J. London Math. Soc. (2) 80 (2009) 135–154 © 2009 London Mathematical Society
doi:10.1112/jlms/jdp021

Non-simple abelian varieties in a family: geometric and analytic approaches

Jordan S. Ellenberg, Christian Elsholtz, Chris Hall and Emmanuel Kowalski

Abstract

We consider, in the special case of certain one-parameter families of Jacobians of curves defined over a number field, the problem of how the property that the generic fiber of such a family is absolutely simple 'spreads' to other fibers. We show that this question can be approached using arithmetic geometry or with more analytic methods based on sieve theory. In the first setting, non-trivial group-theoretic information is needed, while the version of the sieve we use is also of independent interest.

Introduction

Given a family $X \to S$ of algebraic varieties (over a field k, say, with S connected), a natural question of algebraic geometry is to know what type of properties of the generic fiber X_η extend to other fibers and, indeed, in which way they extend. As examples, one can think of Grothendieck's semicontinuity theorem, which is a general purely algebraic result of this type. As a second example, a family of curves with smooth generic fiber will be smooth over an open subset of the base and, after an appropriate base change, all the fibers will be stable. In an arithmetic setting, a celebrated example of great importance is the Hilbert irreducibility theorem, where it is shown that, for a Galois covering $X \to \mathbf{P}^n$ defined over a number field k, the fiber over 'most' rational points $t \in \mathbf{P}^n(k)$ is a finite set of Galois-conjugate points, where G acts freely transitively (in other words, the coordinates of any point $x \in X$ mapping to t generate a Galois extension with Galois group G). Indeed, quantitative estimates are known for the size of the complement; see, for example [**37**, Chapter 9], and arise from very diverse methods, among which we highlight the large sieve arguments of S.D. Cohen (see, for example, [**6**] or [**37**, Chapter 13]).

There are arithmetic properties for which the classical methods known in the context of the Hilbert irreducibility theorem do not seem to be directly applicable. One example is the following question: let $\mathcal{A} \to S$ be a family of abelian varieties defined over a global field k, and assume that the generic fiber is simple, or geometrically simple. What can be said about the set of rational points $s \in S(k)$ for which A_s remains (geometrically) simple over k? (Note here the similarity with the case of Hilbert's irreducibility theorem, when interpreted in terms of irreducibility of specializations of an irreducible polynomial $F(X, Y)$ in two variables.) Note that, for each prime number ℓ, one can pose in this setting the Galois-theoretic question of understanding how the Galois groups of the ℓ-torsion fields of the fibers vary, which are instances of Hilbert's irreducibility-type problems. In fact, it turns out that understanding this, as ℓ varies, plays an important role in the work that follows.

We will develop a variety of techniques to approach this particular problem, especially when $S = \mathbf{P}^1_k$, and we expect that they would be suitable for many others with a similar flavor.

Received 18 September 2008; revised 28 January 2009; published online 22 May 2009.

2000 *Mathematics Subject Classification* 11G10 (primary); 11N35, 14K15, 14D05 (secondary).

The first author was partially supported by NSF-Career grant DMS-0448750 and a Sloan Research Fellowship.

In fact, the parallel with the known approaches to Hilbert's theorem will be obvious: one set of techniques will be built on arithmetic geometry, while the other will involve sieve methods, although both will require some group-theoretic information. This familiar appearance should not be taken too far, however, as the tools involved are quite subtle. In particular, we appeal to difficult results of group theory, which had not yet, to our knowledge, been applied to arithmetic problems (for some, the only published proof depends on the classification of finite simple groups). On the sieve side, the method will also be quite original, and will involve proving a new generalization of Gallagher's larger sieve inequality over number fields, which is likely to be of independent interest. (Because of the interest of this sieve statement for analytic number theorists, independently of the problem in arithmetic geometry which is involved, we have summarized in an Appendix enough information to understand the latter; hence, readers who are not familiar with abelian varieties may want to read this Appendix now, and then continue with the introduction and then with Section 3.)

Since the goal of this paper is partly to emphasize the general methods, rather than to solve a specific particular case, and since the tools borrow quite freely from arithmetic algebraic geometry, group theory, and analytic number theory, which may not be equally familiar to the interested readers, we have chosen a fairly expository style of writing. For instance, we discuss informally the characteristic strengths and weaknesses of the two basic approaches, and, for the sake of clarity, we do not always pursue the strongest possible conclusions.

To give a concrete form to our results, here are prototypical consequences of the more general theorems proved in the main body of the paper. They concern a particular type of family of abelian varieties, namely the family

$$A_f \longrightarrow \mathbf{A}^1$$

of Jacobians of the hyperelliptic curves defined by affine equations

$$y^2 = f(x)(x-t), \quad t \in \mathbf{A}^1,$$

for some fixed square-free polynomial $f \in \mathbb{Z}[X]$ of degree $2g$ for $g \geqslant 1$. It is true (though not obvious) that the generic fiber of this family is geometrically simple, and hence we can ask the question discussed above. We phrase it in a quantitative manner. First, for $t \in \mathbb{Q}$ where $t = a/b$ with coprime integers a and $b \neq 0$, let $H(t) = \max(|a|, |b|)$ be the height of t. Let then $S(B)$ denote the set

$$S(B) = \{t \in \mathbb{Q} \mid H(t) \leqslant B, \text{and the fiber } A_{f,t} \text{ is not geometrically simple}\}.$$

We will show that $S(B)$ is 'small' in some sense.

THEOREM A (Arithmetic geometry method). *There exists a constant $C(f)$, depending on f, such that we have*

$$|S(B)| \leqslant C(f) \tag{1}$$

for all $B \geqslant 1$. In other words, there are only finitely many $t \in \mathbb{Q}$ for which $A_{f,t}$ is not geometrically simple.

This is a special case of Theorem 8 in Section 1 and is elaborated on in Example 14 in Section 2.

THEOREM B (Analytic number theory method). *There exist absolute constants $C \geqslant 0$ and $D \geqslant 1$, independent of f, such that we have*

$$|S(B)| \leqslant C(g^2 D(\log 2B))^{11g^2} \tag{2}$$

for all $B \geqslant 1$.

This is a special case of Theorem 24 in Section 3, where we have simplified the bound by worsening it somewhat.

These results show that the 'geometric simplicity' property does extend to most fibers in these families. Here is one reason why this is not at all obvious (which also, hopefully, suggests what other type of properties might be considered similar). Suppose we first ask the question for all complex fibers (where it remains meaningful): how large is the set of $t \in \mathbb{C}$ for which $A_{f,t}$ is not geometrically simple? Geometrically, this set is the intersection between the rational curve in the moduli space $\mathcal{M}_g$ of curves of genus g, which 'is' the family A_f, and the sublocus NS_g of $\mathcal{M}_g$ parametrizing curves whose Jacobians are non-simple. Difficulty arises from the fact that NS_g is a *countable* union of proper subvarieties, and hence it would suffice for each of those to intersect the family A_f in a single rational point (each distinct from the others) for Theorem A to fail.

In fact, when $g = 2$, the non-simple locus NS_2 is a countable union of divisors, and so a typical curve intersects this locus infinitely many times; however, our result shows that most of the intersection points are not rational.

This discussion suggests the following question (which we do not claim to know the answer to).

QUESTION 1. Is there an absolute constant C such that, for any square-free polynomial $f \in \mathbb{C}[x]$ of degree at least 6, there are at most C complex numbers t such that the Jacobian of $y^2 = f(x)(x - t)$ is not simple? (The condition on the degree ensures that the genus is not $\leqslant 2$.)

One can also restrict to integral polynomials and rational values of t, and there one may observe that our proof of Theorem A shows that if we further allow C to depend on the degree of f (that is, on the genus of the hyperelliptic curves under consideration), then a conjecture of Lang [**28**] implies a positive answer (by the work of Caporaso, Harris, and Mazur [**4**] who have deduced from it a bound *depending only on* g for the number of rational points on a curve of genus g over $\mathbb{Q}$).

Here are now some general comments to compare Theorems A and B, which also apply more generally to the two underlying methods. Theorem A may initially appear to be much stronger. However, note that in (1), we have no idea about the actual value of $C(f)$, in particular about how it may vary with f, whereas in Theorem B, the bound (2) is *effective* in terms of f. In particular this means we can prove bounds for similar problems involving families with more than one parameter (that is, over a more complicated base than the affine or projective line; for instance, we could look at the two-parameter family of Jacobians of

$$y^2 = f(x)(x - t)(x - v),$$

for fixed square-free f of degree $2g - 1$), and this also means that we can deduce an upper bound from (2) for the *smallest height* of a point $t \in \mathbb{Q}$ such that the variety $A_{f,t}$ is geometrically simple (indeed, a simple computation shows that there exists some t of height at most B for which A_t is geometrically simple, where

$$B = C'(D'g^4)^{11g^2}$$

for some constants $C' > 0$ and $D' \geqslant 1$, which are computable in terms of C and D).

This situation may be compared with the problem of counting rational points on a plane curve X of genus at least 2: the theorem of Faltings shows that this set of points is finite, but it gives no effective bound for the heights of the solutions, and only estimates (depending badly on X) the number of points, while on the other hand the method of Heath-Brown [**22**] yields

a completely explicit bound, depending only on the degree of X, for the number of points on X of height at most B.

Another remark of interest in the comparison with the Hilbert irreducibility theorem is that the results are stronger: the bounds for the size of $S(B)$ are much better than those known for a general 'thin' set (see [**37**, § 13.1]). This is particularly transparent with the sieve argument, since our application of the larger sieve is much stronger than the large sieve.

NOTATION. As usual, $|X|$ denotes the cardinality of a set, and $\mathbb{F}_q$ is a field with q elements. For a number field k, $\mathbb{Z}_k$ denotes its ring of integers, and for a prime ideal $\mathfrak{p} \subset \mathbb{Z}_k$, $\mathbb{F}_\mathfrak{p}$ is the residue field $\mathbb{Z}_k/\mathfrak{p}$.

By $f \ll g$ for $x \in X$, or $f = \mathrm{O}(g)$ for $x \in X$, where X is an arbitrary set on which f is defined, we mean synonymously that there exists a constant $C \geqslant 0$ such that $|f(x)| \leqslant Cg(x)$ 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.

1. *Methods from arithmetic geometry, I*

In this section and the next we consider a field k that is finitely generated over the prime field; for example, k could be a number field or a function field over a finite field. (These will be the only fields arising in the analytic section, and the reader can think of these as the most important.) We also assume that the characteristic of k, if positive, is not equal to 2.

The first conditions arise because we need to know that the following mild weakening of Mordell's conjecture holds for k.

THEOREM 2. *With k as above, there is a constant $g_1(k)$ such that, for any smooth projective curve C/k of genus $g > g_1(k)$, the set $C(k)$ of k-rational points on C is finite.*

Proof. At a minimum we must have $g \geqslant 2$, and if $\mathrm{char}(k) = 0$, then we may take $g_1(k) = 2$. If C is not defined over an algebraic closure of the prime field of k, then this is a combination of results of Grauert [**16**] and Manin [**31**] (for $\mathrm{char}(k) = 0$) and Samuel [**34**] (for $\mathrm{char}(k) > 0$). If $\mathrm{char}(k) = 0$ and C is defined over the algebraic closure of $\mathbb{Q}$, then the argument in the corollary of [**32**, Theorem 1] reduces this to the celebrated theorem of Faltings [**11**]. The case which can force us to take $g_1(k) > 2$ is when $k = \mathbb{F}_q(X)$ for a smooth projective variety $X/\mathbb{F}_q$ and C is defined over $\mathbb{F}_q$. If $\mathbb{F}_q$ is algebraically closed in k, then elements of the complement $C(k) - C(\mathbb{F}_q)$ correspond to dominant maps $X \to C$ and repeated composition with the Frobenius $C \to C$ gives rise to an infinite subset of $C(k)$. However, the following proposition shows that, if we take $g_1(k) = \dim H^0(X \times_{\mathbb{F}_q} \overline{\mathbb{F}}_q, \Omega^1)$, there are no such elements, and hence $C(k) = C(\mathbb{F}_q)$ is finite. □

PROPOSITION 3. *Let $Y/\overline{\mathbb{F}}_q$ be a smooth projective curve of genus g. For any dominant map $f : X \to Y$, where $X/\overline{\mathbb{F}}_q$ is a smooth projective variety, we have $g \leqslant \dim H^0(X, \Omega^1)$.*

The following proof was suggested by J. F. Voloch.

Proof of Proposition 3. If $f : X \to Y$ is inseparable, then there is a purely inseparable map of curves $Z \to Y$ through which f factors and such that $X \to Z$ is separable. Moreover, the genus of Y is at most the genus of Z, and so up to replacing Y with Z we may assume f is

separable. Then the pullback map of differentials

$$f^* : H^0(Y, \Omega^1) \longrightarrow H^0(X, \Omega^1)$$

is an embedding (cf. [38, III.6.2, Theorem 1]), and since $\dim(H^0(Y, \Omega^1)) = g$, the conclusion follows. □

Let now C/k be a smooth curve, and let $A/k(C)$ be a principally polarized abelian variety of dimension g over the function field of C. Let ℓ be a prime which is invertible in k and let $A[\ell]$ be the ℓ-torsion of A.

There is an embedding of the group $G = \mathrm{Gal}(k(C)(A[\ell])/k(C))$ into $\Gamma = \mathrm{Aut}(A[\ell])$, where Aut is understood to refer to the group of linear automorphisms preserving the symplectic Weil pairing, up to a scalar. The subgroup of symplectic automorphisms of $A[\ell]$ is denoted Γ_0. We therefore have the isomorphisms as follows:

$$\Gamma \simeq G\mathrm{Sp}(2g, \mathbb{F}_\ell), \quad \Gamma_0 \simeq \mathrm{Sp}(2g, \mathbb{F}_\ell)$$

(where $G\mathrm{Sp}(2g)$ is the group of symplectic similitudes, also sometimes written $C\mathrm{Sp}(2g)$ or even $S\mathrm{Sp}(2g)$).

By the *geometric monodromy* of A *modulo* ℓ, we mean the image of the absolute Galois group of $k^s(C)$ in Γ_0. We say A has *big monodromy mod* ℓ if the geometric monodromy of A is the whole symplectic group Γ_0, so that $\Gamma_0 \leqslant G$. If v is a place of $k(C)$, then we write A_v for the fiber over v of the Neron model of A over C and $G_v \leqslant G$ for the decomposition group. We say A_v has *big monodromy modulo* ℓ if A_v is an abelian g-fold and if $\Gamma_0 \leqslant G_v \leqslant G$. In all this, if ℓ is clear from the context, then we may simply speak of *geometric monodromy*, or say that A or A_v *has big monodromy*, without specifying ℓ.

These notions are relevant to our basic problem because of the following sufficient criterion for geometric simplicity, which will be our main tool in this and the next section. This makes precise the fairly intuitive fact that a factorization of an abelian variety forces the monodromy group to preserve the factors, and hence is incompatible with having big monodromy; but because the factorization may exist only over an extension of k, and is valid only up to isogeny, this requires some care.

PROPOSITION 4. *For any $g \geqslant 1$, there is a constant $\ell_1(g) \geqslant 1$ satisfying the following: if $\ell > \ell_1(g)$ and A/k is an abelian variety of dimension g over a field k such that A has big monodromy modulo ℓ, then A satisfies $\mathrm{End}_{\bar{k}}(A) = \mathbb{Z}$ and in particular is geometrically simple.*

Proof. By a theorem of Chow, we have $\mathrm{End}_{\bar{k}}(A) = \mathrm{End}_{k^s}(A)$ for any abelian variety A/k (see [8, Theorem 3.19]), and hence it suffices to prove the corresponding statement with the endomorphism ring over k^s instead of over $\bar{k}$.

Next, for any A/k, note that the rank of the endomorphism ring $\mathrm{End}_{k^s}(A')$, as a $\mathbb{Z}$-module, is constant as A' runs over the isogeny class of A. If A is not geometrically simple, then there is an abelian variety A' in this isogeny class, which splits over $\bar{k}$ as $A_1 \times A_2$, with A_1, A_2 of dimension at least 1. By the previous paragraph, this means in particular that $\mathrm{End}_{k^s}(A')$ contains a non-trivial endomorphism π satisfying $\pi^2 = \pi$ (for example, the projection onto the non-trivial factor A_1), and then $\mathbb{Z}[\pi]$ is a rank-2 $\mathbb{Z}$-submodule of $\mathrm{End}_{k^s}(A')$ and thus $\mathrm{End}_{k^s}(A) \neq \mathbb{Z}$ (since it has rank at least 2). In particular, by contraposition, A is geometrically simple if $\mathrm{End}_{k^s}(A) = \mathbb{Z}$.

Now, let ℓ be a prime number such that some abelian variety A/k has big monodromy modulo ℓ and satisfies $\mathrm{End}_{k^s}(A) \neq \mathbb{Z}$. Then, by the theory of abelian groups, there is an endomorphism ψ in $\mathrm{End}_{k^s}(A)$ such that $\mathbb{Z}[\psi]$ is a rank-2 $\mathbb{Z}$-submodule of $\mathrm{End}_{k^s}(A)$ and, moreover, $\mathrm{End}_{k^s}(A)/\mathbb{Z}[\psi]$ has no ℓ-torsion. The latter assumption implies that the image of

$\mathbb{Z}[\psi]$ in $\mathrm{End}(A[\ell]) \simeq M_{2g}(\mathbb{F}_\ell)$ is a rank-2 $\mathbb{F}_\ell$-submodule, because otherwise $\psi - m$ would be divisible by ℓ for some $m \in \mathbb{Z}$. More precisely, we may find ψ such that the image of ψ in $\mathrm{End}(A[\ell])$ does not lie in the scalar subgroup $\mathbb{F}_\ell^\times$.

Let K be the Galois closure of the splitting field of ψ (that is, K is the fixed field of the subgroup of $\mathrm{Gal}(\bar{k}/k)$ fixing ψ) and let H be its Galois group of $K(A[\ell])/K$. There is a natural inclusion $H \to G$, where G is the monodromy group of A modulo ℓ.

Since the action of ψ on $A[\ell]$ commutes with H and ψ does not lie in the scalar subgroup $\mathbb{F}_\ell^\times \leqslant \mathrm{End}(A[\ell])$, Schur's lemma implies that the subgroup $H \leqslant M_{2g}(\mathbb{F}_\ell)$ does not act absolutely irreducibly on $A[\ell]$. Since $G \cap \Gamma_0 = \Gamma_0$ does have this property (because of the big monodromy assumption), $H \cap \Gamma_0$ is a proper subgroup of Γ_0. Now, if $\ell > 3$, then we know that Γ_0 is generated by its elements of order ℓ, because they generate a normal subgroup and $Z(\Gamma_0) = \{\pm 1\}$ is the only proper normal subgroup (see [**42**, Theorem 5]). Thus, there exists at least one element σ of order ℓ in the complement $G - H$. In particular, the σ-orbit of H in the permutation representation on G/H has ℓ elements, and hence we find that $[G : H] \geqslant \ell$.

On the other hand, the Galois group $\mathrm{Gal}(K/k)$ acts faithfully on the free $\mathbb{Z}$-module $\mathrm{End}_K(A)$, so that it is isomorphic to a finite subgroup F of $\mathrm{GL}(n, \mathbb{Z})$ for some $n \leqslant 2g$. By a theorem of Minkowski, F injects into $\mathrm{GL}(n, \mathbb{Z}/3\mathbb{Z})$ (see, for example, [**39**]) and thus its order is bounded by a constant depending only on g. Let $\ell_1(g)$ be this constant. Since Galois theory gives

$$[G : H] \leqslant |\mathrm{Gal}(K/k)|,$$

it follows from this and the previous paragraph that

$$\ell \leqslant [G : H] \leqslant |F| \leqslant \ell_1(g),$$

as desired. □

Our first (and most general) approach to the problem mentioned in the introduction uses some deep group-theoretic results of Guralnick [**18**] and Liebeck and Saxl [**30**], in order to apply Proposition 4. This is contained in the following result.

PROPOSITION 5. *If $g_1 \geqslant 0$ is a constant, then there is a constant $\ell_2(g_1)$ satisfying the following. If $\ell > \ell_2(g_1)$ and $f : X \to C$ is a geometric Galois cover with group $G = \mathrm{Sp}(2g, \mathbb{F}_\ell)$, then for any proper subgroup $H < G$, the genus of X/H is at least g_1.*

Proof. In the case where f is tamely ramified (for instance, in characteristic zero), this follows from [**30**, Corollary 2 to Theorem 1] and, in the general case, this follows from [**18**, Theorem 1.5]. □

REMARK 6. The constant $\ell_2(g_1)$ is conjectured to be independent of g_1 (see [**18**, Conjecture 1.6]), and in the tame case this follows from [**13**, Theorem A].

What is required for Proposition 5 is a very thorough understanding of the maximal proper subgroups of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$. As written, the results in [**18**, **30**] both use the classification of finite simple groups. More precisely, the proof of [**18**, Corollary 9.5] uses [**30**, Theorem 1] which in turn rests on the classification-dependent Theorem 4.1 of [**29**]. However, we learned from Guralnick that Magaard has an unpublished proof of [**30**, Theorem 1], which does not use the classification.

Proposition 5 forms the main content of the following proposition.

PROPOSITION 7. *If $\ell > \ell_2(g_1(k))$ and A has big monodromy mod ℓ, then A_v has big monodromy mod ℓ for all but finitely many $v \in C(k)$.*

Proof. Let X/k be the smooth curve with function field $k(C)(A[\ell])$. The map of curves $X \to C$ is generically Galois with group G containing Γ_0. Let v be a point in $C(k)$ and let w be a point in X lying over v with the decomposition group $G_v \leqslant \Gamma$. If $H \leqslant G$ is a subgroup not containing Γ_0, and $G_v \leqslant H$, then the image of w in the quotient curve X/H has degree $[G_v : G_v \cap H] = 1$ over v, and thus is a k-rational point of X/H. In particular, to prove the theorem it suffices to show that X/H has genus greater than $g_1(k)$ for any proper subgroup $H < G$ because then Theorem 2 implies that

$$\bigcup_{H<G} (X/H)(k)$$

is finite. However, this is exactly Proposition 5 applied to the proper subgroup $H \cap \Gamma_0$ of Γ_0. □

We can now deduce the following concrete application.

THEOREM 8. *Let k be an infinite field of finite type over the prime field, for instance, a number field. Let $g \geqslant 1$ be an integer, and let $f \in k[X]$ be a square-free polynomial of degree $2g$.*

Let A be the Jacobian of the hyperelliptic curve of genus g over $k(t)$ with the affine model as follows:

$$y^2 = f(x)(x - t).$$

Then there are only finitely many $t \in k$ such that A_t is not geometrically simple.

Proof. By a result of J.-K. Yu and Hall [**19**], A has big monodromy modulo ℓ for any $\ell \geqslant 3$. Choosing $\ell > \max(2, \ell_1(g), \ell_2(g_1(k)))$ yields the desired result by combining Propositions 4 and 7. □

REMARK 9. Zarhin has recently shown [**44**, Theorem 1.5] that, over any field K of characteristic 0, the Jacobian of a hyperelliptic curve with the equation

$$y^2 = f(x)(x - t), \quad f \in K[X], \ t \in K, \ \deg(f) = 2g \geqslant 8, \ f(t) \neq 0,$$

is always absolutely simple under the condition that the splitting field of the polynomial f has a Galois group containing the alternating group A_{2g}. This gives many examples where the finite exceptional set of Theorem 8 is actually empty!

In the theorems above we have used the fact that A has big monodromy modulo some prime ℓ in order to show that almost all the fibers of A_v have big monodromy modulo the same ℓ. It is worth pointing out that the hypothesis that A_v has big monodromy modulo a sufficiently large fixed ℓ_0 actually implies that it has big monodromy modulo almost all ℓ, although we shall only prove it for global fields.

PROPOSITION 10. *Suppose k is a global field, that is, a number field or a function field of a curve over a finite field. If A_v has big monodromy modulo ℓ_0, for some $\ell_0 \geqslant 5$, then there is a constant $\ell_3(A_v)$, so that A_v has big monodromy modulo ℓ for every prime $\ell > \ell_3(A_v)$.*

Proof. If A_v has big monodromy for $\ell_0 \geqslant 5$, then the ℓ_0-adic monodromy group of A_v contains $\mathrm{Aut}(T_{\ell_0} A) \simeq \mathrm{Sp}(2g, \mathbb{Z}_{\ell_0})$ (see [**36**, Lemme 1]). Therefore, if k is a number field, then [**35**, 2.2.7; **36**, Théorème 3] imply that for every sufficiently large ℓ, the ℓ-adic monodromy group of B contains $\mathrm{Sp}(2g, \mathbb{Z}_\ell)$. If k is a function field over a finite field, then one can apply [**36**, 8.2] to deduce a similar statement. □

It is worth noting here that this method does *not* allow the bound $\ell_3(A_v)$ to be chosen independently of A_v. To prove such a uniform bound over a rational function field, for example, would require showing that the Siegel modular varieties parametrizing abelian g-folds with 'H-level structure' contain no unexpected rational curves; this can be carried out when $g = 1$, since the Siegel modular variety is just a curve (see [**7**]) but seems difficult in general. A theorem of Nadel [**33**] proves such a result (as a special case of a much more general theorem) when H is the trivial subgroup of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$.

2. *Methods from arithmetic geometry*, II

In the special case of families of hyperelliptic curves considered in the present paper, we can also obtain results using easier group theory in place of Proposition 5, as we now explain. Again, we will use Proposition 4 to obtain geometric simplicity.

We continue with the notation introduced in the previous section except that now we must work in characteristic zero, and so we assume k is finitely generated over a number field. This implies that Theorem 2 is valid with $g_1(k) = 2$.

First of all, we remark that when A has big monodromy modulo a sufficiently large ℓ and at least three fibers where the reduction is not potentially good, then one can show that A_v has big monodromy modulo ℓ via the results in the forthcoming paper 'Maximal subgroups of classical groups containing a quadratic element' by Hall, which require only Thompson's classification of so-called quadratic pairs [**43**].

By restricting A further, we can make our work even simpler, while still proving a general enough result to obtain the theorems stated in the introduction. For this, we say *A degenerates simply* at v if the identity component of A_v is the extension of an abelian variety by a one-dimensional torus and if the component group of A_v has order prime to ℓ. There are only finitely many v where A degenerates simply. From the group-theoretic point of view, this geometric condition is useful because of the following fact.

LEMMA 11. *With notation as above, if A degenerates simply at v, then the inertia group $I_v \leqslant G_v$ is generated by a transvection.*

Proof. By [**17**, (2.5.4) and Corollaire 3.5.2], I_v is generated by a unipotent element τ satisfying $\dim((\tau - 1)A[\ell]) \leqslant 1$, and hence τ either is a transvection or is trivial. Moreover, $A[\ell]$ does not split over the strict Henselization of the local field $k(C)_v$ because the component group of A_v has order prime to ℓ (cf. [**17**, (11.1.3)]), and hence $k(C)(A[\ell])$ ramifies over v and $\tau \neq 1$ is a transvection, as claimed. □

We shall also use here the following group-theoretic lemma, the potential significance of which is clear from the previous one.

LEMMA 12. *If $\ell \geqslant 3$, then a subgroup of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$ that contains ℓ^{2g-1} transvections is the whole of $\mathrm{Sp}(2g, \mathbb{F}_\ell)$.*

Proof. This follows immediately from a theorem of Brown and Humphries [3], which gives a criterion for a set of transvections to generate the symplectic group $\mathrm{Sp}(2g, \mathbb{F}_\ell)$. More precisely, recall that there is a natural bijection between cyclic groups generated by transvections and lines in $\mathbb{F}_\ell^{2g}$; namely, we take the group generated by τ to the one-dimensional space $(\tau - 1)(\mathbb{F}_\ell^{2g})$. Let $S \subset \mathbb{P}(\mathbb{F}_\ell^{2g})$ be a set of subgroups generated by transvections. Let $G(S)$ be the graph with a set of vertices S and with edges given by those pairs $(s_1, s_2) \in S \times S$ such that the space spanned by s_1 and s_2 (thought of as lines in $\mathbb{F}_\ell^{2g}$) is not isotropic. Then [3] shows that (for $\ell \geqslant 3$) S generates G if and only if the elements of S span $\mathbb{F}_\ell^{2g}$, and if $G(S)$ is connected. If the lines in S fail to span all of $\mathbb{F}_\ell^{2g}$, then obviously

$$|S| \leqslant \frac{\ell^{2g-1} - 1}{\ell - 1}.$$

On the other hand, if $G(S)$ is the disjoint union of two subgraphs, G_1 and G_2, then the subspaces of $\mathbb{F}_\ell^{2g}$ spanned by the vertices of G_1 and G_2 must be mutually orthogonal, and so in particular the union of these vector spaces contains at most $(\ell^{2g-1} - 1)/(\ell - 1)$ lines. In either case, the number of transvections contained in S is at most $\ell^{2g-1} - 1$. □

Now we deduce the following.

Proposition 13. *Let k be a field finitely generated over a number field, let C/k be a smooth projective curve, and let $A/k(C)$ be a principally polarized abelian g-fold. Suppose $\ell \geqslant 3$ is a prime such that A has big monodromy modulo ℓ and that A degenerates simply at*

$$\left\lceil \frac{2(\ell^{2g} - 1)}{(\ell^g - \ell^{g-1})^2} \right\rceil$$

or more places. Then A_v has big monodromy modulo ℓ for all but finitely many $v \in C(k)$.

Proof. We can assume that the places where A degenerates simply are in $C(k)$, because the conclusion will be even stronger after extending scalars to a field of definition of those places. Then, again let X/k be the smooth curve with the function field $k(C)(A[\ell])$. The map of curves $X \to C$ is generically Galois with group G contained in Γ. Again, we use Theorem 2, applied to the curves X/H as H ranges over proper subgroups of Γ_0. As in the proof of Proposition 7, and because $g_1(k) = 2$ now, it suffices to show that all such X/H have genus at least 2.

Fix a proper subgroup $H < \Gamma_0$ and let Y/k be the quotient curve X/H. Suppose that v is a point where A degenerates simply and let $\tau \in I_v$ be a generator. There is an action of τ on the sheets of $Y \times_k k^s$, which is exactly the permutation action on the cosets of Γ_0/H: the orbits correspond to the points of $Y \times_k k^s$ over v and the size of an orbit is the ramification index. Every orbit has 1 or ℓ elements and the coset gH is fixed by τ if and only if $g^{-1}\tau g$ lies in H. In particular, the computation of the ramification of $Y \to C$ at v is reduced to a problem about the conjugates of transvections in G.

By Lemma 12, we have

$$\frac{|\tau^G \cap H|}{|\tau^G|} \leqslant \frac{\ell^{2g-1} - 1}{\ell^{2g} - 1},$$

and so there are at least

$$\frac{\ell^{2g-2}(\ell - 1)}{\ell^{2g} - 1}[G : H]$$

points of $Y \times_k k^s$ over v of ramification degree ℓ. Therefore, if we write m for the number of v in $C(k)$, where A degenerates simply, then from the Riemann–Hurwitz formula we

have that

$$2g(Y) - 2 \geqslant [G : H] \left(\frac{m\ell^{2g-2}(\ell-1)^2}{\ell^{2g}-1} + 2g(C) - 2 \right).$$

In particular, the right-hand side is positive since $m(\ell^g - \ell^{g-1})^2 > 2(\ell^{2g}-1)$, and hence $Y = X/H$ has genus at least two. □

EXAMPLE 14. When A is the Jacobian of

$$y^2 = f(x)(x-t)$$

with $\deg(f) = 2g$, we observe that, for $\ell \geqslant 3$, A degenerates simply at every prime v in $k(t)$ corresponding to the specialization of t to a root of $f(x)$. *A priori*, one could apply the description of the monodromy of A about v given in Section 5 of Hall's forthcoming paper 'Maximal subgroups of classical groups containing a quadratic element' to deduce that it is a transvection, which is why we want it to be simply degenerate (see Lemma 11), but we can also perform a geometric computation to check this directly.

The fact that A_v is the extension of an abelian variety by a one-dimensional torus follows, for instance, from [**1**, § 9.2, Example 8]. The key point is that the fiber of the curve over v is smooth away from a single ordinary double point.

To compute the order of the component group of A_v, one must compute the minimal regular model of the curve over v, which a straightforward calculation reveals to be the union of curve C_1 of genus $g-1$ and a curve C_2 of genus 0 ([**41**, Remark IV.7.7 and Example IV.7.7.1] gives a nice concrete treatment of the blowing-up process required for this computation). Moreover, C_1 and C_2 intersect at two points, from which it follows that one has the divisor intersection numbers $C_1^2 = C_2^2 = -2$ and $C_1 \cdot C_2 = 2$ (cf. [**41**, Proposition IV.8.1]). Using this information one applies [**1**, § 9.6, Theorem 1] to deduce that the component group of A_v is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.

Thus, when $g \geqslant 2$, we immediately recover Theorem 8 using Proposition 13. (The case $g = 1$ is standard; see, for example, [**7**].)

3. *Methods from analytic number theory*

The analytic approach to our problem is based on the conjunction of two sieves: the sieve for Frobenius of Kowalski (see [**25**]), which is a version of the large sieve, and a generalization of Gallagher's larger sieve [**14**]. The prototype of this approach was described in [**25**, Proposition 6.3], which used a standard large sieve instead of the larger sieve. The latter is much more efficient here.

This combination of two sieves is quite appealing, and it may be of interest in other applications. Although we do not know of any previous use of the large sieve to set up a larger sieve, the Elsholtz has, in an earlier work, used the larger sieve to prepare for application of the large sieve (see [**10**]).

The sieve arises because, instead of the 'big monodromy' argument in Proposition 4, we detect non-simple abelian varieties by means of the following alternate criterion.

PROPOSITION 15. *Let k be a number field and A/k be an abelian variety. Let $\mathfrak{p} \subset \mathbb{Z}_k$ be a prime ideal of k with residue field $\mathbb{F}_\mathfrak{p}$ such that A has good reduction at $\mathfrak{p}$. If the abelian variety $A_\mathfrak{p}/\mathbb{F}_\mathfrak{p}$ obtained by reduction of A modulo $\mathfrak{p}$ is geometrically simple, then so is A.*

Proof. This is a tautology, given the theory of reductions of abelian varieties: if A is not geometrically simple, then there exists an isogeny

$$A \simeq A_1 \times A_2$$

with $\dim A_1, \dim A_2 \geqslant 1$, which is defined over some finite Galois extension k'/k. The factors A_1 and A_2 have good reduction at $\mathfrak{p}$, and so, after reducing, we obtain a corresponding non-trivial factorization for $A_{\mathfrak{p}}$ defined over the residue extension of k'/k at $\mathfrak{p}$. □

REMARK 16. It is well known that there exist integral polynomials that are irreducible over $\mathbb{Q}$ but are reducible modulo every prime (this is due to Hilbert; see, for example, [**2**], where it is shown that such polynomials exist of every non-prime degree). Similarly, there are examples of geometrically simple abelian varieties defined over a number field, which are not geometrically simple modulo any prime (see [**12**, **21**]). It would be interesting to know if the analog of the finiteness statement (1) holds for the set $S'(B)$ of parameters of height at most B for which A_t is not simple modulo all primes.

Sieve methods, in particular the large sieve, will be used to detect factorizations of abelian varieties over finite fields (much as they can be used to detect irreducible polynomials), and thus we will proceed by applying Proposition 15 to many different primes.

We first give a new formulation of Gallagher's sieve in number fields. The works of Goldberg [**15**] and Hinz [**23**] contain other versions, which are much more restricted and weaker, and there is also an ongoing work in progress by D. Zywina with a similar result. It is quite interesting that the efficiency of our argument depends crucially on using the height function in the number field, and not some cruder measure of size based on the coefficients in some integral basis, for instance (other sieves are usually not really sensitive to this type of choice of a norm).

Note that the terminology 'larger sieve' arises because this statement is most efficient when trying to control the size of a set that does not intersect a very large number of residue classes modulo a set of primes.

PROPOSITION 17. *Let $k/\mathbb{Q}$ be a number field, let $B > 0$ be a constant, and let $\mathcal{A}$ be a finite set of elements of k such that $H(a) \leqslant B$ for all $a \in \mathcal{A}$, where H denotes the height in k, normalized as described below.*

Let S be a finite set of prime ideals in the ring of integers $\mathbb{Z}_k$. If the order of the image of $\mathcal{A}$ under the reduction map $k \to \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ is $\leqslant \nu(\mathfrak{p})$ for all $\mathfrak{p} \in S$, then we have

$$|\mathcal{A}| \leqslant \frac{\sum_{\mathfrak{p}\in S} \log N\mathfrak{p} - \log(2^{[k:\mathbb{Q}]}B^2)}{\sum_{\mathfrak{p}\in S} \frac{\log N\mathfrak{p}}{\nu(\mathfrak{p})} - \log(2^{[k:\mathbb{Q}]}B^2)},$$

provided *the denominator in this expression is positive.*

REMARK 18. For many applications, the weaker estimate

$$|\mathcal{A}| \leqslant \frac{\sum_{\mathfrak{p}\in S} \log N\mathfrak{p}}{\sum_{\mathfrak{p}\in S} \log N\mathfrak{p}/\nu(\mathfrak{p}) - \log(2^{[k:\mathbb{Q}]}B^2)}, \tag{3}$$

also valid when the denominator is positive, is sufficient. Indeed, this is what we will use.

We indicate which definition of the height we consider, since there are competing normalizations; we follow [**40**, VIII.5], that is, our H is the same as Silverman's H_k. Thus let M_k

be the set of places of k, defined as in [**40**, VIII.5, p. 206] (the set of absolute values on k, which coincide with the standard absolute values when restricted to $\mathbb{Q}$), and let $|\cdot|_v$ denote the absolute value associated with $v \in M_k$.

For $a \in k$, the height of a is defined by

$$H(a) = \prod_{v \in M_k} \max(1, |a|_v^{n_v}),$$

where n_v is the local degree at v, that is, $n_v = [k_v : \mathbb{Q}_v]$, where k_v and $\mathbb{Q}_v$ are the completions of k and $\mathbb{Q}$, respectively, with respect to the metric defined by $|\cdot|_v$ (in particular $n_v = 2$ if v is a complex place).

We will need the following easy and well-known results:

$$H(a) = H(a^{-1}), \quad H(ab) \leqslant H(a)H(b), \quad H(a+b) \leqslant 2^{[k:\mathbb{Q}]} H(a)H(b) \tag{4}$$

for all a, $b \in k^\times$. We also recall that if $v \in M_k$ is a non-archimedean place, associated with a prime ideal $\mathfrak{p}$, then we have

$$|a|_v^{n_v} = (N\mathfrak{p})^{-v_\mathfrak{p}(a)}, \tag{5}$$

where $v_\mathfrak{p}$ is the $\mathfrak{p}$-adic valuation and $N\mathfrak{p} = |\mathbb{F}_\mathfrak{p}| = |\mathbb{Z}_k/\mathfrak{p}\mathbb{Z}_k|$ is the order of the residue field.

We also comment briefly on the reduction map $k \to \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$: if $a \in k$ and $v_\mathfrak{p}(a) < 0$ (that is, if $\mathfrak{p}$ 'divides the denominator' of a), then the image of a modulo $\mathfrak{p}$ is the point at infinity (denoted ∞) in $\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$. We write simply $a \equiv \infty \pmod{\mathfrak{p}}$ to indicate that this is the case.

Proof of Proposition 17. The proof is very similar to the original argument of Gallagher [**14**]. Let

$$\Delta = \prod_{\substack{a,b \in \mathcal{A} \\ a \neq b}} H(a-b),$$

which is a real number at least 1. We compare upper and lower bounds for Δ to obtain the larger sieve inequality. By (4), we first have the following easy lower bound:

$$\Delta \leqslant (2^{[k:\mathbb{Q}]} B^2)^{|\mathcal{A}|(|\mathcal{A}|-1)}. \tag{6}$$

On the other hand, we bound the height from below as follows: by (4) again, switching to the inverse to use (5) with positive valuations, we have

$$\Delta = \prod_{a \neq b} H((a-b)^{-1}) \geqslant \prod_{a \neq b} \prod_{\substack{\mathfrak{p} \in S \\ v_\mathfrak{p}(a-b) > 0}} (N\mathfrak{p})^{v_\mathfrak{p}(a-b)}.$$

It follows that

$$\log \Delta \geqslant \sum_{a \neq b} \sum_{\substack{\mathfrak{p} \in S \\ v_\mathfrak{p}(a-b) > 0}} (\log N\mathfrak{p}) = \sum_{a \neq b} \sum_{\substack{\mathfrak{p} \in S \\ a \equiv b \pmod{\mathfrak{p}}}} (\log N\mathfrak{p}).$$

Now, for all $\mathfrak{p} \in S$ and $\alpha \in \mathbb{P}^1(\mathbb{F}_\mathfrak{p})$, define

$$R_\mathfrak{p}(\alpha) = |\{a \in \mathcal{A} \mid a \equiv \alpha \pmod{\mathfrak{p}}\}|.$$

We obtain

$$\begin{aligned}\log\Delta &\geqslant \sum_{\mathfrak{p}\in S}(\log N\mathfrak{p}) \sum_{\substack{a\neq b\\ a\equiv b \,(\mathrm{mod}\,\mathfrak{p})}} 1\\ &= \sum_{\mathfrak{p}\in S}(\log N\mathfrak{p}) \sum_{\substack{a,b\in\mathcal{A}\\ a\equiv b \,(\mathrm{mod}\,\mathfrak{p})}} 1 - |\mathcal{A}|\sum_{\mathfrak{p}\in S}\log N\mathfrak{p}\\ &= \sum_{\mathfrak{p}\in S}(\log N\mathfrak{p}) \sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} R_{\mathfrak{p}}(\alpha)^2 - |\mathcal{A}|\sum_{\mathfrak{p}\in S}\log N\mathfrak{p}.\end{aligned}$$

However, by Cauchy–Schwarz, and by definition of $\nu(\mathfrak{p})$, we have the familiar lower bound

$$\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} R_{\mathfrak{p}}(\alpha)^2 \geqslant \frac{\left(\sum_{\alpha\in\mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})} R_{\mathfrak{p}}(\alpha)\right)^2}{\nu(\mathfrak{p})} = \frac{|\mathcal{A}|^2}{\nu(\mathfrak{p})},$$

and therefore we obtain

$$\log\Delta \geqslant \sum_{\mathfrak{p}\in S}\left\{\frac{|\mathcal{A}|^2}{\nu(\mathfrak{p})} - |\mathcal{A}|\right\}\log N\mathfrak{p}.$$

Finally, putting things together, we obtain

$$\sum_{\mathfrak{p}\in S}\left\{\frac{|\mathcal{A}|^2}{\nu(\mathfrak{p})} - |\mathcal{A}|\right\}\log N\mathfrak{p} \leqslant \log\Delta \leqslant |\mathcal{A}|(|\mathcal{A}|-1)\log(2^{[k:\mathbb{Q}]}B^2).$$

Simplifying by $|\mathcal{A}|$ and re-arranging gives the result. □

When applying this proposition, we typically know some upper bound on $\nu(\mathfrak{p})$, on average over S, and estimate the right-hand side of (3). In our case, $\nu(\mathfrak{p})$ will be quite small (less than $(N\mathfrak{p})^{1-\delta}$ for some $\delta > 0$), so that if the set S is chosen to be

$$S = \{\mathfrak{p}\subset\mathbb{Z}_k \mid N\mathfrak{p}\leqslant x\}$$

for some parameter $x \geqslant 2$ (as is typically the case), then the first sum in the denominator grows fairly rapidly as x grows.

The strength of the final estimates stems from this, but in a way that is rather surprising compared with the large sieve (for instance): it will come from the fact that one can choose x quite small to make the denominator positive; then the numerator is also fairly small, and hence so is $\mathcal{A}$, but the actual size of the denominator is, in fact, of little significance (though it does contribute a small saving factor; the quality of the upper bound, in this range at least, comes mainly from the small size of x).

From this sketch, one can guess that the only really delicate issue that may arise is if one tries to have estimates uniform in terms of k, since one is then led directly to the difficult issue of showing that there are sufficiently many prime ideals with small norm.

In order to clarify the mechanism, we define

$$\beta_k(x;\delta) = \min\left\{t\geqslant 2 \mid \sum_{N\mathfrak{p}\leqslant t}(N\mathfrak{p})^{-1+\delta}\geqslant x\right\} \quad \text{for } t\geqslant 2,\ 0\leqslant\delta<1, \tag{7}$$

which, intuitively, quantifies the 'convergence to equilibrium' in the Prime Ideal Theorem for k. Note in particular that

$$\beta_k(x;\delta) \geqslant \min\{n\geqslant 2 \mid \text{there is some prime ideal of norm } n\},$$

since *any* sum over primes of smaller norm is zero by definition.

If k is considered to be fixed, then we can deduce, by summation by parts, from the Prime Ideal Theorem that

$$\sum_{N\mathfrak{p}\leqslant t}(N\mathfrak{p})^{-1+\delta}=\frac{t^\delta}{\log t^\delta}+\mathrm{O}\Big(\log\frac{1}{\delta}+\frac{t^\delta}{(\log t^\delta)^2}\Big)$$

for $\delta>0$ and $t\geqslant 2$ with $t^\delta\geqslant 2$, where the implied constant depends on k only. It then follows easily that

$$\beta_k(x;\delta)\ll(2x\log x)^{1/\delta} \tag{8}$$

for $x\geqslant 2$, where the implied constant depends only on k.

Corollary 19. *Let $k/\mathbb{Q}$ be a number field and let $\mathcal{A}$ be a finite set of elements of k such that $H(a)\leqslant B$ for all $a\in\mathcal{A}$, and such that, for all prime ideals $\mathfrak{p}$ in $\mathbb{Z}_k$, the order of the image of $\mathcal{A}$ under the reduction map $k\to\mathbb{P}^1(\mathbb{F}_\mathfrak{p})$ is $\leqslant\nu(\mathfrak{p})$, where*

$$\nu(\mathfrak{p})\leqslant C(N\mathfrak{p})^{1-\gamma^{-1}}(\log N\mathfrak{p})$$

for some constants $C>0$ and $\gamma\geqslant 1$.

Then we have

$$|\mathcal{A}|\leqslant 2[k:\mathbb{Q}]\beta_k\Big(2C\log(2^{[k:\mathbb{Q}]}B^2);\gamma^{-1}\Big)(\log(2^{[k:\mathbb{Q}]}B^2))^{-1}.$$

Proof. Write $\delta=\gamma^{-1}$. Applying Proposition 17 (in the form of (3)) with S taken to be the set

$$S=\{\mathfrak{p}\mid N\mathfrak{p}\leqslant x\}$$

for some $x\geqslant 2$ to be determined later, the denominator of (3) is

$$-\log(2^{[k:\mathbb{Q}]}B^2)+\sum_{\mathfrak{p}\in S}\frac{\log N\mathfrak{p}}{\nu(\mathfrak{p})}\geqslant-\log(2^{[k:\mathbb{Q}]}B^2)+C^{-1}\sum_{N\mathfrak{p}\leqslant x}(N\mathfrak{p})^{-1+\delta}.$$

Thus if we take

$$x=\beta_k\Big(2C\log(2^{[k:\mathbb{Q}]}B^2);\delta\Big),$$

then the definition (7) shows that the denominator is at least $\log(2^{[k:\mathbb{Q}]}B^2)$.

We bound the numerator, on the other hand, rather wastefully in terms of k:

$$\sum_{N\mathfrak{p}\leqslant x}\log N\mathfrak{p}\leqslant[k:\mathbb{Q}](\log x)\pi(x)\leqslant 2[k:\mathbb{Q}]x,$$

(by the Brun–Titchmarsh or Chebychev upper bound for $\pi(x)$). The result is then a direct translation of Proposition 17. □

Under various assumptions, one can easily transform this into concrete results. For simplicity, we do this for a fixed number field; in that case, using (8), we obtain the following.

Corollary 20. *Let k be a fixed number field. With an assumption as in Corollary 19, we have*

$$|\mathcal{A}|\ll(\log(2^{[k:\mathbb{Q}]}B^2))^{\gamma-1}(4C\log(2C\log(2^{[k:\mathbb{Q}]}B)))^\gamma$$

for all $B\geqslant 2$, the implied constant depending only on k.

EXAMPLE 21. For $k = \mathbb{Q}$, using a lower bound such as

$$\pi(x) \geqslant \frac{1}{6}\frac{x}{\log x}$$

for $x \geqslant 2$ (which follows, for example, from [**20**, p. 342]), one gets easily (and rather wastefully) that

$$\beta_{\mathbb{Q}}(x;\delta) \leqslant \Big(\frac{12x}{\delta}\log\frac{2x}{\delta}\Big)^{1/\delta},$$

and hence

$$|\mathcal{A}| \leqslant 2\left(\frac{24C}{\delta}\right)^{1/\delta}(\log 2B^2)^{1/\delta-1}\left(\log\left\{\frac{4C}{\delta}\log(2B^2)\right\}\right)^{1/\delta},$$

under the assumption of Corollary 19 for $k = \mathbb{Q}$.

Now we come to the application of the splitting of Jacobians in our hyperelliptic families. We use the following result, which is itself proved using a version of the large sieve, to derive assumptions such as those in Corollary 19, involving the type of conditions in Proposition 15.

PROPOSITION 22. *Let $\mathbb{F}_q$ be a finite field with q elements, let $g \geqslant 1$ be an integer and let $f \in \mathbb{F}_q[X]$ be a square-free polynomial of degree $2g$. For $t \in \mathbb{F}_q$, let A_t be the Jacobian of the hyperelliptic curve C_t with affine equation*

$$C_t \,:\, y^2 = f(x)(x-t).$$

Then we have

$$|\{t \in \mathbb{F}_q \mid f(t) \neq 0 \text{ and } A_t \text{ is not geometrically simple}\}| \ll g^2 q^{1-\gamma^{-1}}(\log q), \tag{9}$$

where $\gamma = 4g^2 + 2g + 4$ and the implied constant is absolute.

Proof. Fix a prime number $\ell \neq p$. For $t \in \mathbb{F}_q$, we let P_t denote the numerator of the zeta function of C_t, which is the integral polynomial of degree $2g$ given by

$$P_t = \det(1 - TF \mid H^1(A_t, \mathbb{Z}_\ell)),$$

where $H^1(A_t, \mathbb{Z}_\ell) \simeq H^1(C_t, \mathbb{Z}_\ell)$ is the first étale cohomology group of A_t or C_t (this is the 'spectral interpretation' of the zeros of the zeta function of C_t).

Let G_t be the Galois group of the splitting field of P_t. We write W for the Weyl group of the symplectic group $\mathrm{Sp}(2g)$ or, more concretely, the group of order $2^g g!$ consisting of signed permutation matrices in $\mathrm{GL}(n, \mathbb{Z})$. From the application of the sieve for Frobenius in [**26**, Remark after Theorem 8.13], it is known that G_t is, most of the time, isomorphic to W: we have

$$|\{t \in \mathbb{F}_q \mid f(t) \neq 0 \text{ and } G_t \not\simeq W\}| \ll g^2 q^{1-\gamma^{-1}}(\log q),$$

where $\gamma = 4g^2 + 2g + 4$ and the implied constant is *absolute* (the earlier result in [**25**, Theorem 6.2] has $\gamma = 4g^2 + 3g + 5$ instead, which is virtually indistinguishable; it also misses the g^2 factor, due to a slip in the final step of the estimate).

Precisely, this result trivially implies (9) if 'geometrically simple' is replaced by 'simple', since an isogeny (over $\mathbb{F}_q$) of the type

$$A_t \simeq A_1 \times A_2 \tag{10}$$

with $\dim A_1, \dim A_2 \geqslant 1$, implies that

$$P_t = \det(1 - TF \mid H^1(A_1, \mathbb{Z}_\ell))\det(1 - TF \mid H^1(A_2, \mathbb{Z}_\ell)), \tag{11}$$

where both factors are integral polynomials of degree $\geqslant 1$, which can certainly not occur if P_t has the Galois group W.

To claim the result stated in the geometric context, one must exclude factorizations as above, which hold after A_t is base-extended by a finite extension of $\mathbb{F}_q$. For fixed g, one can adapt straightforwardly the corresponding qualitative argument of Chavdarov [**5**, Theorem 2.1, Lemma 5.3]. The dependency on g might be worse than what we claim when applying this directly, but for $g \geqslant 5$ (at least), one can use instead the following elementary argument exploiting the size of the Galois group. First, one can show (see [**27**, Proposition 2.4(2)]) that $G_t \simeq W$ and $g \geqslant 5$ imply that the only multiplicative relations between zeros of P_t must follow from the Riemann hypothesis, that is, if $(\alpha_1, \dots, \alpha_{2g})$ are the inverse roots of P_t, then we have $\mathbb{Q} \otimes_{\mathbb{Z}} R = T$, where we denote

$$R = \left\{ (n_i) \in \mathbb{Z}^{2g} \mid \prod_i \alpha_i^{n_i} = 1 \right\},$$

$$T = \left\{ (m_i) \in \mathbb{Q}^{2g} \mid \sum_j m_j = 0, \text{ and} m_i = m_j \text{ if } \alpha_i = \bar{\alpha}_j \right\}.$$

Now if (10) holds over $\mathbb{F}_{q^m}$, $m \geqslant 1$, then it is easy to see that there must be a relation $\alpha_j^m = \alpha_k^m$ with $j \neq k$, and this corresponds to a relation $(n_i) \in R$ with $n_i = 0$ except $n_j = n_k = m$, which is incompatible with the definition of T. □

Remark 23. The uniformity in g is a nice additional feature of the sieve method, but it is not necessarily crucial here; the uniformity in terms of the characteristic of $\mathbb{F}_q$ is what matters for the later use of this proposition.

It is worth noting one common feature of the geometric and analytic approaches here: the proof of Proposition 22 depends crucially on the same result of J.-K. Yu (reproved in [**19**]) concerning the monodromy modulo ℓ of our hyperelliptic families, over finite fields.

Theorem 24. *Let $k/\mathbb{Q}$ be a number field, let $g \geqslant 1$ be an integer and let $f \in k[X]$ be a square-free polynomial of degree $2g$. For $t \in k$, t not a zero of f, let A_t be the Jacobian of the hyperelliptic curve with the affine equation as follows:*

$$y^2 = f(x)(x - t).$$

For $B \geqslant 1$, let

$$S(B) = \{t \in k \mid H(t) \leqslant B \text{ and } A_t \text{ is not geometrically simple}\}.$$

Then there exists an absolute constant $D \geqslant 0$ such that, for $B \geqslant 2$, we have

$$|S(B)| \ll (\log(2^{[k:\mathbb{Q}]} B^2))^{\gamma-1} (g^2 D \log\log(2^{[k:\mathbb{Q}]} B))^{\gamma},$$

with $\gamma = 4g^2 + 2g + 4$, where the implied constant depends only on k.

Proof. The basic observation is that, if $t \in S(B)$, then for any prime ideal $\mathfrak{p}$, $t \pmod p \in \mathbb{P}^1(\mathbb{F}_{\mathfrak{p}})$ is either a zero of f modulo $\mathfrak{p}$, or ∞, or else ($f(t)$ being non-zero modulo $\mathfrak{p}$ so that A_t has good reduction modulo $\mathfrak{p}$, and its fiber over $\mathfrak{p}$ then being not geometrically simple) $t \pmod{\mathfrak{p}}$ lies in the set $\Omega_{\mathfrak{p}}$ defined by (9) for f relative to $q = N\mathfrak{p}$.

Hence the image of $S(B)$ modulo $\mathfrak{p}$ has cardinality $\nu(\mathfrak{p})$ with

$$\nu(\mathfrak{p}) \leqslant 2g + 1 + |\Omega_{\mathfrak{p}}| \ll g^2 (N\mathfrak{p})^{1-\gamma^{-1}} (\log N\mathfrak{p}),$$

where the implied constant is absolute by Proposition 22. Thus Corollary 20 directly implies the result. □

REMARK 25. In an extremely narrow range, the large sieve (as used originally in [25]) is better than the larger sieve. Indeed, as discussed with many examples in [9], the original larger sieve is better when the number of permitted residue classes (that is, the size of $\Omega_{\mathfrak{p}}$, in our case) is smaller than half of $N\mathfrak{p}$ (this is not quite true any more in our inequality because of the term $\log(2^{[k:\mathbb{Q}]}B^2)$ in the denominator). Proposition 22 clearly shows that we cannot prove this (it may be true, for all we know) unless $N\mathfrak{p}$ is (roughly) larger than $\delta^{-1/\delta}$ (with $\delta \asymp g^2$). However, the bound in Proposition 22 also becomes trivial for g not much beyond this point, and so the range of applicability where the large sieve would be the best is very small.

Appendix. *Survey of abelian varieties for analytic number theorists*

While the basic information about abelian varieties that we use will certainly be well known to readers more familiar with the methods of Sections 1 and 2, this is less likely to be the case for readers whose interests lie more in the direction of analytic number theory and sieves. In order to motivate the basic problem for these readers, we summarize here briefly some background information, which we hope will suffice to make accessible the contents of Section 3 for such readers.

The simplest case of abelian varieties is that of elliptic curves; although our basic question of geometric simplicity is not of interest in this setting (any elliptic curve is geometrically simple), a basic knowledge of elliptic curves can help motivate and understand the general theory. We refer for this to Silverman's book [40], and to the summary in [24, § 11.10], which may also be helpful.

Let k be a number field (for instance, $k = \mathbb{Q}$). An abelian variety A defined over k is, first of all, a *proper irreducible variety* over k; that is, we may think of A as a subset of projective space over k cut out by some set of homogeneous equations in the coordinates, which generate a prime ideal. (In practice, though, one almost never writes down these equations!) What makes A an abelian variety is the presence of a *group law*: a map from $A \times A$ to A which is given by polynomials in the coordinates, and satisfies the usual group axioms: associativity, presence of an inverse, and so on. (One might compare A with the more familiar example of SL_n/k, which is also determined as a subset of k^{n^2} by a set of equations, and which also has a group operation that is polynomial in the matrix entries. The difference is that A is cut out by equations in projective space, while SL_n is cut out by equations in the affine space k^{n^2}.)

Since k is contained in $\mathbb{C}$, we can ask not only about the group of solutions over k to the defining equations of A, but about the set of complex solutions, denoted by $A(\mathbb{C})$. Write g for the dimension of A. It is known that A is necessarily isomorphic to $\mathbb{C}^g/\Lambda$ for some lattice $\Lambda \simeq \mathbb{Z}^{2g} \subset \mathbb{C}^g$; in the one-dimensional case $g = 1$, A is an elliptic curve over k.

In particular, it follows that the subgroup $A[n]$ of elements of order dividing n in A, for any integer $n \geqslant 1$, is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^{2g}$, and moreover the fact that A is defined over k easily implies that the coordinates of elements in $A[n]$ are algebraic numbers, which together generate a finite Galois extension $k(A[n])$ of k.

Algebraic curves provide a natural source of abelian varieties via the construction of the *Jacobian*, which over $\mathbb{C}$ goes back to Jacobi, and over k to Weil. To each non-singular algebraic curve C/k of genus g, one can attach a natural abelian variety $J(C)$ over k of dimension g. One nice feature of Jacobians is that they are *principally polarized*: this is a kind of self-duality, which imposes on $J(C)[n]$ a natural perfect pairing

$$J(C)[n] \times J(C)[n] \longrightarrow \boldsymbol{\mu}_n \simeq \mathbb{Z}/n\mathbb{Z},$$

where $\boldsymbol{\mu}_n$ denotes the group of n th roots of unity.

In fact, the action of $\mathrm{Gal}(\bar{k}/k)$ on the coordinates of $k(A[n])$ is not merely linear, but compatible with the symplectic pairing above and its action on the roots of unity; thus it provides a representation

$$\mathrm{Gal}(\bar{k}/k) \longrightarrow \mathrm{Aut}(A[n]) \simeq G\mathrm{Sp}(2g, \mathbb{Z}/n\mathbb{Z}).$$

The primary examples of abelian varieties treated in this paper are Jacobians of curves; in any event, all the abelian varieties we consider are for simplicity assumed to be principally polarized.

The most delicate issue for Section 3 is that of reductions of an abelian variety modulo prime ideals of $\mathbb{Z}_k$. Suffice it to say here that this can be defined for all but finitely many prime ideals of k (the 'primes of bad reduction'), and that if concrete equations for A are given so that, modulo $\mathfrak{p}$, the resulting equations still define a smooth algebraic variety, then the reduction coincides pretty much with the naïve notion of looking at solutions of the equations with coefficients in extensions of the residue field $\mathbb{Z}_k/\mathfrak{p}$.

Now our basic problem takes root in the following definition: an abelian variety A/k is *simple* if and only if there is no non-trivial abelian variety B over k which is a subvariety of A, except A itself. It is *geometrically simple* if it remains simple even when considered as an abelian variety over an algebraically closed field containing k (such as $\mathbb{C}$ when k is a number field, or an algebraic closure of a finite field when k is finite).

Implicit in the notion of geometric simplicity is that, for most lattices $\Lambda \subset \mathbb{C}^g$, the quotient $\mathbb{C}^g/\Lambda$ is not an abelian variety. It is merely a complex torus; the condition that it embeds as an algebraic subvariety of projective space imposes very strong restrictions on Λ (originally described by Riemann). In particular, if $\mathbb{C}^g/\Lambda$ is an abelian variety, it is not usually possible to find a subspace $V \subset \mathbb{C}^g$, $V \notin \{0, \mathbb{C}^g\}$, such that $\Lambda \cap V$ is a lattice in V and $V/(\Lambda \cap V)$ is an abelian variety. In other words, abelian varieties over $\mathbb{C}$ are 'typically' simple.

Now the question considered in this paper is essentially the following: we form a family, parameterized by elements in k, of curves; then we have an associated family of Jacobian varieties, and we ask: *how frequent is it that those abelian varieties are not geometrically simple*?

The basic approach in Section 3 is founded on the following fact: if an abelian variety A/k is not geometrically simple, then its reduction modulo a prime ideal $\mathfrak{p}$ has the same property (which is intuitive enough). Moreover, a result going back in principle to Poincaré shows that a non-trivial subvariety $B \subset A$ is 'essentially' a direct factor, that is, we have

$$A \simeq B \times C$$

for some other abelian subvariety C, up to finite groups ('up to isogeny'). This is the property (10), which leads to the factorization (11), which we use to control the occurrence of non-geometrically simple varieties.

Note added in proof. We thank J. Achter for pointing out to us a paper of D. Masser ('Specializations of endomorphism rings of abelian varieties', Bull. S.M.F. 124 (1996), 457–476), where questions similar to those of this work are considered using methods of transcendence theory. Masser's main theorem, applied to the special case of our Theorem A, leads to a bound $|S(B)| \ll (\log B)^\lambda$ *for some fixed* λ*, like our Theorem B, but the value of* λ *is super-exponential in terms of the genus.*

Acknowledgements. We wish to thank the referee for indicating a simplification and slight strengthening of our larger-sieve bound.

References

1. S. Bosch, W. Lütkebohmert and M. Raynaud, *Néron models*, Ergebnisse der Mathematik and ihrer Grenzgebiete (3) 21 (Springer, Berlin, 1990).

2. R. Brandl, 'Integer polynomials that are reducible modulo all primes', *Amer. Math. Monthly* 93 (1986) 286–288.

3. R. Brown and S. Humphries, 'Orbits under symplectic transvections, I', *Proc. London Math. Soc.* (3) 52 (1986) 517–531.

4. L. Caporaso, J. Harris and B. Mazur, 'Uniformity of rational points', *J. Amer. Math. Soc.* 10 (1997) 1–35.

5. N. Chavdarov, 'The generic irreducibility of the numerator of the zeta function in a family of curves with large monodromy', *Duke Math. J.* 87 (1997) 151–180.

6. S. D. Cohen, 'The distribution of Galois groups and Hilbert's irreducibility theorem', *Proc. London Math. Soc.* (3) 43 (1981) 227–250.

7. C. A. Cojocaru and J. C. Hall, 'Uniform results for Serre's theorem for elliptic curves', *Int. Math. Res. Notices* 2005 (2005) 3065–3080.

8. B. Conrad, 'Chow's K/k-image and K/k-trace, and the Lang-Néron theorem', *Enseign. Math.* (2) 52 (2006) 37–108.

9. S. E. Croot and C. Elsholtz, 'Variants of Gallagher's larger sieve', *Acta Math. Hungar.* 103 (2004) 243–254.

10. C. Elsholtz, 'The inverse Goldbach problem', *Mathematika* 48 (2003) 151–158.

11. G. Faltings, 'Endlichkeitssätze für abelsche Variatäten über Zahlkörpern', *Invent. Math.* 73 (1983) 349–366.

12. R. J. Fisher, 'Review of "A note on good reduction of simple abelian varieties", by C. Adimoolam', *Math Rev.* 56 (1978) MR 0447259 (electronic) or MR 56 ♯5574 (printed).

13. D. Frohardt and K. Magaard, 'Composition factors of monodromy groups', *Ann. of Math.* (2) 154 (2001) 327–345.

14. P. X. Gallagher, 'A larger sieve', *Acta Arith.* 18 (1971) 77–81.

15. E. L. Goldberg, 'Electrostatic sieve', *Mathematika* 23 (1976) 51–56.

16. H. Grauert, 'Mordells Vermutung über rationale Punkte auf algebraischen Kurven und Funktionenkörper', *Inst. Hautes Études Sci. Publ. Math.* 25 (1965) 131–149.

17. A. Grothendieck, 'Modèles de Néron et monodromie', *Groupes de monodromie en géométrie algébrique, I*, Seminaire de Géometrié Algébrique du Bois-Marie 1967–1969 (SGA 7 I), no. 9, Lecture Notes in Mathematics 288 (Springer, Berlin, 1972) 313–523.

18. R. Guralnick, 'Monodromy groups of coverings of curves', *Galois groups and fundamental groups,* 1–46, Mathematica Sciences Research Institute Publication 41 (Cambridge University Press, Cambridge, 2003).

19. C. Hall, 'Big symplectic or orthogonal monodromy modulo ℓ', *Duke Math J.* 141 (2008) 179–203.

20. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edn (Oxford University Press, Oxford, 1979).

21. K. Hashimoto and N. Murabayashi, 'Shimura curves as intersections of Humbert surfaces and defining equations of QM-curves of genus two', *Tohoku Math. J.* (2) 47 (1995) 271–296.

22. D. R. Heath-Brown, 'The density of rational points on curves and surfaces', *Ann. of Math.* (2) 155 (2002) 553–595.

23. J. Hinz, 'Square-free values of cubic polynomials in algebraic number fields', *J. Number Theory* 32 (1986) 203–320.

24. H. Iwaniec and E. Kowalski, Analytic number theory, Colloquium Publications 53, (American Mathematical Society, Providence, RI, 2004).

25. E. Kowalski, 'The large sieve, monodromy and zeta functions of curves', *J. reine angew. Math.* 601 (2006) 29–69.

26. E. Kowalski, *The large sieve and its applications: arithmetic geometry, random walks and discrete groups.* Cambridge Tracts in Mathematics 175 (Cambridge University Press, Cambridge, MA, 2008).

27. E. Kowalski, 'The large sieve, monodromy and zeta functions of algebraic curves, II: independence of the zeros', *Int. Math. Res. Notices. IMRN* 2008 (2008) 57, Art. ID rnn 091.

28. S. Lang, 'Hyperbolic and Diophantine analysis', *Bull. Amer. Math. Soc.* (*N.S.*) 14 (1986) 159–205.

29. M. Liebeck, 'On the orders of maximal subgroups of the finite classical groups', *Proc. London Math. Soc.* (3) 50 (1985) 426–446.

30. M. Liebeck and J. Saxl, 'Minimal degrees of primitive permutation groups, with an application to monodromy groups of covers of Riemann surfaces', *Proc. London Math. Soc.* (3) 63 (1991) 266–314.

31. Ju. I. Manin, 'Rational points on algebraic curves over function fields', *Izv. Akad. Nauk SSSR Ser. Mat.* 27 (1963) 1395–1440.

32. M. Martin-Deschamps, 'La construction de Kodaira–Parshin, Seminar on arithmetic bundles: the Mordell conjecture, Paris, 1983/84), *Astérisque* 127 (1985) 261–273.

33. A. Nadel, 'The nonexistence of certain level structures on abelian varieties over complex function fields', *Ann. of Math.* (2) 129 (1989) 161–178.

34. P. Samuel, 'Compléments à un article de Hans Grauert sur la conjecture de Mordell', *Inst. Hautes Études Sci. Publ. Math.* 29 (1966) 55–62.

35. J.-P. Serre, *Résumé des cours de 1984–1985 Œuvres*, Collected Papers IV (French) 1985–1998 (Springer, Berlin, 2000).
36. J.-P. Serre, *Letter to Marie–France Vignéras Œuvres*, Collected Papers IV (French) 1985–1998 (Springer, Berlin, 2000).
37. J.-P. Serre, *Lectures on the Mordell–Weil theorem*, Aspects of Mathematics 15 (Vieweg, Wiesbaden, 1989).
38. I. R. Shafarevich, *Basic algebraic geometry. 1. Varieties in projective space*, 2nd edn (Springer, Berlin, 1994) (Translated from the 1988 Russian edition and with notes by Miles Reid).
39. A. Silverberg and Y. Zarhin, 'Semistable reduction and torsion subgroups of abelian varieties', *Ann. Inst. Fourier* (Grenoble) 45 (1995) 403–420.
40. J. Silverman, *The arithmetic of elliptic curves*, Graduate Text in Mathematics 106 (Springer, New York, 1986).
41. J. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics 151 (Springer, New York, 1994).
42. R. Steinberg, *Lectures on Chevalley groups* (Yale University, New Haven, CT, 1968) (Notes prepared by John Faulkner and Robert Wilson).
43. J. G. Thompson, *Quadratic pairs*, Actes du Congrès International des Mathématiciens, Nice, 1970, 1 (Gauthier-Villars, Paris, 1971) 375–376.
44. Y. Zarhin, 'Families of absolutely simple hyperelliptic jacobians', Preprint, 2008, arXiv:0804.4264v1.

Jordan S. Ellenberg
Department of Mathematics
University of Wisconsin
480 Lincoln Drive
Madison, WI 53705
USA

ellenber@math.wisc.edu

Christian Elsholtz
Department of Mathematics
Royal Holloway University of London
Egham
Surrey
TW20 0EX
United Kingdom

christian.elsholtz@rhul.ac.uk

Chris Hall
Department of Mathematics
University of Michigan
Ann Arbor MI 48109
USA

hallcj@umich.edu

Emmanuel Kowalski
ETH Zürich – D-MATH
Rämistrasse 101
8092 Zürich
Switzerland

kowalski@math.ethz.ch