fixing an integral model of \mathbf{G}). Thus G might be of infinite index in the lattice $\mathbf{G}(\mathbb{Q}) \cap \mathrm{GL}_m(\mathbb{Z})$ (the “thin case”, in the terminology suggested by [10]), and neither Property (T) nor automorphic methods are applicable. There has however been much recent progress in understanding expansion properties of Cayley graphs in this situation. We will use mostly the following very general criterion of Pyber and Szabó [53]:

Theorem 11 (Pyber-Szabó). *Let $m \geq 1$ be fixed, let (G_ℓ) be a family of subgroups of $\mathrm{GL}_m(\mathbb{F}_\ell)$ indexed by all but finitely many prime numbers, and let S_ℓ be symmetric generating sets of G_ℓ with bounded order, i.e. $|S_\ell| \leq s$ for all ℓ and some $s \geq 1$. Then, if the groups G_ℓ are all non-trivial perfect groups and are generated by their elements of order ℓ , the family of Cayley graphs $(C(G_\ell, S_\ell))_\ell$ is an esperantist family.*

This follows from [53, Th. 8]: Pyber and Szabó show, under these assumptions, that the diameters d_ℓ of the Cayley graphs $\Gamma_\ell = C(G_\ell, S_\ell)$ satisfy

$$(13) \quad d_\ell \ll (\log |G_\ell|)^{M(m)}$$

where $M(m) \geq 0$ depends only on m , and we can then apply a general bound of Diaconis and Saloff-Coste [20, Cor. 1]: for any finite group G with symmetric generating set S , we have

$$(14) \quad \lambda_1(C(G, S)) \geq \frac{1}{|S| \mathrm{diam}(C(G, S))^2},$$

which translates here to

$$\lambda_1(\Gamma_\ell) \gg \frac{1}{(\log |G_\ell|)^{2A}},$$

proving the esperantist property.

The flexibility and generality of the Pyber-Szabó theorem will be important in Theorem 7. We should however mention some earlier results of similar type. The first breakthrough was Helfgott’s proof of an estimate like (13) for $G_\ell = \mathrm{SL}_2(\mathbb{F}_\ell)$ (see [34, Main th.] and [34, Cor. 6.1]). This was generalized to SL_3 by Helfgott, to SL_n (with some restriction) by Gill and Helfgott [29], and to all cases where $G_\ell = \mathbf{G}(\mathbb{F}_\ell)$ for a simple split Chevalley group \mathbf{G}/\mathbb{Z} by Pyber-Szabó [53] and (independently) Breuillard-Green-Tao [10]. This last result could be used, instead of Theorem 11, for all applications except Theorem 7. In Section 6.1, we will

make some further comments concerning recent extensions of these results which imply that many families of Cayley graphs are in fact expander families.

– The following simple observation will be used to pass from Cayley graphs to Cayley-Schreier graphs:

Proposition 12 (Big quotients remain esperantist). *Let $(C(G_i, S_i))$ be an esperantist family of Cayley graphs, and let $N_i \subset G_i$ be subgroups of G_i such that*

$$\log(2[G_i : N_i]) \geq \delta \log(2|G_i|)$$

for some $\delta > 0$ independent of i . Then the family of Cayley-Schreier graphs $(C(G_i/N_i, S_i))$ is also an esperantist family.

Proof. Because $\Gamma_i = C(G_i/N_i, S_i)$ is a quotient of the Cayley graph $\tilde{\Gamma}_i = C(G_i, S_i)$, the Laplace eigenvalues of $\tilde{\Gamma}_i$ appear among those of Γ_i . Thus

$$\lambda_1(\Gamma_i) \geq \lambda_1(\tilde{\Gamma}_i) \geq \frac{c}{(\log 2|G_i|)^A} \geq \frac{c\delta^A}{(\log 2|G_i/N_i|)^A},$$

which proves the esperantist property of the (Γ_i) . □

We are now ready to give the proofs of the arithmetic applications of Theorem 3 described in the introduction, referring to Section 6.1 for more discussion and comparison of the esperantist condition with the more common expander condition. But before, here are two direct applications of Theorem 8, which seem enlightening.

Proposition 13 (Existence of towers with increasing gonality). *Let X_0/\mathbb{C} be a compact connected Riemann surface of genus $g \geq 2$. There exists a tower*

$$\cdots \rightarrow X_{n+1} \rightarrow X_n \rightarrow X_{n-1} \rightarrow \cdots \rightarrow X_0$$

of étale Galois coverings such that the gonality of X_n tends to infinity as $n \rightarrow +\infty$.

Proof. By Theorem 8, it is enough to construct a tower (X_n) of this type in such a way that the Cayley graphs of the Galois groups form an expander with respect to a fixed set of generators of $\pi_1(X_0)$. This is possible because $\pi_1(X_0)$ is sufficiently big (since $g \geq 2$) to have a quotient which is a discrete group with Property (T), e.g., $\mathrm{SL}_3(\mathbb{Z})$ (see [11, Cor. 6] and the first item in this section). □

The second example illustrates that sometimes esperantism is the best that can be hoped for:

Proposition 14. *Let $U = \mathbb{P}^1 - \{0, 1, \infty\}$, let $x_0 \in U$ be any point, and let $S = \{a_0^{\pm 1}, a_1^{\pm 1}\}$ be the generating set of $\pi_1(U, x_0)$ where a_i is a loop around i . There exists a family of étale Galois covers $(U_{m,k} \rightarrow U)_{m \geq 3, k \geq 2}$ with Galois group $\mathrm{Gal}(U_{m,k}/U) \simeq \mathrm{SL}_m(\mathbb{Z}/k\mathbb{Z})$ such that the Cayley graphs $C(\mathrm{Gal}(U_{m,k}/U), S)$ form an esperantist, but not an expander, family. In particular, for all $N \geq 1$, only finitely many of $U_{m,k}$ have gonality $\leq N$.*

Proof. Kassabov and Riley [40, Th. 1.1] give explicit two-element generating sets $S_m = \{a_m, b_m\}$ of $\mathrm{SL}_m(\mathbb{Z})$ for $m \geq 3$ such that the diameter of $\mathrm{SL}_m(\mathbb{Z}/k\mathbb{Z})$ with respect to $S_m \cup S_m^{-1}$ satisfies

$$d_{m,k} \leq 3600 \log(|\mathrm{SL}_m(\mathbb{Z}/k\mathbb{Z})|),$$

so that the family of Cayley graphs $(C(\mathrm{SL}_m(\mathbb{Z}/k\mathbb{Z}), S_m \cup S_m^{-1}))_{m \geq 3, k \geq 2}$ is an esperantist family, but the Cheeger constant is $\ll 1/m$ (an observation of Y. Luz), so that it can not be an expander family.

Since $\pi_1(U, x_0)$ is a free group generated by a_0 and a_1 , we have surjective homomorphisms

$$\phi_{m,k} \begin{cases} \pi_1(U, x_0) \rightarrow \mathrm{SL}_m(\mathbb{Z}/k\mathbb{Z}) \\ a_0 \mapsto a_m \pmod{k} \\ a_1 \mapsto b_m \pmod{k}, \end{cases}$$

and we can define $U_{m,k}$ as the covering of U associated to the kernel $\ker(\phi_{m,k})$. The Cayley graph $C(\mathrm{Gal}(U_{m,k}/U), S)$ is isomorphic to $C(\mathrm{SL}_m(\mathbb{Z}/k\mathbb{Z}), S_m)$, hence the result follows. \square

4. FIRST ARITHMETIC APPLICATIONS

We give here the proofs of Theorems 4 and 6. Theorem 7, which requires more preparatory work, is considered in the next section.

4.1. Proof of Theorem 4 and Corollary 5. The proof of Theorem 4 begins like the argument in [23]. We denote by $\Gamma \subset \mathrm{Sp}_{2g}(\mathbb{Z})$ the image of the topological monodromy homomorphism ρ associated to \mathcal{A} , and we fix once and for all a finite symmetric generating set S of $\pi_1(U_{\mathbb{C}}, x_0)$.

By hypothesis, Γ is Zariski-dense in $\mathrm{Sp}_{2g}(\mathbb{Z})$, and therefore suitable forms of the Strong Approximation Theorem (see [46]) imply that the image Γ_ℓ of the reduction map

$$\Gamma \rightarrow \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$$

is equal to $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ for all but finitely many ℓ .

The pairs (ℓ, H) , where ℓ is a prime such that $\Gamma_\ell = \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ and $H < \Gamma_\ell$ varies in a fixed set of representatives of the conjugacy classes of maximal proper subgroup of Γ_ℓ form an infinite countable set I . To each such pair $i = (\ell, H)$ corresponds an étale k -covering

$$U_i \xrightarrow{\pi_i} U$$

with a graph isomorphism

$$C(\pi_1(U_{\mathbb{C}}, x_0)/\pi_1(U_{i,\mathbb{C}}, x_i), S) \simeq C(N_i, S)$$

where $N_i = N_{\ell,H} = \Gamma_\ell/H$ and x_i is some point in U_i over x_0 .

In particular, for any finite extension k_1/k , we have

$$\{t \in U(k_1) \mid \mathrm{Im}(\bar{\rho}_{t,\ell}) \not\supset \Gamma_\ell\} \subset \bigcup_{(\ell,H) \in I} \pi_{\ell,H}(U_{\ell,H}(k_1)).$$

Since the set of H for a given ℓ is finite, it follows that Theorem 3 leads to the desired conclusion once we know that the family of Cayley-Schreier graphs $(C(N_i, S))$ is an esperantist family.

We first check (2) holds, which is easy: if the degree of the U_i over U were bounded by some N , the Galois group of the splitting field of U_i/U would be contained in S_N for all i , which is evidently not the case for ℓ large enough.

The esperantist property (3) follows from Theorem 11 of Pyber-Szabó (or from [10]). Precisely, it is well-known that $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ is perfect for $\ell \geq 5$, which we may assume, and generated by elements of order ℓ , and hence we obtain first

$$\lambda_1(C(\Gamma_\ell, S)) \geq \frac{c}{(\log |\Gamma_\ell|)^A}$$

for some $c > 0$ and $A \geq 0$. Then, since $N_{\ell, H} = \Gamma_\ell/H$ and it is known that the index of any maximal subgroup H of $\mathrm{Sp}_{2g}(\mathbb{F}_\ell)$ satisfies

$$|N_{\ell, H}| = [\mathrm{Sp}_{2g}(\mathbb{F}_\ell) : H] \geq \frac{1}{2}(\ell^g - 1)$$

(e.g., from [42, Lemma 4.6] and Frobenius reciprocity), we can apply Proposition 12 to conclude that the family $(C(N_{\ell, H}, S))_{\ell, H}$ is also an esperantist family. This concludes the proof of Theorem 4.

We now come to the proof of Corollary 5. By [23, Prop. 4], we know that, for all $t \in k$ and all sufficiently large ℓ (in terms of g), the surjectivity of the mod ℓ Galois representation

$$\bar{\rho}_{t, \ell} : \mathrm{Gal}(\bar{\mathbb{Q}}/k(\zeta_\ell)) \rightarrow \mathrm{Sp}(J(\mathcal{C}_t)[\ell]) \cong \mathrm{Sp}_{2g}(\mathbb{F}_\ell)$$

implies that $\mathrm{End}_{\mathbb{C}}(J(\mathcal{C}_t)) = \mathbb{Z}$.

Thus it is enough to prove that Theorem 4 is applicable to these families of jacobians. This follows from a theorem of J-K. Yu [61, Th. 7.3 (iii), §10]: the image of the monodromy representation is not only Zariski-dense in Sp_{2g} , in that case, it is known precisely to be the principal congruence subgroup

$$\Gamma = \{x \in \mathrm{Sp}_{2g}(\mathbb{Z}) \mid x \equiv 1 \pmod{2}\},$$

which is of finite index in $\mathrm{Sp}_{2g}(\mathbb{Z})$ (Yu derives this from the explicit form of the monodromy around each missing point $t \in \mathbb{C}$ with $f(t) = 0$; indeed, these are $2g$ transvections, and Yu is able to compute precisely the group they generate in $\mathrm{Sp}_{2g}(\mathbb{Z})$). In other words, for this particular case, we can appeal to Property (T) (as explained in the beginning of Section 3) instead of using the Pyber-Szabó theorem. (There is a fairly direct and elementary proof of Property (T) for these groups, due to Neuhauser [48], based on methods of Shalom.)

4.2. Proof of Theorem 6. The idea is quite similar to the proof of Theorem 4. First of all, for any prime ℓ , there exists a cover

$$U_\ell \xrightarrow{\pi_\ell} U$$

defined over k such that U_ℓ parametrizes pairs (t, ϕ) where $t \in U$ and

$$\phi : \mathcal{E}_{1,t}[\ell] \rightarrow \mathcal{E}_{2,t}[\ell]$$

is an isomorphism. It follows that for any finite extension k_1/k , we have

$$\{t \in U(k_1) \mid \mathcal{E}_{1,t}[\ell] \simeq \mathcal{E}_{2,t}[\ell]\} \subset \pi_\ell(U_\ell(k_1)),$$

so that the theorem will follow from Theorem 3 once we establish that the family $(U_\ell)_\ell$ has the desired expansion property.

First of all, we observe that we may assume both \mathcal{E}_1 and \mathcal{E}_2 are non-isotrivial (indeed, since they are not geometrically isogenous, at most one can be isotrivial; if \mathcal{E}_1 is isotrivial and \mathcal{E}_2 is not, then after passing to a finite cover of U , we can assume \mathcal{E}_1 is actually constant, and in that case the curves U_ℓ are isomorphic over \bar{k} to the usual modular curves $X(\ell)$, whose gonality is already known to go to infinity as $\ell \rightarrow \infty$, see [62, Th. 5] and [2]).

Now consider the monodromy representation

$$\rho : \pi_1(U_{\mathbb{C}}, x_0) \rightarrow \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$$

associated to the “split” family $\mathcal{E}_1 \times \mathcal{E}_2$ of abelian surfaces. Let $G \subset \mathrm{SL}_2 \times \mathrm{SL}_2$ denote the Zariski closure of the image of ρ . Because \mathcal{E}_1 and \mathcal{E}_2 are both non-isotrivial, we know that G surjects to SL_2 on each factor, and because \mathcal{E}_1 and \mathcal{E}_2 are geometrically non-isogenous, it follows by the Goursat-Kolchin-Ribet lemma that in fact we have

$$G = \mathrm{SL}_2 \times \mathrm{SL}_2.$$

Let V_ℓ be the curve parameterizing triples (t, ϕ_1, ϕ_2) , where ϕ_i are isomorphisms

$$\phi_i : \mathcal{E}_{1,t}[\ell] \xrightarrow{\sim} (\mathbb{Z}/\ell\mathbb{Z})^2.$$

Then $V_\ell \rightarrow U$ is a Galois covering whose Galois group is contained in $\mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell)$, this containment being an identity for all but finitely many ℓ by strong approximation. We have a map $V_\ell \rightarrow U_\ell$ given by

$$(t, \phi_1, \phi_2) = (t, \phi_2^{-1}\phi_1),$$

which, for almost all ℓ , expresses U_ℓ as the quotient of V_ℓ by the diagonal subgroup $\Delta \subset \mathrm{SL}_2(\mathbb{F}_\ell) \times \mathrm{SL}_2(\mathbb{F}_\ell)$.

The esperantist property for the family (V_ℓ) follows from Theorem 11 (since G_ℓ is perfect for $\ell \geq 5$ and generated by its elements of order ℓ). As in the proof of Theorem 4, it also follows easily, using Proposition 12, for the quotients (U_ℓ) .

Example 15. Let $c \in \mathbb{Q}$ be a fixed rational number not equal to 0 or 1 (for instance $c = 2$). Consider first the Legendre family

$$\mathcal{L} : y^2 = x(x-1)(x-\lambda)$$

over $V = \mathbb{A}^1 - \{0, 1\}$. It is well-known that (± 1) times the image of the associated monodromy representation

$$\pi_1(V, \lambda_0) \rightarrow \mathrm{SL}_2(\mathbb{Z})$$

is the principal congruence subgroup $\Gamma(2)$ of level 2 [49]. Now fix some rational number $c \notin \{0, 1\}$ and take $\mathcal{E}_1 = \mathcal{L}$ and \mathcal{E}_2 defined by

$$\mathcal{E}_{2,\lambda} = \mathcal{L}_{c\lambda},$$

both restricted to a common base U/\mathbb{Q} , where $U = \mathbb{A}^1 - \{0, 1, c^{-1}\}$.

These two families are non-geometrically isogenous, and hence our theorem applies. Its meaning is that, in a very strong sense, the torsion fields of $\mathcal{E}_{1,\lambda}$ and $\mathcal{E}_{2,\lambda}$ tend to be independent. For instance, for a given degree $d \geq 1$, we find that for all $\ell \geq \ell_0(d)$ large enough (depending on d) the set

$$\{\lambda \in \bar{\mathbb{Q}} \mid [\mathbb{Q}(\lambda) : \mathbb{Q}] \leq d, \quad \mathbb{Q}(\lambda, \mathcal{E}_{1,\lambda}[\ell]) = \mathbb{Q}(\lambda, \mathcal{E}_{2,\lambda}[\ell])\}$$

is finite.

Furthermore, in that case, Nori [49] has shown that the image of the monodromy representation

$$\mathrm{Im}(\pi_1(U_{\mathbb{C}}, x_0) \rightarrow \mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z}))$$

is *not* of finite index in $\mathrm{SL}_2(\mathbb{Z}) \times \mathrm{SL}_2(\mathbb{Z})$. This means that our result can not be obtained, in that special case, using only expansion properties of quotients of lattices. We expect that this phenomenon is much more general.

5. GENERAL ABELIAN VARIETIES

In this section, we will prove Theorem 7. However, before doing so, some preliminaries of independent interest are required. Essentially, these amount to proving that, for an arbitrary one-parameter family of abelian varieties $\mathcal{A} \rightarrow U$ over a number field k , the Galois groups of the coverings U_ℓ associated to the kernel of the composition

$$(15) \quad \pi_1(U_{\mathbb{C}}, x_0) \rightarrow \mathrm{GL}_{2g}(\mathbb{Z}) \rightarrow \mathrm{GL}_{2g}(\mathbb{F}_\ell)$$

“almost” satisfy the assumptions of the Pyber-Szabó theorem for all but finitely many ℓ . (Theorems 4 and 6 used special cases of this fact, which were obvious from the underlying assumptions.)

Since the proof of this fact requires quite different arguments of arithmetic geometry than those of the rest of the paper, we state the conclusion in a self-contained way and use it to prove Theorem 7 before going into the details.

Proposition 16. *Let k be a number field and let U/k a smooth geometrically connected algebraic curve over k . Let $\mathcal{A} \rightarrow U$ be an abelian scheme of dimension $g \geq 1$, defined over k . Then there exists a finite étale cover $V \rightarrow U$ such that, if we denote by*

$$\mathcal{A}_V = \mathcal{A} \times_U V \rightarrow V$$

the base change of \mathcal{A} to V , the image of the monodromy action on ℓ -torsion

$$\pi_1(V_{\mathbb{C}}, x_0) \rightarrow \mathrm{GL}_{2g}(\mathbb{F}_\ell)$$

is, for all but finitely many primes ℓ , a perfect subgroup of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$ generated by elements of order ℓ .⁴

Using this, which will be proved later, we can prove Theorem 7.

Proof of Theorem 7. As in the previous results, we denote by U_ℓ the covering of U_ℓ of $U_{\mathbb{C}}$ corresponding to the kernel of the composition

$$\pi_1(U_{\mathbb{C}}, x_0) \rightarrow \mathrm{GL}_{2g}(\mathbb{Z}) \rightarrow \mathrm{GL}_{2g}(\mathbb{F}_\ell).$$

Applying Proposition 16, we find that, possibly after performing a base-change to a fixed finite covering $V \rightarrow U$, the image G_ℓ^0 of this representation is, for all but finitely many ℓ (say, for $\ell \geq \ell_0$), a perfect subgroup of $\mathrm{GL}_{2g}(\mathbb{F}_\ell)$, generated by its elements of order ℓ (which may be trivial). We start by proving (5). Since, clearly, the finiteness of

$$\bigcup_{[k_1:k]=d} \{t \in V(k_1) \mid \mathcal{A}_{V,t}[\ell](k_1) \text{ is non-zero}\}$$

implies that of

$$\bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \mathcal{A}_t[\ell](k_1) \text{ is non-zero}\},$$

we may assume in fact that $V = U$, without loss of generality.

We will now apply Theorem 3 to conclude. Precisely, it is enough to show that the non-trivial geometrically connected components of the (possibly disconnected) covers

$$\mathcal{A}[\ell] \rightarrow U$$

⁴ Note that it is permitted for this subgroup to be trivial.

form an esperantist family as ℓ varies (where the trivial connected component is the image of the zero section $0 : U \rightarrow \mathcal{A}[\ell]$).

We let $(U_{\ell,i} \rightarrow U_{\mathbb{C}})_{\ell,i}$ denote the family of étale covers of $U_{\mathbb{C}}$ arising as all Riemann surfaces coming from non-trivial geometrically connected components of $\mathcal{A}[\ell]$ (the index i parametrizes the components for a given ℓ), ℓ ranging over primes $\geq \ell_0$.

The covering $\mathcal{A}[\ell]_{\mathbb{C}} \rightarrow U_{\mathbb{C}}$ corresponds to the (not-necessarily transitive) action of $\pi_1(U_{\mathbb{C}})$ on $\mathcal{A}[\ell]$, which factors through the quotient $\pi_1(U_{\mathbb{C}}) \rightarrow G_{\ell}^0$. Any component $U_{\ell,i}$ of $\mathcal{A}[\ell] \rightarrow U$ corresponds to an orbit of this action, hence

$$\pi_1(U_{\ell,i,\mathbb{C}})/\pi_1(U_{\mathbb{C}}) \simeq G_{\ell}^0/H_i$$

for some subgroup H_i of G_{ℓ}^0 . Because G_{ℓ}^0 is generated by elements of order ℓ , it cannot act non-trivially on a set of size smaller than ℓ . Thus, $U_{\ell,i,\mathbb{C}} \rightarrow U_{\mathbb{C}}$ is either an isomorphism or

$$(16) \quad \deg(U_{\ell,i,\mathbb{C}} \rightarrow U_{\mathbb{C}}) \geq \ell.$$

For those $\ell \geq \ell_0$ such that G_{ℓ}^0 is non-trivial (hence of order $\geq \ell$), we can apply the Pyber-Szabó Theorem (Theorem 11) to deduce that

$$\lambda_1(C(G_{\ell}^0, S)) \gg \frac{1}{(\log |G_{\ell}^0|)^A} \gg \frac{1}{(\log \ell)^A}$$

for some constant A independent of ℓ (the implied constant depending also on g), and then we derive

$$\lambda_1(C(G_{\ell}^0/H_i, S)) \geq \lambda_1(C(G_{\ell}^0, S)) \gg \frac{1}{(\log \ell)^A} \geq \frac{1}{(\log |G_{\ell}^0/H_i|)^A}$$

for every proper subgroup H_i of G_{ℓ}^0 .

Then, the remaining ℓ , as well as the covers $U_{\ell,i,\mathbb{C}}$ for which $H_i = G_{\ell}^0$, are covers for which $U_{\ell,i}$ is isomorphic to U , and therefore we only need to show that those exist only for finitely many ℓ . Indeed, such geometric components are parametrized by the group $A(K\mathbb{C})$, where $K = k(U)$, which might be infinite (for instance if A is isotrivial, e.g., if it is a product $B \times U$, where B/k is a fixed abelian variety over k). But for each extension k_1/k of degree d , the only geometric components which can contribute to $\mathcal{A}_t[\ell](k_1)$ are those which are themselves defined over the compositum Kk_1 . So what remains is just to show that

$$\bigcup_{[k_1:k]=d} A(Kk_1)[\ell] = 0$$

for all ℓ large enough. This is immediate by spreading out \mathcal{A} and U to a model over an open subscheme of \mathbb{Z}_k , and comparing the torsion of $A(Kk_1)$ with the torsion of the fiber of \mathcal{A} over a finite field.

We consider now the finiteness statement (6), arguing simply that if (t, e) is a pair where $t \in U$ and e is a non-zero torsion point on $\mathcal{A}_t[\ell]$, and if in addition $t \in U(k_1)$ for some extension k_1/k of degree d and $k_1(e)$ has degree d' over k_1 , then (t, e) corresponds to a point $x \in U_{i,\ell}(k_1(e))$ for one among our auxiliary curves. In particular, there are only finitely many such pairs for $dd' \leq 2\gamma(U_{i,\ell})$, which by (7) and (16) translates to the finiteness under the condition

$$dd' \ll \ell/(\log \ell)^{2A},$$

as claimed. □

We now proceed to the proof of Proposition 16. We start with the following general preliminaries from algebraic geometry. If K is a field, then given an abelian variety A/K and a finite extension L/K , we write G_ℓ for the Galois group of $L(A[\ell])/L$ and $G_\ell^+ \leq G_\ell$ for the characteristic subgroup generated by the ℓ -Sylow subgroups of G_ℓ .

The following theorem shows that when K is finitely generated over \mathbb{Q} , there exists an L/K such that G_ℓ^+ and G_ℓ/G_ℓ^+ are very nicely behaved for almost all ℓ . Serre [57] proved it in the special case where K is a number field, and indicated that the same argument should extend to finitely generated fields.

Theorem 17 (Semisimple approximation of Galois groups of torsion fields). *Suppose K/\mathbb{Q} is a finitely generated extension and A/K is an abelian variety of dimension g . Then there is a finite extension L/K and a constant $c = c(K, A)$ depending only on K and A such that if ℓ is a prime number $\geq c$, then*

- (1) G_ℓ/G_ℓ^+ has order prime to ℓ ;
- (2) there is a semisimple group $\mathbf{G}_\ell \subset \mathbf{GL}_{2g}/\mathbb{F}_\ell$ such that $\mathbf{G}_\ell(\mathbb{F}_\ell)^+ = G_\ell^+$;
- (3) if $S_\ell = G_\ell \cap \mathbf{G}_\ell(\mathbb{F}_\ell)$, then G_ℓ/S_ℓ is abelian.

The proof we give for the general case is an adaptation of that of Serre. In particular, the arguments on algebraic subgroups of $\mathbf{GL}_{2g}/\mathbb{F}_\ell$ and their \mathbb{F}_ℓ -rational points are transported essentially unchanged from Serre's paper; the extra ingredient is that we need to invoke finiteness theorems for étale covers of positive-dimensional varieties over number fields, while [57] only needs finiteness theorems for unramified extensions of the number field itself.

Before embarking on the proof of the theorem we remark on one behavior of the Galois groups G_ℓ under finite base change. If L/K is an arbitrary extension, then replacing L by a finite extension L'/L (e.g. the extension induced by a finite extension K'/K) has the effect of replacing G_ℓ, G_ℓ^+ by subgroups H_ℓ, H_ℓ^+ respectively of index at most $[L' : L]$. Since G_ℓ^+ has no proper subgroup of index less than ℓ (because it is generated by its ℓ -Sylow subgroups), we have also $H_\ell^+ = G_\ell^+$ for $\ell > [L' : L]$.

Throughout the proof, we will use “bounded” as shorthand for “bounded by a constant which may depend on K, L, A but which is independent of ℓ .”

Proof. We start by taking $L = K$, but finitely many times throughout the proof of the theorem we will replace L by a finite extension L'/L . By the remark following the statement of the theorem, as far as the groups G_ℓ^+ are concerned, the effect of such a replacement is to increase c . As far as the quotients G_ℓ/G_ℓ^+ are concerned, for $\ell \geq c$, they will be replaced by subgroups $H_\ell/H_\ell^+ \leq G_\ell/G_\ell^+$.

There is a canonical embedding $G_\ell \rightarrow \text{Aut}(A[\ell]) \simeq \text{GL}_{2g}(\mathbb{F}_\ell)$, thus we can apply results of Nori and Serre to the subgroup $G_\ell^+ \leq \text{GL}_{2g}(\mathbb{F}_\ell)$. As summarized in Appendix B, we start by associating to each (finite) subgroup $G \leq \text{GL}_{2g}(\mathbb{F}_\ell)$ the characteristic subgroup $G^+ \leq G$ generated by its unipotent elements, and then we associate to $G^+ \leq \text{GL}_{2g}(\mathbb{F}_\ell)$ an algebraic subgroup $\mathbf{G}^+ \subseteq \mathbf{GL}_{2g}$. One can say quite a bit about \mathbf{G}^+ , especially when G acts semisimply on $A[\ell]$, and as a result one can also say quite a bit about G and G^+ .

If $\ell \geq 2g - 1$, then Proposition 21 implies that G_ℓ/G_ℓ^+ has order prime to ℓ , thus (1) holds.

For some constant $\ell_1 = \ell_1(2g)$, Theorem 23 implies $G_\ell^+ = \mathbf{G}_\ell^+(\mathbb{F}_\ell)^+$, for $\ell \geq \ell_1$. If $\ell \geq c_1(K, A)$, then G_ℓ acts semisimply on $A[\ell]$ (cf. Theorem 1 in [26, VI.3]), so if ℓ also satisfies $\ell \geq \ell_1$, then Corollary 24 implies $\mathbf{G}_\ell = \mathbf{G}_\ell^+$ is semisimple. Hence (2) holds.

We suppose for the remainder of the proof that $\ell \geq \ell_1$ and that \mathbf{G}_ℓ is semisimple, and we write $\mathbf{N}_\ell \subseteq \mathbf{GL}_{2g}$ for the normalizer of \mathbf{G}_ℓ . The fact that G_ℓ normalizes G_ℓ^+ implies it also normalizes \mathbf{G}_ℓ , thus $G_\ell \leq \mathbf{N}_\ell(\mathbb{F}_\ell)$. By Corollary 28, there is a positive integer $r = r(2g)$ (independent of ℓ and \mathbf{G}_ℓ) and a faithful representation $\mathbf{GL}_m \rightarrow \mathbf{GL}_r$ which identifies the image of \mathbf{G}_ℓ with the algebraic subgroup of elements in \mathbf{GL}_m acting trivially on the subspace of \mathbf{G}_ℓ -invariants. Moreover, the image of \mathbf{N}_ℓ in \mathbf{GL}_n stabilizes this space, and for some $s \leq r$, its action on the space induces a faithful representation $\mathbf{N}_\ell/\mathbf{G}_\ell \rightarrow \mathbf{GL}_s$.

Let $S_\ell = G_\ell \cap \mathbf{G}_\ell(\mathbb{F}_\ell)$ and let $J_\ell \leq G_\ell$ be a subgroup of minimal index among those such that $S_\ell \leq J_\ell$ and J_ℓ/S_ℓ is abelian. The image of G_ℓ/S_ℓ in the faithful representation $G_\ell/S_\ell \rightarrow \mathbf{GL}_s(\mathbb{F}_\ell)$ has order prime to ℓ , thus we can lift it to a faithful representation $G_\ell/S_\ell \rightarrow \mathbf{GL}_s(\mathbb{C})$ and apply Jordan's Theorem to infer that $[G_\ell : J_\ell] = [G_\ell/S_\ell : J_\ell/S_\ell]$ is bounded. In particular, we will show that the fixed fields $L(A[\ell])^{J_\ell}$ all lie a single finite extension L'/L , so up to replacing L , (3) will hold.

So far, the argument has paralleled that in [57] quite closely. We now attend to the new features that appear when K/\mathbb{Q} has positive transcendence degree.

Write k for the largest algebraic extension of \mathbb{Q} contained in K , and write S for $\text{Spec } \mathbb{Z}_k$. Let X be a smooth scheme dominant and of finite type over $\text{Spec}(\mathbb{Z})$ such that the function field $k(X)$ is L and such that A has good reduction over L , and let $\pi_1^{\text{ét}}(X)$ be the étale fundamental group of X . For each prime ℓ , let $X[1/\ell]$ be the pullback of X to $\text{Spec}(\mathbb{Z}[1/\ell])$ and let $\pi_1^{\text{ét}}(X[1/\ell])$ be the étale fundamental group of $X[1/\ell]$. The cover $X_\ell \rightarrow X[1/\ell]$ induced by the extension L_ℓ/L is étale because A has good reduction over X , thus G_ℓ is a quotient of $\pi_1^{\text{ét}}(X[1/\ell])$.

Let $\pi_1^t(X[1/\ell])$ denote the quotient of $\pi_1^{\text{ét}}(X[1/\ell])$ corresponding to the maximal étale cover $X' \rightarrow X[1/\ell]$ which is tamely ramified over $X - X[1/\ell]$. The kernel of the quotient map $\pi_1^{\text{ét}}(X[1/\ell]) \rightarrow \pi_1^t(X[1/\ell])$ is generated by pro- ℓ groups (coming from wild ramification), hence the image in G_ℓ of this kernel lies in G_ℓ^+ and the quotient $\pi_1^{\text{ét}}(X[1/\ell]) \rightarrow G_\ell/G_\ell^+$ factors through $\pi_1^t(X[1/\ell]) \rightarrow \pi_1^t(X[1/\ell])$.

Each irreducible component Z of $X - X[1/\ell]$ gives rise to an inertia group in G_ℓ ; we now show that the images of these inertia groups in G_ℓ/G_ℓ^+ generate an *abelian* group.

If $I \leq G_\ell$ is one such inertia group, then I^+ is the unique ℓ -Sylow subgroup of I and $I \rightarrow I/I^+$ splits, so there is an embedding $i : I/I^+ \rightarrow \mathbf{GL}_{2g}(\mathbb{F}_\ell)$ defined up to conjugation by an element of I^+ . If $\ell \geq c_2(K)$, there is a connected torus $\mathbf{I}'/\mathbb{F}_\ell$ in \mathbf{GL}_{2g} such that $i(I/I^+) = \mathbf{I}'(\mathbb{F}_\ell)$ (see [56, Section 1.9]). Moreover, the characters of the induced representation $\mathbf{I}' \rightarrow \mathbf{GL}_{2g}$ all have amplitude at most $2g$ (see the discussion in [32, Section 2]).

One can show that $\mathbf{I}' \subset \mathbf{N}_\ell$, and while \mathbf{I}' depends on our choice of splitting $I/I^+ \rightarrow I$, the image $\mathbf{I} \subset \mathbf{N}_\ell/\mathbf{G}_\ell$ of $\mathbf{I}' \rightarrow \mathbf{N}_\ell/\mathbf{G}_\ell$, which we call an inertial torus, is canonical because I^+ lies in $\mathbf{G}_\ell(\mathbb{F}_\ell)^+$. Above we saw that the induced representation $\mathbf{I} \rightarrow \mathbf{GL}_s$ comes from the action of \mathbf{I}' on the subspace of \mathbf{G}_ℓ -invariants in the tensor representation $\mathbf{G}_\ell \rightarrow \mathbf{GL}_r$, and thus, if $n = r_1(2g)$ is the constant in the statement of corollary 28, then the characters of $\mathbf{I}' \rightarrow \mathbf{GL}_r$ and $\mathbf{I} \rightarrow \mathbf{GL}_s$ have amplitude at most $n \cdot 2g$.

The subgroup $\mathbf{I}'(\mathbb{F}_\ell) \cap J_\ell$ has bounded index in $\mathbf{I}'(\mathbb{F}_\ell)$ because J_ℓ has bounded index in G_ℓ , thus the subgroup of elements in $\mathbf{I}'(\mathbb{F}_\ell)$ which commute with J_ℓ/G_ℓ has the same index or smaller. Therefore, by an argument involving rigidity of tori (cf. [32, §2]), if $\ell \geq c_3(n, 2g)$, then $\mathbf{I}'(\mathbb{F}_\ell)$ commutes with J_ℓ/S_ℓ in G_ℓ/S_ℓ . In particular, $J'_\ell = \mathbf{I}'(\mathbb{F}_\ell)J_\ell$ must lie in J_ℓ because of how we chose the latter. A similar argument shows that any pair of inertial tori commute,

hence the subgroup $\mathbf{T}_\ell \subset \mathbf{N}_\ell/\mathbf{G}_\ell$ generated by all such tori is a connected torus and $\mathbf{T}_\ell(\mathbb{F}_\ell) \leq J_\ell/S_\ell$.

It follows that the image in G_ℓ of the kernel of $\pi_1^{\text{ét}}(X[1/\ell]) \rightarrow \pi_1^{\text{ét}}(X)$ lies in J_ℓ . In other words, there is a maximal normal subgroup $J'_\ell \leq G_\ell$ satisfying $S_\ell \leq J_\ell \leq J'_\ell$ such that the quotient G_ℓ/J'_ℓ is bounded and $\pi_1^{\text{ét}}(X[1/\ell]) \rightarrow G_\ell/J'_\ell$ factors through $\pi_1^{\text{ét}}(X)$. But we know (for instance, by Theorem 2.9 of [33]) that there are only finitely many quotients of $\pi_1^{\text{ét}}(X)$ of bounded index. Thus, we can replace X with some finite étale cover $X' \rightarrow X$ (which has the effect of replacing L with a finite extension of L') and be assured that G_ℓ/J'_ℓ is trivial, which is exactly to say that G_ℓ/S_ℓ is abelian, as desired. \square

We now study the *geometric* Galois group $G_\ell^0 = \text{Gal}(L\bar{k}(A[\ell])/L\bar{k})$.

Theorem 18. *Suppose k/\mathbb{Q} is a finitely generated field and K/k is a finitely generated regular extension. If A/K is an abelian variety of dimension g , then there is a finite extension L/K and a constant $\ell_0(A)$ such that the geometric Galois group G_ℓ^0 is a perfect subgroup of $\text{GL}_{2g}(\mathbb{F}_\ell)$ generated by elements of order ℓ for all $\ell \geq \ell_0(A)$.*

This immediately implies Proposition 16 by taking $K = k(U)$ the function field of U and A/K the generic fiber of $\mathcal{A} \rightarrow U$, after noting that the Riemann surface corresponding to the étale cover of U which has function field $K(A[\ell])$ is the covering U_ℓ defined by (15).

Proof. As in the previous theorem, we start with a fixed L/K (the extension given in the previous theorem), but finitely many times throughout the following proof we may replace L with a finite extension L'/L . As far as the groups G_ℓ^0 are concerned, the effect of such a replacement is to increase ℓ_0 . As far as the quotients G_ℓ/G_ℓ^0 are concerned, for $\ell \geq \ell_0$, they may be replaced by a proper subgroup H_ℓ/H_ℓ^0 .

Let X/k be a smooth geometrically-connected variety such that $K = k(x)$. After replacing X by an open dense subscheme, we may suppose that A has good reduction over X (that is, there is an abelian scheme \mathcal{A}/X whose generic fiber is A .) If we write $\bar{X} = X \times_k \bar{k}$, we have an exact sequence of étale fundamental groups

$$\pi_1^{\text{ét}}(\bar{X}) \longrightarrow \pi_1^{\text{ét}}(X) \longrightarrow \text{Gal}(\bar{k}/k) \longrightarrow 1.$$

Up to replacing k by a finite extension, we may suppose $X(k)$ is non-empty, and thus that this sequence splits. In particular, if $N^0 \leq \pi_1^{\text{ét}}(\bar{X})$ is an open subgroup, then there is an open subgroup $N \leq \pi_1^{\text{ét}}(X)$ such that $N^0 = N \cap \pi_1^{\text{ét}}(\bar{X})$ and $N \rightarrow \text{Gal}(\bar{k}/k)$ is surjective. (In fact, we may just take $N = N^0 \text{Gal}(\bar{k}/k)$ where $\text{Gal}(\bar{k}/k)$ is viewed as a subgroup of $\pi_1^{\text{ét}}(X)$ via the chosen splitting.) Moreover, $\pi_1^{\text{ét}}(\bar{X})$, being topologically finitely generated, has only finitely many quotients of bounded degree, so if we have an infinite family of étale covers $X_\ell \rightarrow X$ with bounded geometric monodromy, then we can find a finite étale cover $X' \rightarrow X$ such that the pullbacks $X'_\ell \rightarrow X'$ all have trivial geometric monodromy.

Theorem 1 of [38] implies that the intersection $[G_\ell, G_\ell] \cap G_\ell^0$ has bounded index in G_ℓ^0 and Theorem 17 above implies $[G_\ell, G_\ell] \leq S_\ell$, so $S_\ell \cap G_\ell^0$ also has bounded index in G_ℓ^0 . Thus up to replacing L by a finite extension, we can assume $G_\ell^0 \leq S_\ell$. The index of G_ℓ^+ in S_ℓ is bounded, thus the index of $G_\ell^0 \cap G_\ell^+$ in G_ℓ^0 is also bounded, so up to replacing L by a finite extension, we may suppose $G_\ell^0 \leq G_\ell^+$.

Suppose the algebraic envelope \mathbf{G}_ℓ of G_ℓ^+ is semisimple and $\mathbf{G}_\ell(\mathbb{F}_\ell)^+ = G_\ell^+$. We say a subgroup $G \leq \text{GL}_{2g}(\mathbb{F}_\ell)$ is quasi-simple if its center $Z \leq G$ has bounded size and if G/Z is a simple group. If $\ell \geq 5$, then G_ℓ^+ is generated by a bounded set Σ_ℓ of pairwise commuting

quasi-simple subgroups of $G \leq \mathrm{GL}_{2g}(\mathbb{F}_\ell)$ such that $G^+ = G$. Moreover, for each $G \in \Sigma_\ell$, the index of $[G, G]$ in G is bounded by $|Z(G)|$, so if ℓ is sufficiently large, then every $G \in \Sigma_\ell$ is perfect. For every normal subgroup $N \leq G_\ell^+$, the commutator subgroup $[N, N]$ has bounded index in N . It is also generated by a subset of Σ_ℓ , so $[N, N]^+ = [N, N]$. This applies in particular to G_ℓ^0 , so up to replacing L by a finite extension L'/L , we may suppose, for all ℓ , that G_ℓ^0 is perfect and generated by its elements of order ℓ . \square

6. FURTHER REMARKS AND QUESTIONS

We conclude this paper with some remarks and further questions.

6.1. Various forms of expansion. The strongest possible form of expansion for a family (Γ_i) of graphs is given by the expander condition. This is in fact often a crucial requirement for applications, as seen for instance in the case of applications of sieve methods in discrete groups with exponential growth (see [41, §5.2] for a discussion). Motivated by these other applications, there has been extensive, and impressive, work towards a proof that various families of graphs are expanders. In particular, after many intermediate works, it has been proved by Salehi-Golsefidy and Varjú [55] that the Cayley graphs of congruence quotients

$$\Gamma_m = \Gamma / \ker(\Gamma \rightarrow \mathrm{GL}_n(\mathbb{Z}/m\mathbb{Z}))$$

form an expander family when m runs over squarefree integers and Γ is a finitely-generated subgroup of $\mathrm{GL}_n(\mathbb{Z})$ which is Zariski-dense in a semisimple algebraic group \mathbf{G}/\mathbb{Q} (the case of $\mathbf{G} = \mathrm{SL}_2$, for m prime, is due to Bourgain-Gamburd [6], and for m squarefree to Bourgain-Gamburd-Sarnak, while Varjú [59] had obtained the result for SL_n).

Note that although many of the graphs we use in this paper are quotients of graphs of this type, this is not the case for all: in Theorem 7, we do not have such precise control of the groups which appear. This is one reason why we have chosen to emphasize the weaker esperantist condition for our graphs. Another is that the starting point in [55] (as in [6] and [59]), when Γ which is not a lattice (so that neither Property (T) nor automorphic methods are available), is the growth theorem of [53] or [10], which by itself implies immediately the esperantist property. Moreover, in terms of effectivity, the esperantist property might be much easier to establish with actual, explicit, constants (we discuss this in Section 6.5).

In the opposite direction, the reader may have noticed that even weaker expansion conditions than (3) lead to a growth of gonality (i.e., to Theorem 8): it would be enough to have a bound of the form

$$(17) \quad \lambda_1(N_i) \geq \vartheta(i)|N_i|^{-1/2}, \quad \text{with} \quad \lim_{i \rightarrow +\infty} \vartheta(i) = +\infty.$$

On the other hand, a variant of the Pyber-Szabó Theorem proving this in the context of Theorem 11 would *not* suffice for this paper, since we applied the bound to quotients of Cayley graphs, and the index of subgroups would not in general be large enough to preserve (17), as in Proposition 12.

Another condition which would suffice for this paper is

$$(18) \quad \lambda_1(N_i) \gg |N_i|^{-\varepsilon}$$

for all i and any $\varepsilon > 0$, the implied constant depending on ε . Indeed, taking $\varepsilon < 1/2$ gives (17), and if M_i is any quotient of N_i with $\log |M_i| \geq c \log |N_i|$ for some fixed constant $c > 0$ (as happens in our applications), taking $\varepsilon < c/4$, say, leads to (17) for (M_i) . This

remark may have some applications since, as J. Bourgain pointed out to us, Hrushovski [36, Th. 1.3, Cor. 1.4] has proved (18) in many cases related to our applications in this paper.

In another direction, one might wonder whether there is any kind of structure theorem for “highly non-expanding” Cayley-Schreier graphs with an eigenvalue violating (17) with $\vartheta(i)$ being, say, a large constant. For instance, if such a graph is associated to a finitely generated group Γ acting on a finite set S , what can one say about the composition factors of the image of Γ in $\text{Aut}(S)$? (Such structure results are known for covers (U_i) with bounded genus, in the work of Guralnick [31] and Frohardt-Magaard [28]; these families, of course, fail to satisfy (13).)

6.2. Relation with the work of Cadoret and Tamagawa. Our main result, and its concrete diophantine applications, are related to recent work of Cadoret and Tamagawa [16, 17]. Given an ℓ -adic representation

$$\rho : \pi_1^{\text{ét}}(X) \rightarrow \text{GL}_m(\mathbb{Z}_\ell)$$

for some “nice” scheme X defined over a field k with étale fundamental group $\pi_1^{\text{ét}}(X)$, with G the image of ρ , they consider the structure (e.g., finiteness properties) of sets of $x \in X(k_1)$, for some k_1/k , such that the image in G of the natural map

$$\text{Gal}(\bar{k}_1/k_1) \rightarrow G$$

associated to x is not *open* (in the ℓ -adic topology), or has large codimension in G , etc. In [16, Th. 1.1], general conditions on ρ are found which imply that such sets of $x \in X(k)$ are finite when X/k is a smooth curve and k finitely generated over \mathbb{Q} and in [17, Th. 1.1], this is extended to all $x \in X(k_1)$ with $[k_1 : k] \leq d$ for $d \geq 1$. The strategy parallels ours: a suitable *tower* $(X_{n+1} \rightarrow X_n)_{n \geq 0}$ of coverings is constructed so that its rational points control the desired set, and Cadoret and Tamagawa show that either the genus [16] or the gonality [17] of the curves X_n tends to infinity. However, the details of the proofs of this facts are strikingly different from our Theorem 8.

Note that although we have not considered such “vertical” towers of coverings in this paper, our results can also be applied in this context. Indeed, works of Bourgain and Gamburd [7, 8] show that families of Cayley graphs of $\text{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$ are expanders, for d and p fixed and n varying, and recently Dinai [21, 22] has proved the polylogarithmic growth of the diameter (implying the esperantist property by (14)) for families $(\mathbf{G}(\mathbb{Z}/p^n\mathbb{Z}))_{n \geq 1}$ when \mathbf{G}/\mathbb{Z}_p is an arbitrary split semisimple algebraic group. The argument is very elementary, and leads to explicit constants (c, A) in (3), which is of great interest when thinking of effectiveness (as discussed below).

6.3. Higher-dimensional families. Our work is intrinsically limited to one-parameter families, in at least two ways: (1) the use of gonality of curves to deduce diophantine consequences through the theorem of Faltings; (2) the use of the Li-Yau inequality to relate gonality to the Laplace operator and then the combinatorial laplacian of graphs. It would be quite interesting to know whether any similar result holds when dealing with families of coverings of higher-dimensional varieties when the associated Cayley-Schreier graphs are expanders or esperantist.

6.4. Extension to positive characteristic. A basic question suggested by Theorem 3 is the following: what happens when the base field k is a global field of positive characteristic? It is easy to modify the assumption so that it makes sense, and we know that some version of the first part of Theorem 8 extends (as follows from [23, Prop. 5, Prop. 7]). However, the crucial step where we use the theorem of Li and Yau is not available for the gonality argument. Moreover, a naïve idea of “lifting” to characteristic zero (if possible) runs into difficulties, since the gonality of a lift might be larger than that over k . It would be very interesting to know if the analogue of this gonality bound is true over all global fields. We therefore raise the following question:

Question 19. Let k be a global field of positive characteristic $p > 0$, or a finite field. Let U/k be a smooth geometrically connected curve, and let (U_i) be a family of finite, tamely ramified, étale covers of U , such that the Cayley-Schreier graphs of the finite quotient sets

$$\pi_1^{\text{et}}(U)/\pi_1^{\text{et}}(U_i)$$

(with respect to a fixed finite, symmetric, set S of topological generators of the tame fundamental group $\pi_1^{\text{tame}}(U)$) form an expander graph. Is it true, or not, that we necessarily have

$$(19) \quad \lim_{i \rightarrow +\infty} \gamma(U_i) = +\infty?$$

Note that in this setting we do have

$$\lim_{i \rightarrow +\infty} g(U_i) = +\infty$$

since in the tamely ramified case we can lift the covering $U_i \rightarrow U$ to a field K of characteristic 0 without changing the genus of either curve, at which point we can embed K in \mathbb{C} and use the arguments of the present paper. (To be precise, we should require that S is the image in $\pi_1^{\text{et}}(U)$ of some generating set of the *discrete* group $\pi_1(U_{\mathbb{C}})$.)

Poonen has shown [52] that (19) holds when $U = X(1)$ is the moduli space of elliptic curves and (U_i) is a sequence of modular curves of increasing level.

It is unclear to us whether any results along the lines of those proved here can be expected when wild ramification is allowed. As a cautionary note we remark that, by contrast with the present paper, Abhyankar has constructed many (wildly ramified) coverings $U_i \rightarrow \mathbb{A}^1/\mathbb{F}_{p^e}$ whose Galois groups are linear groups over fields of characteristic p , and where U_i has genus 0 (see [1]). On the other hand, in the contexts considered here (covers coming from ℓ -torsion points of an abelian scheme \mathcal{A} over U , with ℓ large relative to the other data) these pathologies can perhaps be avoided; in our earlier paper [23] we show that for some families of covers of this kind one can indeed show that $g(U_i)$ is unbounded.

6.5. Issues of effectivity. Because of its dependency on Faltings’s theorem, there is currently no chance of being able to effectively compute sets like

$$\bigcup_{[k_1:k]=d} U_i(k_1),$$

with notation as in Theorem 3, even if we know that it is a finite set.

However, a more accessible kind of effectivity would be to ask for an effective determination, for a fixed $d \geq 1$, of a finite set $I_d \subset I$ of exceptional i such that the set above is finite

when $i \notin I_d$. In the context of Theorem 7, for instance, this would mean finding an effective $\ell_0 = \ell_0(d)$ such that

$$\bigcup_{[k_1:k]=d} \{t \in U(k_1) \mid \mathcal{A}_t[\ell](k_1) \text{ is non-zero}\}$$

is finite if $\ell \geq \ell_0$. Or one might ask for an effective growth result for gonality in the context of Theorem 8.

As our argument shows, this is directly related to the issue of finding effective expansion constants for the families of Cayley graphs that we use,⁵ which is a delicate question in general, even if the methods of [10] and [53] are effective in principle. Here using vertical towers can lead to drastic simplifications, as shown by the results of Dinai [21, 22], where simple explicit constants (c, A) are obtained. We hope to use these to make progress towards effectivity of some of our results.

APPENDIX A: THE BURGER METHOD

In this appendix, we sketch the extension of Burger's comparison principle to finite-area hyperbolic surfaces, as required in our arguments. The arguments follow Burger's method (most clearly explained in his thesis [15, Ch. 6], which is not readily available, and only briefly sketched in [13, 14]).

Theorem 20 (Burger). *Let $U' \rightarrow U$ be a finite covering of a connected hyperbolic Riemann surface with finite hyperbolic area. Fix a symmetric system of generators S of $\pi_1(U, x_0)$ and let*

$$\Gamma = C(\pi_1(U, x_0)/\pi_1(U', x'_0), S)$$

be the associated Cayley-Schreier graph, where $x'_0 \in U'$ is a point above x_0 . Then there exists a constant $c > 0$, depending only on U and S , such that

$$\lambda_1(U') \geq c\lambda_1(\Gamma).$$

Let P be the set of points in U' above x_0 , \tilde{P} the set of those in the universal cover $\tilde{U} = \mathbb{H}$ of U , so that $|P| = |\Gamma|$. For $x \in P$, $\tilde{x} \in \tilde{P}$, let

$$\begin{aligned} \mathcal{F}(x) &= \{u \in U' \mid d(u, x) < d(u, x') \text{ for all } x' \in P, x' \neq x\}, \\ \tilde{\mathcal{F}}(\tilde{x}) &= \{u \in \tilde{U} \mid d(u, \tilde{x}) < d(u, x') \text{ for all } x' \in \tilde{P}, x' \neq \tilde{x}\}. \end{aligned}$$

It is well-known that each $\tilde{\mathcal{F}}(\tilde{x}) \subset \tilde{U}$ is a fundamental domain for the action of $\pi_1(U, x_0)$ on \tilde{U} , and $\mathcal{F}(x) \subset U'$ is one for the covering $U' \rightarrow U$. When \tilde{x} (resp. x) varies, these are disjoint. The closures $\overline{\mathcal{F}(x)}$ cover U' , with boundaries having measure 0, and hence

$$\mu(\mathcal{F}(x)) = \mu(U) < +\infty$$

for all $x \in P$. Moreover, the set

$$T = \{g \in \pi_1(U, x_0) \mid g \neq 1, \overline{g\tilde{\mathcal{F}}(\tilde{x})} \cap \overline{\tilde{\mathcal{F}}(\tilde{x})} \neq \emptyset\}$$

is a finite symmetric generating set of $\pi_1(U, x_0)$. It is an elementary fact that we need only prove the result when the generating set S is replaced by T . We denote

$$r = |T| + 1.$$

⁵ The other ingredient which we can not obviously estimate is the first Neumann eigenvalue η that occurs in the proof of the comparison inequality (12), as described in Appendix A below (see 21).

Now consider the graph Γ' with vertex set P and edges joining x and x' in P , $x \neq x'$, if and only if

$$\overline{\mathcal{F}(x)} \cap \overline{\mathcal{F}(x')} \neq \emptyset.$$

This graph may be non-regular, but its valence function $v : P \rightarrow \mathbb{R}$ satisfies $1 \leq v(x) \leq |T|$ for all x . In fact, one checks that Γ' is obtained from the Cayley-Schreier graph

$$\Gamma_T = C(\pi_1(U, x_0)/\pi_1(U', x'_0), T)$$

by (i) replacing multiple edges by simple ones; (ii) removing loops. For simplicity, we will assume that $\Gamma' = \Gamma_T$, and in particular that $v(x) = |T|$ for all x . (See also [15, Ch.3, §4] for details about this construction.)

To prove the theorem, we use the variational characterization (or definition, see (9)) of $\lambda_1 = \lambda_1(U')$

$$\lambda_1 = \inf \left\{ \frac{\int_{U_i} \|\nabla \varphi\|^2 d\mu}{\|\varphi\|^2} \mid \varphi \text{ smooth and } \int_{U'} \varphi(x) d\mu(x) = 0 \right\},$$

where again $\nabla \varphi$ refers to the hyperbolic gradient of φ .

Precisely, we have already recalled that either this quantity is $= 1/4$ (in which case we are done) or else there exists a non-zero (eigenfunction) $\psi \in L^2(U', d\mu)$ with mean zero over U' and which attains the infimum. Of course, we now consider this case, and we may assume that ψ has L^2 -norm equal to 1.

Let $L^2(P)$ be the space of functions on P , with the inner product

$$\langle g_1, g_2 \rangle = \sum_{x \in P} g_1(x) \overline{g_2(x)}.$$

Now we must perform a transfer of some kind from smooth functions on U' to discrete functions on the vertex set P . The idea is quite simple: to a function f , we associate the function

$$\Phi(f) : x \mapsto \int_{\mathcal{F}(x)} f d\mu$$

on P . This linear map Φ is of course not an isometry from $L^2(U', d\mu)$ to $L^2(P)$, but it is at least continuous since

$$(20) \quad \|\Phi(f)\|^2 = \sum_{x \in P} \left| \int_{\mathcal{F}(x)} f d\mu \right|^2 \leq \mu(U) \|f\|^2$$

by the Cauchy-Schwarz inequality and the fact that the $\mathcal{F}(x)$ are disjoint and have measure $\mu(U)$.

Proof of Theorem 20. For $x \in P$, let $N(x) = \{x\} \cup \{x' \text{ adjacent to } x\}$, and define

$$\mathcal{G}(x) = \bigcup_{x' \in N(x)} \overline{\mathcal{F}(x')} \subset U',$$

so that (under our assumption $\Gamma_T = \Gamma'$, and recalling that $r = |T| + 1$) we have $|N(x)| = r$ and

$$\mu(\mathcal{G}(x)) = r\mu(U).$$

We start by stating the following fact, to be proved below (this is where the distinction between compact and finite-area surfaces will occur):

Fact 1. There exists a constant $\eta > 0$, depending only on U , such that, for all $x \in P$ and for $\mathcal{H} = \mathcal{F}(x)$ or $\mathcal{G}(x)$, we have

$$(21) \quad \inf \left\{ \frac{\int_{\mathcal{H}} \|\nabla \varphi\|^2 d\mu}{\int_{\mathcal{H}} |\varphi|^2 d\mu} \mid 0 \neq \varphi \text{ smooth and } \int_{\mathcal{H}} \varphi(x) d\mu(x) = 0 \right\} \geq \eta.$$

Assuming this, consider a non-zero function of the type

$$f = \alpha + \beta\psi$$

on U' with $\alpha, \beta \in \mathbb{R}$, and ψ the eigenfunction described above. We have an obvious inequality

$$(22) \quad \int_{U'} \|\nabla f\|^2 d\mu = \lambda_1 \beta^2 \leq \lambda_1 \|f\|^2.$$

Now we proceed to bound the left-hand side from below using the pieces $\mathcal{G}(x)$. For any $x \in P$, the function

$$\varphi = f - \frac{1}{\mu(\mathcal{G}(x))} \int_{\mathcal{G}(x)} f d\mu$$

(with $\nabla \varphi = \nabla f$) can be used to test (21), and therefore we have

$$\begin{aligned} \int_{\mathcal{G}(x)} \|\nabla f\|^2 &\geq \eta \int_{\mathcal{G}(x)} \left(f - \frac{1}{\mu(\mathcal{G}(x))} \int_{\mathcal{G}(x)} f d\mu \right)^2 d\mu \\ &= \eta \left\{ \int_{\mathcal{G}(x)} f^2 d\mu - \frac{1}{\mu(\mathcal{G}(x))} \left(\int_{\mathcal{G}(x)} f d\mu \right)^2 \right\}. \end{aligned}$$

Since we assumed that Γ' is regular, each $\mathcal{G}(x)$ is the union of r among the $\mathcal{F}(x')$. Therefore, if we sum over $x \in P$, divide by r and use the fact that $\mu(\mathcal{G}(x)) = r\mu(U)$, we obtain

$$\|\nabla f\|^2 \geq \eta \left\{ \|f\|^2 - \frac{1}{r^2 \mu(U)} \sum_{x \in P} \left(\sum_{x' \in N(x)} \Phi(f)(x') \right)^2 \right\}.$$

Comparing with (22) and dividing by $\|f\|^2$, we find using (20) that

$$\lambda_1 \geq \eta \frac{\langle B\Phi(f), \Phi(f) \rangle}{\|\Phi(f)\|^2}$$

where the linear operator B on $L^2(P)$ is defined by

$$B = 1 - \frac{1}{r^2} A^2,$$

with A being the self-adjoint linear map on $L^2(P)$ defined by

$$A(g)(x) = \sum_{x' \in N(x)} g(x').$$

The crucial point is that since the combinatorial Laplace operator Δ of Γ' is given by $\Delta = r\text{Id} - A$ (where the assumption $\Gamma' = \Gamma_T$ is used again), the operator B is itself closely related to Δ , namely

$$(23) \quad B = \frac{1}{r^2} (r^2 \text{Id} - A^2) = \frac{1}{r^2} \Delta (2r - \Delta).$$

It is clear that B is ≥ 0 and has eigenvalue 0 with multiplicity 1 for the constant eigenfunction. Let $\lambda'_1 > 0$ denote the smallest positive eigenvalue of B . We claim:

Fact 2. There exists $c > 0$, depending only on U , such that either $\lambda_1 \geq c$ or else there exists $\alpha, \beta \in \mathbb{R}$ not both zero for which $\Phi(f) = \Phi(\alpha + \beta\psi)$ is non-zero and has mean zero on P .

If this is the case, we construct the test function f using these α and β ; then, since

$$\langle \Phi(f), 1 \rangle = 0,$$

by the variational inequality for the spectrum of B , we have

$$\frac{\langle B\Phi(f), \Phi(f) \rangle}{\|\Phi(f)\|^2} \geq \lambda'_1.$$

However, using (23), we can compare λ'_1 and the first eigenvalue $\lambda_1(\Gamma')$: from $\|\Delta g\| \leq r\|g\|$ for all g , we get

$$\lambda'_1 \geq \frac{1}{r}\lambda_1(\Gamma') = \frac{1}{r}\lambda_1(\Gamma_T)$$

by looking on the subspace

$$L_0^2(P) = (\mathbb{C} \cdot 1)^\perp \subset L^2(P),$$

which is stable under B , Δ and $2r - \Delta$, and where each of these operators is invertible: indeed, we have

$$\frac{1}{\lambda'_1} = \|B^{-1}\| \leq r^2 \|\Delta^{-1}\| \|(2r - \Delta)^{-1}\| \leq r \|\Delta^{-1}\| = \frac{r}{\lambda_1(\Gamma')},$$

all operators and norms thereof being computed on $L_0^2(P)$ (see [15, p. 73, (d), (e)] or [14, §3, Cor. 1 (a)] for the general case where $\Gamma' \neq \Gamma_T$; Burger shows that $\lambda'_1 \geq \frac{2}{r^3}\lambda_1(\Gamma)$).

Combining these inequalities, we find that

$$\lambda_1 \geq \min\left(c, \frac{\eta}{r}\lambda_1(\Gamma_T)\right),$$

which concludes our proof.

We now justify the two claims above. For Fact 1, we note that the infimum considered, say $\eta(\mathcal{H})$, are nothing but the smallest positive eigenvalue for the Laplace operator with Neumann boundary condition on \mathcal{H} – or more precisely, because the area of \mathcal{H} is finite, the constant function 1 gives the base eigenvalue 0 as before, and $\eta(\mathcal{H})$ is either 1/4 or the first positive eigenvalue (by [51, Th. 2.4], which states in much greater generality that the spectrum is discrete in $[0, 1/4]$; if \mathcal{H} were compact, this becomes standard spectral geometry of compact Riemannian manifolds). So $\eta(\mathcal{H}) > 0$, but we must still show that there is a lower-bound depending only on U , not on U' .

For this, fix any $\tilde{x} \in \tilde{U}$ above x_0 . The reasoning in [15, p. 71] applies identically to show that $\mathcal{G}(x)$ is always isometric to a quotient of the domain

$$\mathcal{A} = \bigcup_{s \in T \cup \{1\}} s\tilde{\mathcal{F}}(\tilde{x}_1) \subset \tilde{U} = \mathbb{H},$$

(which depends only on U) under an equivalence relation of congruence modulo a subset of T^3 . Each such quotient is a finite-area domain in \mathbb{H} , hence also its first non-zero Neumann eigenvalue (defined variationally) is > 0 by [51, Th. 2.4]. Since T is finite, there are only

finitely many such quotients to consider, depending only on U , hence the smallest among these Neumann eigenvalues is still $\eta > 0$, and we have of course

$$\eta(\mathcal{H}) \geq \eta$$

for all \mathcal{H} , proving Fact 1.

For Fact 2, we note that to find the required test function f it is enough to know that the map Φ is injective on the \mathbb{R} -span of 1 and ψ . Indeed, we can then find a non-zero f in the kernel of the linear functional

$$f \mapsto \langle \Phi(f), 1 \rangle$$

(which is non-trivial since 1 maps to $|P|$), and this f will satisfy the required conditions.

Now we have two cases. If $\lambda_1 \geq \eta$, where η is given by Fact (1), we are done (and take $c = \eta$). Otherwise, we have

$$(24) \quad 0 < \lambda_1 < \eta,$$

and we now show that this implies that Φ is injective on the (real) span of 1 and ψ , which thus concludes the proof.

Thus, let $\alpha, \beta \in \mathbb{R}$ be such that $\Phi(f) = \Phi(\alpha + \beta\psi) = 0$. Then, for all $x \in P$, we have

$$\int_{\mathcal{F}(x)} \|\nabla f\|^2 d\mu \geq \eta \int_{\mathcal{F}(x)} f^2 d\mu,$$

since $\Phi(f) = 0$ means that f restricted to $\mathcal{F}(x)$ can be used to test (21). Summing over x , we get

$$\|\nabla f\|^2 \geq \eta \|f\|^2,$$

but $f = \alpha + \beta\psi$ implies then that

$$\eta \|f\|^2 \leq \|\nabla f\|^2 = \beta^2 \lambda_1 \leq \lambda_1 \|f\|^2,$$

and by comparing with (24), we see that $f = 0$. □

APPENDIX B: SEMISIMPLE APPROXIMATION À LA NORI AND SERRE

For m a positive integer and for ℓ varying over the primes, there are two kinds of groups that we focus on in this section. The first are the (finite) semisimple subgroups $G \leq \mathrm{GL}_m(\mathbb{F}_\ell)$, that is, subgroups which act semisimply in the natural representation of $\mathrm{GL}_m(\mathbb{F}_\ell)$ on $V = \mathbb{F}_\ell^m$, and the second are connected semisimple groups $\mathbf{G} \subseteq \mathbf{GL}_m/\mathbb{F}_\ell$. Nori showed that, outside of an explicit finite set of exceptional ℓ , there is a bijection between the finite semisimple G which are generated by their elements of order ℓ and “exponentially-generated” \mathbf{G} (see [50]). Serre showed that, up to excluding finitely many more ℓ , the semisimple groups \mathbf{G} which occur come from a finite collection of groups in characteristic zero (cf. [57]). We will give a brief review of these results following both [57] and a set of notes taken during the course mentioned in *op. cit.*.

Let ℓ be a prime and $G \leq \mathrm{GL}_m(\mathbb{F}_\ell)$ be a (finite) subgroup. We write $G_u \subseteq G$ for the subset of unipotent elements and $G^+ \leq G$ for the characteristic subgroup $G^+ = \langle G_u \rangle$.

Proposition 21. *If $\ell \geq m - 1$ and if $G \leq \mathrm{GL}_m(\mathbb{F}_\ell)$, then $g^\ell = 1$, for every $g \in G_u$, and G/G^+ has order prime to ℓ .*

Proof. Let $P \leq G$ be an ℓ -Sylow subgroup of G . Every element $g \in P$ lies in G_u , and thus $(g-1)^{m-1} = 0$. On the other hand, because $\ell \geq m-1$, $g^\ell - 1 = (g-1)^\ell = 0$, thus g is killed by ℓ . Therefore $P \leq G^+$ and G/G^+ has order prime to ℓ because G/P does. \square

If $\ell \geq m$, the exponential and logarithm maps give mutually-inverse bijections between the unipotent elements of $\mathrm{GL}_m(\mathbb{F}_\ell)$ and the nilpotent elements of $\mathrm{M}_m(\mathbb{F}_\ell)$, and we write $\mathfrak{g} \leq \mathrm{M}_m(\mathbb{F}_\ell)$ for the \mathbb{F}_ℓ -span of $\log(G_u)$.

Proposition 22. *If $\ell \geq 2m-1$, then \mathfrak{g} is an \mathbb{F}_ℓ -Lie subalgebra of $\mathrm{M}_m(\mathbb{F}_\ell)$ and every \mathfrak{g} -submodule of $\bar{V} = V \otimes \bar{\mathbb{F}}_\ell$ is a G^+ -submodule.*

Proof. This follows from Lemmas 1.4 (applied with $W_1 = W_2 = W$) and 1.6 of [50]. \square

For each $g \in G_u - \{1\}$, we can use the embedding $\langle \log(g) \rangle \rightarrow \mathrm{M}_m(\mathbb{F}_\ell)$ to extend the embedding $\langle g \rangle \rightarrow \mathrm{GL}_m(\mathbb{F}_\ell)$, to a one-parameter subgroup $\mathbb{G}_a \rightarrow \mathbf{GL}_m$ over \mathbb{F}_ℓ . We write $\mathbf{G}^+ \subset \mathbf{GL}_m$ for the algebraic subgroup generated by the images of all such one-parameter subgroups and $\mathrm{Lie}(\mathbf{G}^+) \subseteq \mathrm{M}_m(\mathbb{F}_\ell)$ for the \mathbb{F}_ℓ -Lie subalgebra of $\mathbf{G}^+ \subset \mathbf{GL}_m$.

Theorem 23. *There is a constant $\ell_1 = \ell_1(m) \geq 2m-1$ such that if $\ell \geq \ell_1$ and if $G \leq \mathrm{GL}_m(\mathbb{F}_\ell)$, then $G^+ = \mathbf{G}^+(\mathbb{F}_\ell)^+$ and $\mathfrak{g} = \mathrm{Lie}(\mathbf{G}^+)$.*

Proof. This is Theorem B of [50]. \square

We call the rational representation $\mathbf{G}^+ \rightarrow \mathbf{GL}_m$ the algebraic envelope of $G^+ \rightarrow \mathrm{GL}_m(\mathbb{F}_\ell)$. We are most interested in the case where G acts semisimply, and then the following corollary shows that, for almost all ℓ , the algebraic envelope $\mathbf{G}^+ \rightarrow \mathbf{GL}_m$ is a rational representation of a semisimple group. We will see that there are strong restrictions on the dominant weights occurring in this representation and that there are finitely many \mathbb{Z} -groups which give rise to them.

Corollary 24. *If $\ell \geq \ell_1$ and if $G \leq \mathrm{GL}_m(\mathbb{F}_\ell)$ is semisimple, then \mathbf{G}^+ is semisimple.*

Proof. By assumption, G acts semisimply on V , so Clifford's Theorem (see, e.g., [18, Theorem 49.2]) implies that $G^+ = \mathbf{G}^+(\mathbb{F}_\ell)^+$ acts semisimply on V . Because \mathbf{G}^+ is exponentially generated, the radical of \mathbf{G}^+ is unipotent, so we denote it \mathbf{U} . Another application of Clifford's Theorem implies that $\mathbf{U}(\mathbb{F}_\ell)$ also acts semisimply on V , and hence is trivial. But $\mathbf{U}(\mathbb{F}_\ell)$ has $\ell^{\dim(\mathbf{U})}$ elements, and so the triviality of the group $\bar{U}(\mathbb{F}_\ell)$ implies that \mathbf{U} itself is trivial as algebraic group. Thus \mathbf{G}^+ is semisimple. \square

For the remainder of this section we suppose $\ell \geq \ell_1$ and $G \leq \mathrm{GL}_m(\mathbb{F}_\ell)$ acts semisimply and satisfies $G = G^+$, i.e., it is generated by elements of order ℓ . We write $\mathbf{G} \rightarrow \mathbf{G}^+$ for the simply-connected cover of \mathbf{G} , and $\mathbf{G} \rightarrow \mathbf{GL}_m$ for the induced rational representation. The hypotheses on ℓ and G imply that $\mathbf{G}/\bar{\mathbb{F}}_\ell$ is a simply-connected semisimple group of rank at most $m-1$, the rank of \mathbf{SL}_m . Moreover, there is a finite collection $\{\mathbf{G}_i \rightarrow \mathrm{Spec}(\mathbb{Z})\}$ of split simply-connected semisimple groups (independent of ℓ and G) such that, for some i , the group $\mathbf{G}/\bar{\mathbb{F}}_\ell$ is isomorphic to $\mathbf{G}_i/\bar{\mathbb{F}}_\ell$.

For each i , the group $\mathbf{G}_i \rightarrow \mathrm{Spec}(\mathbb{Z})$ is a simply-connected Chevalley group. If we fix a maximal torus $\mathbf{T}_i \subset \mathbf{G}_i$ over \mathbb{Z} , then the irreducible representations of \mathbf{G}_i/\mathbb{C} are parametrized by their dominant weights $\lambda \in X(\mathbf{T}_i)_+$. Steinberg showed that there are \mathbb{Z} -forms $\rho_\lambda : \mathbf{G}_i \rightarrow \mathbf{GL}(V_\lambda)$ of these representations (see [58]), and one can show there is an explicit constant $\ell(\lambda)$ such that, for every $\ell \geq \ell(\lambda)$, the fiber $\rho_\lambda/\bar{\mathbb{F}}_\ell$ is also irreducible. If we fix a set $\{\mathfrak{w}_{ij}\}$

of fundamental weights of \mathbf{T}_i , then one can also show that the finite subset $\Lambda_i \subset X(\mathbf{T}_i)_+$ of dominant weights $\lambda = \sum_j c_j \mathbf{w}_{ij}$ satisfying $\max\{c_j\} \leq m - 1$ contains all λ satisfying $\dim(V_\lambda) \leq m$. We will see that, for almost all ℓ , each irreducible subrepresentation of $\mathbf{G} \rightarrow \mathbf{GL}_m$ over $\overline{\mathbb{F}}_\ell$ is isomorphic to $\rho_\lambda/\overline{\mathbb{F}}_\ell$ for some $\rho_\lambda : \mathbf{G}_i \rightarrow \mathbf{GL}(V_\lambda)$ with $\lambda \in \Lambda_i$.

We fix a maximal torus $\mathbf{T} \subset \mathbf{G}$ and a set $\{\mathbf{w}_i\}$ of fundamental weights of \mathbf{T} , and let $\Lambda_\ell \subset X(\mathbf{T})$ be the finite set of dominant weights $\lambda = \sum_i c_i \mathbf{w}_i$ which occur in $\mathbf{G} \rightarrow \mathbf{GL}_m$. The following proposition shows that the weights $\lambda \in \Lambda_\ell$ are ℓ -restricted, and thus the rational representation $\mathbf{G} \rightarrow \mathbf{GL}_m$ is restricted.

Proposition 25. *If $\lambda = \sum_i c_i \mathbf{w}_i \in \Lambda_\ell$, then $c_i \leq \ell - 1$.*

Proof. On the one hand, the irreducible submodules for G and \mathbf{G} of $\bar{V} = V \otimes \overline{\mathbb{F}}_\ell$ coincide, and Proposition 22 implies they are all \mathfrak{g} -irreducible. On the other hand, the only irreducible \mathbf{G} -modules over $\overline{\mathbb{F}}_\ell$ which are \mathfrak{g} -irreducible are those whose dominant weight $\lambda = \sum_i c_i \mathbf{w}_i$ satisfies $c_i \leq \ell - 1$ (cf. [37, Part II, Section 3.15]). \square

A priori the set Λ_ℓ could grow with ℓ , but the following proposition shows that it is bounded in a very strong sense.

Proposition 26. *If $\lambda = \sum_i c_i \mathbf{w}_i \in \Lambda_\ell$, then $c_i \leq m - 1$.*

Proof. By the previous proposition, λ is ℓ -restricted. On the one hand, for $n = c_i$, the rational representation $\mathbf{SL}_2 \rightarrow \mathbf{GL}_{n+1}$ corresponding to the ℓ -restricted weight $c_i \mathbf{w}_i$ is the n -th symmetric power of the standard representation $\mathbf{SL}_2 \rightarrow \mathbf{GL}_2$ and is irreducible (cf. [37, Part II, Section 3.0]). On the other hand, for each i , there is an embedding $\mathbf{SL}_2 \rightarrow \mathbf{G}$ such that $\lambda_i = c_i \mathbf{w}_i$ is one of the dominant weights of the induced representation $\mathbf{SL}_2 \rightarrow \mathbf{GL}_m$, thus $m \geq n + 1 = c_i + 1$. \square

We already saw that $\mathbf{G}/\overline{\mathbb{F}}_\ell$ is isomorphic to $\mathbf{G}_i/\overline{\mathbb{F}}_\ell$, for some i , and together with the last proposition we complete the proof of the claim that the dominant weights λ occurring in $\mathbf{G} \rightarrow \mathbf{GL}_m$ lie in Λ_i . The upshot is that we obtain the following theorem.

Theorem 27. *There exists a finite collection $\{\rho_{ij} : \mathbf{G}_i \rightarrow \mathbf{GL}_m\}$ of \mathbb{Z} -representations of simply-connected Chevalley groups and a constant $\ell_2 = \ell_2(m) \geq \ell_1$ such that if $\ell \geq \ell_2$ and if $G \leq \mathbf{GL}_m(\mathbb{F}_\ell)$ is semisimple and satisfies $G = G^+$, then for some i, j , the fiber $\rho_{ij}/\overline{\mathbb{F}}_\ell$ is isomorphic to $\mathbf{G} \rightarrow \mathbf{GL}_m$.*

For each pair of integers $r, s \geq 1$, we write $T_{rs}V$ for the vector space $T_{rs}V = (\bigoplus_{i=1}^r V^{\otimes i})^{\oplus s}$ and $\mathbf{GL}(V) \rightarrow \mathbf{GL}(T_{rs}V)$ for the corresponding tensor representation.

Corollary 28. *There are constants $\ell_3 = \ell_3(m) \geq \ell_2$, $r = r_1(m)$, and $s = s_1(m)$ such that if $\ell \geq \ell_3$ and if $G \leq \mathbf{GL}_m(\mathbb{F}_\ell)$ is semisimple and satisfies $G = G^+$, then the composite representation $\mathbf{G} \rightarrow \mathbf{GL}(V) \rightarrow \mathbf{GL}(T_{rs}V)$ identifies \mathbf{G} with the algebraic subgroup of elements in $\mathbf{GL}(V)$ acting trivially on the subspace of \mathbf{G} -invariants in $T_{rs}V$.*

Proof. The main idea is to show that, for each i, j , an analogous statement holds for the \mathbb{Q} -fiber of $\rho_{ij} : \mathbf{G}_i \rightarrow \mathbf{GL}_m$. More precisely, if we write $V_{\mathbb{Q}} = \mathbb{Q}^m$, then for some $r = r(i, j, m)$ and $s = s(i, j, m)$ depending on i and j , the tensor representation $\mathbf{G}_i(\mathbb{Q}) \rightarrow \mathbf{GL}(T_{rs}V_{\mathbb{Q}})$ identifies \mathbf{G}_i/\mathbb{Q} with the algebraic subgroup of \mathbf{GL}_m acting trivially on the subspace of \mathbf{G}_i -invariants.⁶ Moreover, there is a \mathbb{Z} -form of this tensor representation, and for almost all ℓ , the

⁶ Every irreducible finite-dimensional rational representation of $\mathbf{GL}(V_{\mathbb{Q}})$ is a subquotient of $\mathbf{GL}(V_{\mathbb{Q}}) \rightarrow \mathbf{GL}(V_{\mathbb{Q}}^{\otimes r})$ for some r , so every finite-dimensional rational representation is a subquotient of $\mathbf{GL}(V_{\mathbb{Q}}) \rightarrow$

corresponding tensor representation $\mathbf{G}_i(\mathbb{F}_\ell) \rightarrow \mathrm{GL}(T_{rs}V)$ identifies $\mathbf{G}_i/\mathbb{F}_\ell$ with the algebraic subgroup of $\mathbf{GL}(T_{rs}V)$ acting trivially on the subspace of \mathbf{G}_i -invariants. In particular, in light of the theorem it suffices to take $r_1(m) \geq \max\{r(i, j, m)\}$ and $s_1(m) \geq \max\{s(i, j, m)\}$. \square

REFERENCES

- [1] Abhyankar, S. Nice equations for nice groups. *Israel J. of Math.* 88 (1994), 1–23.
- [2] Abramovich, D. A linear lower bound on the gonality of modular curves. *International Math. Res. Notices* 20 (1996), 1005–1011.
- [3] Abramovich, D. and Harris, J. Abelian varieties and curves in $W_d(C)$. *Compositio Math.* 78 (1991), 227–238.
- [4] Abramovich, D. and Voloch, F. Lang’s conjectures, fibered powers, and uniformity. *New York J. of Math.* 2 (1996), 20–34, also nyjm.albany.edu:8000/j/v2/Abramovich-Voloch.html
- [5] Bekka, B., de la Harpe, P. and Valette, A. Kazhdan’s Property (T). *New Math. Monographs* 11, Cambridge Univ. Press (2008).
- [6] Bourgain, J. and Gamburd, A. Uniform expansion bounds for Cayley graphs of $\mathrm{SL}_2(\mathbb{F}_p)$. *Ann. of Math.* 167 (2008), 625–642.
- [7] Bourgain, J. and Gamburd, A. Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$, I. *Journal of the Europ. Math. Soc.* 10 (2008), 987–1011.
- [8] Bourgain, J. and Gamburd, A. Expansion and random walks in $\mathrm{SL}_d(\mathbb{Z}/p^n\mathbb{Z})$, II. *Journal of the Europ. Math. Soc.* 11 (2009), 1057–1103.
- [9] Bourgain, J., Gamburd, A. and Sarnak, P. Generalization of Selberg’s 3/16 Theorem and affine sieve. preprint (2010), [arXiv:0912.5021](https://arxiv.org/abs/0912.5021)
- [10] Breuillard, E., Green, B. and Tao, T. Approximate subgroups of linear groups. *GAF*, to appear, [arXiv:1005.1881](https://arxiv.org/abs/1005.1881).
- [11] Brooks, R. On the angles between certain arithmetically defined subspaces of \mathbb{C}^n . *Annales Inst. Fourier* 37 (1987), 175–185.
- [12] Brooks, R. The spectral geometry of a tower of coverings. *J. Diff. Geometry* 23 (1986), 97–107.
- [13] Burger, M. Estimations de petites valeurs propres du laplacien d’un revêtement de variétés riemanniennes compactes. *C.R. Acad. Sc. Paris*, 302 (1986), 191–194.
- [14] Burger, M. Spectre du laplacien, graphes et topologie de Fell. *Comment. Math. Helvetici*, 63 (1988), 226–252.
- [15] Burger, M. Petites valeurs propres du Laplacien et topologie de Fell. Thèse de doctorat (1986), Econom Druck AG (Basel).
- [16] Cadoret, A. and Tamagawa, A. A uniform open image theorem for ℓ -adic representations, I. to appear in *Duke Math. Journal*.
- [17] Cadoret, A. and Tamagawa, A. A uniform open image theorem for ℓ -adic representations, II. preprint (2009), http://www.math.u-bordeaux1.fr/~cadoret/uo12_4.pdf
- [18] Curtis, C.W. and Reiner, I. Representation theory of finite groups and associative algebras. Reprint of the 1962 original; AMS Chelsea Publishing, Providence, RI, 2006.
- [19] Demazure, M. and Gabriel, P. Introduction to algebraic geometry and algebraic groups. North-Holland Mathematics Studies, 39.
- [20] Diaconis, P. and Saloff-Coste, L. Comparison techniques for random walk on finite groups. *Annals of Prob.* 21 (1993), 2131–2156.
- [21] Dinai, I. Poly-log diameter bounds for some families of finite groups. *Proc. Amer. Math. Soc.* 134 (2006), 3137–3142.
- [22] Dinai, I. Diameters of Chevalley groups over local rings. preprint (2011).
- [23] Ellenberg, J., Elsholtz, C., Hall, C. and Kowalski, E. Non-simple abelian varieties in a family: geometric and analytic approaches. *J. London Math. Soc.* 80 (2009), 135–154; [doi:10.1112/jlms/jdp021](https://doi.org/10.1112/jlms/jdp021)

$\mathbf{GL}(T_{rs}V_{\mathbb{Q}})$ for some r, s . In particular, there is a finite-dimensional rational representation $\rho : \mathbf{GL}(V_{\mathbb{Q}}) \rightarrow \mathbf{GL}(W_{\mathbb{Q}})$ which identifies \mathbf{G}_i with the stabilizer in $\mathbf{GL}(V_{\mathbb{Q}})$ of a line in $W_{\mathbb{Q}}$ (see, e.g., Corollary 3.5 of [19, II.2]), and because \mathbf{G}_i is semisimple, it acts trivially on the line.

- [24] Faltings, G. Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. *Invent. math.* 73 (1983), 349–366.
- [25] Faltings, G. Diophantine approximation on abelian varieties. *Annals of Math.* 133 (1991), 549–576.
- [26] Faltings, G., Wüstholz, G., Grunewald, F., Schappacher, N., and Stuhler, U. *Rational points*. Third edition. Papers from the seminar held at the Max-Planck-Institut für Mathematik, Bonn/Wuppertal, 1983/1984.
- [27] Frey, G. Curves with infinitely many points of fixed degree. *Israel J. Math.* 85 (1994), 79–83.
- [28] Frohardt, D. and Magaard, K. Composition factors of monodromy groups. *Ann. of Math.* 154, no.2 (2001), 327–345.
- [29] Gill, N. and Helfgott, H. Growth of small generating sets in $SL_n(\mathbb{Z}/p\mathbb{Z})$. *International Math. Res. Notices*, to appear; [arXiv:1002.1605](https://arxiv.org/abs/1002.1605)
- [30] Gromov, M. and Guth, L. Generalizations of the Kolmogorov-Barzdin embedding estimates. preprint (2011), [arXiv:1103.3423](https://arxiv.org/abs/1103.3423)
- [31] Guralnick, R. Monodromy groups of coverings of curves. In *Galois Groups and Fundamental Groups*, Cambridge U. Press, 2003.
- [32] Hall, C.J. An open-image theorem for a general class of abelian varieties. *Bulletin of the L.M.S.*, to appear; [arXiv:0803.1682](https://arxiv.org/abs/0803.1682)
- [33] Harada, S. and Hiranouchi, T. Smallness of fundamental groups for arithmetic schemes. *Journal of Number Theory* 129 (2009) 2702–2712.
- [34] Helfgott, H. Growth and generation in $SL_2(\mathbb{Z}/p\mathbb{Z})$. *Ann. of Math.* 167 (2008), 601–623.
- [35] Hoory, S., Linial, N. and Wigderson, A. Expander graphs and their applications. *Bull. Amer. Math. Soc.* 43 (2006), 439–561.
- [36] Hrushovski, E. Stable group theory and approximate subgroups. *Journal of the AMS* 25 (2012), 189–243, [arXiv:0909.2190](https://arxiv.org/abs/0909.2190).
- [37] Jantzen, J.C. Representations of algebraic groups. Math. Surveys and Monographs 107, A.M.S., 2003.
- [38] Katz, N. and Lang, S. Finiteness theorems in geometric classfield theory. *Enseign. Math.* 27 (1981), 285–314.
- [39] Kelner, J. Spectral partitioning, eigenvalue bounds, and circle packings for graphs of bounded genus. *Siam J. Comput.* 35 (2006), 882–902.
- [40] Kassabov, M. and Riley, T.R. Diameters of Cayley graphs of Chevalley Groups *Eur. J. Comb.* 28 (2007), 791–800.
- [41] Kowalski, E. Sieve in expansion. *Bourbaki Seminar*, exposé 1028 (2010), <http://www.math.ethz.ch/~kowalski/sieve-expansion-bourbaki.pdf>
- [42] Landazuri, V. and Seitz, M. On the minimal degrees of projective representations of the finite Chevalley groups. *Journal of algebra* 32 (1974), 418–443.
- [43] Li, P. and Yau, S.T. A new conformal invariant and its applications to the Willmore conjecture and the first eigenvalue of compact surfaces. *Invent. math.* 69 (1982), 269–291.
- [44] Lubotzky, A. Discrete groups, expanding graphs and invariant measures. Progress in Math. 125, Birkhäuser 1994.
- [45] Masser, D. Specializations of endomorphism rings of abelian varieties. *Bull. S.M.F.* 124 (1996), 457–476.
- [46] Matthews, C.R., Vaserstein, L.N., Weisfeiler, B. Congruence properties of Zariski-dense subgroups. *I. Proc. London Math. Soc.* (3) 48 (1984), no. 3, 514–532.
- [47] Merel, L. Bornes pour la torsion des courbes elliptiques sur les corps de nombres. *Inventiones math.* 124 (1996), 437–449.
- [48] Neuhauser, M Kazhdan’s Property T for the symplectic group over a ring. *Bull. Belg. Math. Soc. Simon Stevin* 10, no. 4 (2003), 537–550.
- [49] Nori, M. A nonarithmetic monodromy group. *C. R. Acad. Sci. Paris Sér. I Math.* 302 (1986), 71–72.
- [50] Nori, M. On subgroups of $GL_n(\mathbb{F}_p)$. *Invent. math.* 88 (1987), 257–275.
- [51] Phillips, R. and Sarnak, P. The Laplacian for domains in hyperbolic space and limit sets of Kleinian groups. *Acta Math.* 155 (1985), 173–241.
- [52] Poonen, B. Gonality of modular curves in characteristic p . *Math. Res. Lett.* 14, no. 4 (2007), 691–701
- [53] Pyber, L. and Szabó, E. Growth in finite simple groups of Lie type of bounded rank. preprint (2010), [arXiv:1005.1858v1](https://arxiv.org/abs/1005.1858v1)

- [54] Rosenberg, S. Gauss-Bonnet theorems for noncompact surfaces. *Proceedings A.M.S* 86 (1982), 184-185
- [55] Salehi Golsefidy, A. and Varjú, P. *Expansion in perfect groups* Preprint (2010).
- [56] Serre, J-P. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. math.* 15 (1972), 259–331.
- [57] Serre, J-P. Lettre à Marie-France Vignéras du 10/02/1987. Œuvres, vol. IV, pp. 38–55; Springer (2000).
- [58] Steinberg, R. Lectures on Chevalley groups. Yale University Press (1968).
- [59] Varjú, P. Expansion in $SL_d(O_K/I)$, I square-free. preprint (2010), [arXiv:1001.3664](https://arxiv.org/abs/1001.3664).
- [60] Yang, P. and Yau, S.T. Eigenvalues of the laplacian of compact Riemann surfaces and minimal submanifolds. *Ann. Scuola Norm. Sup. Pisa* 7 (1980), 55–63.
- [61] Yu, J-K. Toward a proof of the Cohen-Lenstra conjecture in the function field case. preprint (1995).
- [62] Zograf, P. Small eigenvalues of automorphic Laplacians in spaces of cusp forms. *Zap. Nauchn. Sem. Leningrad. Otdel. Mat. Inst. Steklov (LOMI)* 134 (1984), 157-168 translation in *Journal of Math. Sciences* 36, Number 1, 106-114, DOI:10.1007/BF01104976.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF WISCONSIN, 480 LINCOLN DRIVE, MADISON, WI 53705 USA

E-mail address: ellenber@math.wisc.edu

DEPARTMENT OF MATHEMATICS UNIVERSITY OF WYOMING, ROSS HALL, LARAMIE, WY 82071, USA

E-mail address: chall114@uwyo.edu

ETH ZÜRICH – D-MATH, RÄMISTRASSE 101, 8092 ZÜRICH, SWITZERLAND

E-mail address: kowalski@math.ethz.ch