J. Inst. Math. Jussieu (2021) **20**(5), 1455–1496
Published by Cambridge University Press.

doi:10.1017/S1474748019000537

DENSITY RESULTS FOR SPECIALIZATION SETS OF GALOIS COVERS

JOACHIM KÖNIG[1] AND FRANÇOIS LEGRAND[2]

[1] *Department of Mathematical Sciences, KAIST, 291 Daehak-ro Yuseong-gu Daejeon 34141, South Korea* (jkoenig@kaist.ac.kr)
[2] *Institut für Algebra, Fachrichtung Mathematik, TU Dresden, 01062 Dresden, Germany* (francois.legrand@tu-dresden.de)

(Received 20 April 2019; revised 23 September 2019; accepted 28 September 2019; first published online 25 October 2019)

Abstract We provide evidence for this conclusion: given a finite Galois cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ of group G, almost all (in a density sense) realizations of G over $\mathbb{Q}$ do not occur as specializations of f. We show that this holds if the number of branch points of f is sufficiently large, under the abc-conjecture and, possibly, the lower bound predicted by the Malle conjecture for the number of Galois extensions of $\mathbb{Q}$ of given group and bounded discriminant. This widely extends a result of Granville on the lack of $\mathbb{Q}$-rational points on quadratic twists of hyperelliptic curves over $\mathbb{Q}$ with large genus, under the abc-conjecture (a diophantine reformulation of the case $G = \mathbb{Z}/2\mathbb{Z}$ of our result). As a further evidence, we exhibit a few finite groups G for which the above conclusion holds unconditionally for almost all covers of $\mathbb{P}^1_{\mathbb{Q}}$ of group G. We also introduce a local–global principle for specializations of Galois covers $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ and show that it often fails if f has abelian Galois group and sufficiently many branch points, under the abc-conjecture. On the one hand, such a local–global conclusion underscores the 'smallness' of the specialization set of a Galois cover of $\mathbb{P}^1_{\mathbb{Q}}$. On the other hand, it allows to generate conditionally 'many' curves over $\mathbb{Q}$ failing the Hasse principle, thus generalizing a recent result of Clark and Watson devoted to the hyperelliptic case.

Keywords: Galois theory; specializations; the abc-conjecture; the Malle conjecture; the uniformity conjecture; hyperelliptic and superelliptic curves; rational points; twisted covers; the Hasse principle

2010 *Mathematics subject classification*: Primary 11R32
Secondary 11G30; 14E20; 14G05

1. Introduction

Given a finite Galois extension E of the rational function field $\mathbb{Q}(T)$, and a point $t_0 \in \mathbb{P}^1(\mathbb{Q})$, there is a well-known notion of *specialization* $E_{t_0}/\mathbb{Q}$ (see § 2.2.1 for more details). If E is the splitting field of a monic separable polynomial $P(T, Y) \in \mathbb{Q}[T][Y]$ and $t_0 \in \mathbb{Q}$ is such that $P(t_0, Y)$ is separable, then the field E_{t_0} is the splitting field over $\mathbb{Q}$ of $P(t_0, Y)$.

The specialization process has been much studied toward the *inverse Galois problem*, which asks whether every finite group G occurs as the Galois group of a finite Galois extension $F/\mathbb{Q}$. In that case, we shall say that such an extension $F/\mathbb{Q}$ is a *G-extension*.

Indeed, if $E/\mathbb{Q}(T)$ is a finite Galois extension with Galois group G, then *Hilbert's irreducibility theorem* asserts that the specialization $E_{t_0}/\mathbb{Q}$ still has Galois group G for infinitely many $t_0 \in \mathbb{Q}$. Moreover, if $E/\mathbb{Q}(T)$ is $\mathbb{Q}$-*regular* (i.e., if $\mathbb{Q}$ is algebraically closed in E), in which case we shall say that $E/\mathbb{Q}(T)$ is a *regular* G-*extension*, and if $G \neq \{1\}$, then infinitely many linearly disjoint G-extensions of $\mathbb{Q}$ occur as specializations of $E/\mathbb{Q}(T)$. In fact, most known realizations over $\mathbb{Q}$ of finite non-abelian simple groups G have been obtained by specializing regular G-extensions of $\mathbb{Q}(T)$, generally derived from the *rigidity method*. See the books [20, 36, 38, 41] for more details and references within.

Recent progress has been made on the set $\mathrm{Sp}(E)$ of all specializations of a given regular G-extension $E/\mathbb{Q}(T)$. For example, for many groups G, no regular G-extension $E/\mathbb{Q}(T)$ is *parametric*, i.e., $\mathrm{Sp}(E)$ does not contain all G-extensions of $\mathbb{Q}$ (see [26] and [27, § 7]). Another result by Dèbes [13] gives a lower bound for the number of G-extensions of $\mathbb{Q}$ with bounded discriminant lying in the set $\mathrm{Sp}(E)$ for a given regular G-extension $E/\mathbb{Q}(T)$. An even more fundamental question was raised in [14, 17]: does the set $\mathrm{Sp}(E)$, a collection of arithmetic objects, characterize the extension $E/\mathbb{Q}(T)$, a geometric one?

1.1. A central question

Given a regular G-extension $E/\mathbb{Q}(T)$, the main purpose of this paper is to further study the set $\mathrm{Sp}(E)$ and to provide evidence for this striking conclusion: this set is in general 'small', i.e., 'almost all' G-extensions of $\mathbb{Q}$ do not lie in the set $\mathrm{Sp}(E)$.

Let us make this more precise. Given an integer $x \geqslant 1$, let $\mathcal{S}(G, x)$ denote the set of all G-extensions $F/\mathbb{Q}$ such that $|d_F| \leqslant x$, where d_F denotes the absolute discriminant of F. By Hermite's theorem, the set $\mathcal{S}(G, x)$ is finite. Moreover, say that the set $\mathrm{Sp}(E)$ of all specializations of a given regular G-extension $E/\mathbb{Q}(T)$ is *of density zero* if the equality $|\mathrm{Sp}(E) \cap \mathcal{S}(G, x)| = o(|\mathcal{S}(G, x)|)$ holds as x tends to ∞.

Question 1.1. *Let G be a finite group. Is it true that the specialization set $\mathrm{Sp}(E)$ of a given regular G-extension $E/\mathbb{Q}(T)$, not in some 'small' exceptional list, is of density zero?*

The reason why we have to consider an exceptional list in Question 1.1 is that, for some regular G-extensions $E/\mathbb{Q}(T)$, the specialization set $\mathrm{Sp}(E)$ is not of density zero. For example, this happens for all parametric extensions $E/\mathbb{Q}(T)$, in which case a fully opposite conclusion holds. However, all extensions which are known to satisfy this property are in fact *generic* (that is, remain parametric after every base change) and, in particular, are all of genus 0 and belong to a very short list (see [17, Theorem 1.6] for more details).

In addition to the generic extensions $E/\mathbb{Q}(T)$, there are some more counterexamples in genus 1. For instance, results of Vatsal [40], Byeon [5], and later Byeon–Jeon–Kim [6] about rank 1 quadratic twists of elliptic curves yield infinite families of separable degree 3 polynomials $P(T) \in \mathbb{Z}[T]$ such that a positive proportion of all quadratic extensions of $\mathbb{Q}$ occur as specializations of the extension $\mathbb{Q}(T)(\sqrt{P(T)})/\mathbb{Q}(T)$. More generally, under Goldfeld's conjecture, 50% of all quadratic extensions of $\mathbb{Q}$ are expected to be reached by specializing the function field extension corresponding to an elliptic curve over $\mathbb{Q}$.

However, we are not aware of any counterexample in genus at least 2, and we in fact expect the answer to Question 1.1 to be 'Yes' if regular G-extensions of $\mathbb{Q}(T)$ of genus at most 1, which are quite rare and do not even exist for many finite groups G (e.g., for

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

all finite non-solvable groups), are left aside. Evidence for this is provided by [17], which proves an analog over the rational function field $\mathbb{C}(Y)$, with the notion of specialization replaced by a geometric analog of 'rational pullback' and the notion of density also replaced by a geometric analog via the Zariski topology.

In this paper, we make progress on Question 1.1 in several directions. First, in § 3, we show that the answer is affirmative if one excludes regular G-extensions of $\mathbb{Q}(T)$ with very few branch points, conditionally on widely accepted conjectures (see § 1.2). Second, in § 4, we show for some exemplary small finite groups G that, upon ignoring a 'small' (in a density sense) set of regular G-extensions of $\mathbb{Q}(T)$, the answer to Question 1.1 is positive unconditionally (see § 1.3). In this latter context, we do not have any restriction on the number of branch points or the genus, thus suggesting that the density zero conclusion, which we expect to hold always in genus at least 2, may also hold for 'many' regular G-extensions of $\mathbb{Q}(T)$ of genus at most 1. For example, it is plausible that this conclusion holds for all genus 0 extensions which are not parametric.

1.2. Conditional results

We first give an upper bound for the number of specializations of a given regular G-extension of $\mathbb{Q}(T)$ with bounded discriminant, under the abc-conjecture:

The abc-conjecture. *For every $\epsilon > 0$, there exists a positive constant $K(\epsilon)$ such that, for all coprime integers a, b, and c fulfilling $a + b = c$, the following holds:*

$$c \leqslant K(\epsilon) \cdot \mathrm{rad}(abc)^{1+\epsilon},$$

where the radical $\mathrm{rad}(n)$ *of an integer $n \geqslant 1$ is the product of the distinct prime factors of n.*

Theorem 1.2. *Let G be a finite group and $E/\mathbb{Q}(T)$ a regular G-extension with $r \geqslant 5$ branch points. Suppose the abc-conjecture holds. Then there is a 'small' constant $e > 0$, depending only on r, $|G|$, and the ramification indices of the branch points of $E/\mathbb{Q}(T)$, such that the following holds. For every $\epsilon > 0$ and every sufficiently large integer x, one has*

$$|\mathrm{Sp}(E) \cap \mathcal{S}(G, x)| \leqslant x^{e+\epsilon}. \tag{1.1}$$

See Theorem 3.1 for a more precise statement where we relax the lower bound on r and give the precise definition of the exponent e.

To show that the specialization set of a given regular G-extension of $\mathbb{Q}(T)$ with sufficiently many branch points is of density 0 (under the abc-conjecture), it then suffices, by (1.1), to show that $|\mathcal{S}(G, x)|$ is asymptotically 'bigger' than x^e. A main difficulty to get this conclusion is that the asymptotic behavior of $|\mathcal{S}(G, x)|$ is widely unknown for arbitrary finite groups G. However, general conjectures are available in the literature.

For example, the Malle conjecture [35], a classical landmark in this context, asserts that if k is a number field and G a finite group, then the number of G-extensions of k whose relative discriminant has norm at most x is roughly asymptotic to $x^{\alpha(G)}$, for some well-defined constant $\alpha(G)$ (recalled in (1.3)). See [35] for more details and [13, § 1.1] for a recent review of the state of the art on the conjecture and its generalizations.

We only recall in details the lower bound predicted by the conjecture (in the specific case $k = \mathbb{Q}$), which is enough for our purposes:

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

The Malle conjecture (lower bound). *Let G be a non-trivial finite group and let p be the smallest prime divisor of $|G|$. Then there exists a positive constant $c(G)$ such that*

$$c(G) \cdot x^{\alpha(G)} \leqslant |\mathcal{S}(G, x)| \tag{1.2}$$

for every sufficiently large integer x, where

$$\alpha(G) = \frac{1}{|G|} \cdot \frac{p}{p-1}. \tag{1.3}$$

Note that if the lower bound (1.2) holds for a given finite group G (for sufficiently large x), then G occurs as a Galois group over $\mathbb{Q}$.

The combination of (1.1) and (1.2) then allows us to give this answer to Question 1.1:

Theorem 1.3. *Let G be a finite group and $E/\mathbb{Q}(T)$ a regular G-extension with $r \geqslant 7$ branch points. Suppose (1.2) is fulfilled for the group G and the abc-conjecture holds. Then the set of specializations of $E/\mathbb{Q}(T)$ is of density zero.*

See Corollary 3.3 for a more precise statement. It should be pointed out that the bound $r \geqslant 7$ is not sharp (toward a density zero conclusion for every regular G-extension of $\mathbb{Q}(T)$ of genus at least 2). For example, we can easily drop to $r \geqslant 6$ if $|G|$ is odd or to $r \geqslant 5$ if $|G|$ is prime to 6. Moreover, we obtain a conditional linear bound (depending on G) on the genus of a given regular G-extension $E/\mathbb{Q}(T)$ for the set $\mathrm{Sp}(E)$ being of density 0. See Remark 3.4 for more details.

The bound (1.2) is known to hold for several finite groups, thus providing concrete situations for which Theorem 1.3 can be worded without mentioning it. For instance, relying on Shafarevich's theorem solving the inverse Galois problem for solvable groups, Klüners and Malle [30] proved the (lower bound of the) Malle conjecture for nilpotent groups. Another example is given by dihedral groups of order $2p$ with p an odd prime, as proved by Klüners in [28]. Moreover, many finite groups G are such that every regular G-extension of $\mathbb{Q}(T)$ has at least 7 branch points, thus yielding examples of groups G for which the specialization set of *every* regular G-extension of $\mathbb{Q}(T)$ is of density zero, under the abc-conjecture and, possibly, the lower bound (1.2). Such considerations are collected in Corollary 3.5.

Although there is no known counterexample, the bound (1.2) remains widely open, e.g., for most non-solvable groups. In the sequel, we give a variant of Theorem 1.3 which applies to all finite groups, where the assumption that (1.2) holds is not needed but where the bound on the number of branch points is less explicit. See Theorem 3.7 for more details. This uses the already mentioned result of Dèbes [13], whose aim was to provide an unconditional weak version of the bound (1.2) for regular Galois groups over $\mathbb{Q}$ (i.e., for finite groups G such that there is a regular G-extension of $\mathbb{Q}(T)$), obtained by considering G-extensions of $\mathbb{Q}$ which arise as specializations of a single regular G-extension of $\mathbb{Q}(T)$. It should be pointed out that, by Theorem 1.3, one cannot hope (for arbitrary finite groups G) to obtain the exact bound (1.2) in this way, thereby showing the limitations of the approach in [13].

As a further result, we give a second variant, where the abc-conjecture is not required and no assumption on the number of branch points is made, provided the

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

uniformity conjecture[1] holds and the upper bound from the Malle conjecture for some quotient of the underlying Galois group is taken into account (see Theorem 3.9). As under the abc-conjecture, we may derive explicit examples of finite groups G for which the specialization set of every regular G-extension of $\mathbb{Q}(T)$ is of density zero, under the uniformity conjecture (see Corollary 3.11). Note that, as Theorem 1.3 and its consequences, Corollary 3.11 easily provides density zero conclusions for regular G-extensions of $\mathbb{Q}(T)$ with few branch points.

1.3. Unconditional results

We start with the quadratic case. In the work [34], it was proved that, for 'almost all' regular $\mathbb{Z}/2\mathbb{Z}$-extensions $E/\mathbb{Q}(T)$, at least one quadratic extension of $\mathbb{Q}$ is not in $\mathbf{Sp}(E)$. Here, we sharpen this result as follows:

Theorem 1.4. *Given an even positive integer r, the proportion of all regular $\mathbb{Z}/2\mathbb{Z}$-extensions $E/\mathbb{Q}(T)$ with r branch points, 'height' at most H, and whose set of specializations is of density* 0 *tends to* 1 *as H tends to ∞.*

From a diophantine point of view, this means that 'most' quadratic twists of 'most' hyperelliptic curves over $\mathbb{Q}$ have only trivial $\mathbb{Q}$-rational points, unconditionally (see Proposition 2.3(b)). See Theorems 4.1 and 4.2 for more precise statements, and § 1.6 for diophantine considerations in a more general context.

On the one hand, Theorem 1.4 shows that invoking the abc-conjecture in the case $G = \mathbb{Z}/2\mathbb{Z}$ of Theorem 1.3 is only necessary for comparatively few extensions. On the other hand, it shows that even among regular $\mathbb{Z}/2\mathbb{Z}$-extensions of $\mathbb{Q}(T)$ to which Theorem 1.3 does not apply (i.e., those with $r \leqslant 6$ branch points), only a few can be exceptions in Question 1.1.[2]

The second example we discuss is the symmetric group S_3. In this context, we have this result (see Theorem 4.7 for a more precise statement):

Theorem 1.5. *Let D be a positive integer. Then inside the set of all polynomials $P(T, Y) = Y^3 + a(T)Y^2 + b(T)Y + c(T)$ with $a(T), b(T), c(T) \in \mathbb{Z}[T]$ of degree $\leqslant D$ and of height $\leqslant H$, the set of those $P(T, Y)$ which additionally define a regular S_3-extension of $\mathbb{Q}(T)$ whose specialization set is of density zero, makes up a proportion tending to* 1 *as H tends to ∞.*

1.4. Comparison with previous non-parametricity results

As already said, it was known from [26] and [27, § 7] that many finite groups G do not have any parametric extension $E/\mathbb{Q}(T)$. However, our results sharpen conditionally this conclusion. Indeed, by Theorem 1.3, for many finite groups G, not only at least one G-extension of $\mathbb{Q}$ but actually almost all of them are not specializations of a given regular

[1] Which asserts that the number of $\mathbb{Q}$-rational points on any given smooth curve over $\mathbb{Q}$ of genus at least 2 is bounded by a quantity which depends only on the genus of the curve (but not on the curve itself).
[2] Clearly, there are exceptions in the case $r = 2$ and, as already recalled in § 1.1, exceptions also exist in the case $r = 4$. However, no exception seems to be expected in the case $r = 6$ [24, Conjecture 1].

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

G-extension of $\mathbb{Q}(T)$, under the abc-conjecture. Moreover, this yields (conditional) new examples of finite groups with no parametric extension $E/\mathbb{Q}(T)$ (see Remark 3.6(b)). Furthermore, a property shared by the groups $\mathbb{Z}/2\mathbb{Z}$ and S_3 is that they admit a parametric extension $E/\mathbb{Q}(T)$. Theorems 1.4 and 1.5 show that if $G = \mathbb{Z}/2\mathbb{Z}$ or S_3, then parametric realizations are rare and, for almost all regular G-extensions $E/\mathbb{Q}(T)$, the same fully opposite conclusion on the size of $\mathrm{Sp}(E)$ holds.

1.5. Local–global considerations

Our conditional results are global results, in the sense that they depend on diophantine properties and the arithmetic of curves over $\mathbb{Q}$. On the contrary, our unconditional results are mostly due to local arguments. Namely, given a regular G-extension $E/\mathbb{Q}(T)$, let $\mathrm{Sp}(E)^{\mathrm{loc}}$ be the set of all G-extensions $F/\mathbb{Q}$ such that $F\mathbb{Q}_p/\mathbb{Q}_p$ is a specialization of $E\mathbb{Q}_p/\mathbb{Q}_p(T)$ for all primes p (including $p=\infty$, in which case $\mathbb{Q}_p = \mathbb{R}$). Our local arguments consist in proving that, for almost all regular G-extensions $E/\mathbb{Q}(T)$,

$$\frac{|\mathrm{Sp}(E)^{\mathrm{loc}} \cap \mathcal{S}(G,x)|}{|\mathcal{S}(G,x)|} \tag{1.4}$$

tends to 0 as x tends to ∞, thus yielding, in particular, that $\mathrm{Sp}(E)$ is of density 0. That is, almost all G-extensions $F/\mathbb{Q}$ are not specializations of $E/\mathbb{Q}(T)$ as this is wrong even up to base change from $\mathbb{Q}$ to $\mathbb{Q}_p$ (for at least one suitable prime p depending on F). This suggests this refinement of Question 1.1, which asks whether the specialization set of $E/\mathbb{Q}(T)$ is of density 0 even within the set of those G-extensions of $\mathbb{Q}$ who pass these local obstructions:

Question 1.6. *Let G be a finite group. Does it hold that, for a given regular G-extension $E/\mathbb{Q}(T)$, not in some exceptional list, the ratio*

$$\frac{|\mathrm{Sp}(E) \cap \mathcal{S}(G,x)|}{|\mathrm{Sp}(E)^{\mathrm{loc}} \cap \mathcal{S}(G,x)|} \tag{1.5}$$

tends to 0 as x tends to ∞?

A positive answer means that there exist 'many' G-extensions of $\mathbb{Q}$ which are not specializations of $E/\mathbb{Q}(T)$, but this cannot be detected by local considerations, implying the failure of a local–global principle for specializations.

In § 5, we prove the following result, which provides some evidence for a positive answer to Question 1.6 and strengthens the conclusion of Theorem 1.3 for abelian groups:

Theorem 1.7. *Let G be a finite abelian group and $E/\mathbb{Q}(T)$ a regular G-extension with $r \geqslant 7$ branch points. Then the ratio (1.5) tends to 0 as x tends to ∞, under the abc-conjecture.*

See Theorem 5.2 for a more general result which applies to any finite group G with non-trivial center and to any regular G-extension $E/\mathbb{Q}(T)$ with $r \geqslant 8$ branch points ($r \geqslant 7$ is sufficient for abelian groups) and suitable geometric inertia groups.

1.6. Diophantine aspects

In § 6, we discuss diophantine aspects of our results, whose most general versions in the sequel are actually worded in terms of Galois covers of $\mathbb{P}^1$.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Given a regular Galois cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ with Galois group G and a (continuous) epimorphism $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$, where $\mathrm{G}_{\mathbb{Q}}$ denotes the absolute Galois group of $\mathbb{Q}$, there is a notion of *twisted cover* $\widetilde{f}^{\varphi} : \widetilde{X}^{\varphi} \to \mathbb{P}^1_{\mathbb{Q}}$, introduced by Dèbes in [11], which satisfies this property: φ is a specialization morphism of f[3] if and only if $\widetilde{X}^{\varphi}$ has a *non-trivial* $\mathbb{Q}$-rational point, i.e., a $\mathbb{Q}$-rational point which does not extend any branch point of f. See § 6.1 for more details.

Hence, the most general versions of Theorems 1.2–1.5 can be stated with this diophantine flavor. For example, the corresponding variant of Theorem 1.2 provides, for a regular Galois cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ of group G with $r \geqslant 5$ branch points, an upper bound for the number of epimorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ of bounded discriminant such that the twisted curve $\widetilde{X}^{\varphi}$ has at least one non-trivial $\mathbb{Q}$-rational point. See Theorem 6.4 for a more precise statement. The special case $G = \mathbb{Z}/2\mathbb{Z}$ of our result is nothing but a well-known result of Granville [24, Corollary 1] on the number of quadratic twists of a given hyperelliptic curve over $\mathbb{Q}$ of genus at least 2 with non-trivial $\mathbb{Q}$-rational points, under the abc-conjecture (see Corollary 6.5).

Similarly, the same applies to Theorem 1.7. Given a regular Galois cover $f : X \to \mathbb{P}^1_{\mathbb{Q}}$ of group G, the existence of an epimorphism $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ which occurs as a specialization morphism of f everywhere locally but not globally means that the twisted curve $\widetilde{X}^{\varphi}$ has a non-trivial $\mathbb{Q}_p$-rational point for every prime p but only trivial $\mathbb{Q}$-rational points. This diophantine reformulation of the failure of our local–global principle for specializations is actually strictly identical to the failure of the Hasse principle for curves, provided f has no $\mathbb{Q}$-rational branch point. In particular, the diophantine analog of Theorem 1.7 provides the following:

Theorem 1.8. *Let C be a $\mathbb{Q}$-curve with a finite abelian cover f to $\mathbb{P}^1$ such that f has at least 7 branch points and f has no $\mathbb{Q}$-rational branch point. Assume the abc-conjecture holds. Then there exist 'many' $\mathbb{Q}$-curves C', which are isomorphic to C up to base change from $\mathbb{Q}$ to $\overline{\mathbb{Q}}$ and which do not fulfill the Hasse principle.*

See Corollary 6.6 for a more general result, which also applies in some non-abelian situations, and Corollary 6.9 for a variant which in fact applies to any regular Galois group over $\mathbb{Q}$ with non-trivial center, at the cost of choosing the curve C more suitably. In the quadratic case, our results allow to retrieve a recent result of Clark and Watson [8, Theorem 2], which asserts that 'many' quadratic twists of a hyperelliptic curve $C : y^2 = P(t)$ with $P(T) \in \mathbb{Z}[T]$ separable, of even degree $\geqslant 8$, and with no root in $\mathbb{Q}$ do not fulfill the Hasse principle, under the abc-conjecture (see Corollary 6.7).

2. Basics

The aim of this section is fourfold. Section 2.1 is devoted to some general notation we shall use in the sequel. In § 2.2, we recall classical material about Galois covers of the projective line while § 2.3 is devoted to rational points on superelliptic curves. As to § 2.4, we there make the content of § 2.2 explicit in the quadratic case, in relation with the material from § 2.3.

[3] A refined version of 'a G-extension $F/\mathbb{Q}$ occurs as a specialization of a regular G-extension $E/\mathbb{Q}(T)$'.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

2.1. General notation

Denote the absolute Galois group of a field k of characteristic zero by G_k. If k' is a field containing k, we use the notation $\otimes_k k'$ for the scalar extension from k to k'. For example, if X is a k-curve, then $X \otimes_k k'$ is the k'-curve obtained by scalar extension from k to k'. Conjugation automorphisms in a group G are denoted by $\mathrm{conj}(\omega)$ for $\omega \in G$: $\mathrm{conj}(\omega)(x) = \omega x \omega^{-1}$ $(x \in G)$.

Let $n \geqslant 2$, $N \geqslant 1$, $x \geqslant 1$, and $H \geqslant 1$ be integers. Let G be a finite group and T an indeterminate. We use the following notation:

(a) $\mathcal{S}(G, x)$: set of all G-extensions $F/\mathbb{Q}$ such that $|d_F| \leqslant x$, where d_F denotes the absolute discriminant of the number field F.

(b) $\overline{\mathcal{S}}(G, x)$: set of all (continuous) epimorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ such that $\overline{\mathbb{Q}}^{\ker(\varphi)}/\mathbb{Q} \in \mathcal{S}(G, x)$, modulo the equivalence which identifies φ and φ' if $\varphi' = \mathrm{conj}(\omega) \circ \varphi$ for some $\omega \in G$ (the set $\overline{\mathcal{S}}(G, x)$ refines the set $\mathcal{S}(G, x)$ but note that the cardinalities are equal up to an explicit multiplicative constant depending only on G).

(c) $\mathcal{N}_n$: set of all n-free integers, that is, of all integers d such that $d \notin \{0, 1\}$ and p^n divides d for no prime number p (if $n = 2$, we say squarefree instead of 2-free); recall that $\mathcal{N}_n$ has density $1/\zeta(n)$, where ζ denotes the Riemann zeta function.

(d) $\mathcal{N}_n(x)$: subset of $\mathcal{N}_n$ defined by the extra condition that $|d| \leqslant x$.

(e) $\mathcal{P}(n, N)$: set of all degree N polynomials $P(T) \in \mathbb{Z}[T]$ whose roots have multiplicity $\leqslant n - 1$.

(f) $\mathcal{P}(n, N, H)$: subset of $\mathcal{P}(n, N)$ defined by the extra condition that the height is at most H; recall that the height of $a_0 + a_1 T + \cdots + a_N T^N$ is $\max(|a_0|, \ldots, |a_N|)$.

(g) $\mathcal{P}_2(n, N)$: subset of $\mathcal{P}(n, N)$ which consists of all elements $P(T)$ with squarefree content.

(h) $\mathcal{P}_2(n, N, H) = \mathcal{P}_2(n, N) \cap \mathcal{P}(n, N, H)$.

Definition 2.1. Let B be a set, $(B_n)_{n \geqslant 1}$ an increasing sequence of finite subsets of B such that $B = \bigcup_{n \geqslant 1} B_n$, and A a subset of B. If

$$\frac{|A \cap B_n|}{|B_n|}$$

tends to some $d \in [0, 1]$ as n tends to ∞, we say that d is the *density* of the set A (in B).

Although this notion depends on the sequence $(B_n)_{n \geqslant 1}$, we do not make this dependency explicit in the terminology as our choices in the sequel will always be natural.

2.2. Finite Galois covers of the projective line

Let k be a field of characteristic zero, T an indeterminate, Ω an algebraic closure of $k(T)$, and $\overline{k}$ the algebraic closure of k in Ω.

2.2.1. Generalities. For more on the material below, we mostly refer to [16, § 2.1].

A *k-cover* of $\mathbb{P}^1$ is a finite and generically unramified morphism $f : X \to \mathbb{P}^1$ defined over k, with X a normal and irreducible k-curve. We make no distinction between a

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

k-cover $f : X \to \mathbb{P}^1$ and the associated function field extension $E/k(T)$ (with $E \subseteq \Omega$): f is the normalization of $\mathbb{P}^1$ in E and E is the function field $k(X)$ of X. The k-cover $f : X \to \mathbb{P}^1$ is said to be *regular* if E is a regular extension of k (i.e., if $E \cap \overline{k} = k$) or, equivalently, if X is geometrically irreducible. We also say that the k-cover $f : X \to \mathbb{P}^1$ is *Galois* if $E/k(T)$ is. If, in addition, G denotes the Galois group of $E/k(T)$, we say that f is a *k-G-cover*.

Fix a regular k-cover $f : X \to \mathbb{P}^1$ and denote its function field extension by $E/k(T)$.

A point $t_0 \in \mathbb{P}^1(\overline{k})$ is a *branch point* of f (or of $E/k(T)$) if the prime ideal of $\overline{k}[T - t_0]$ generated by $T - t_0$ ramifies in the integral closure of $\overline{k}[T - t_0]$ in the compositum $\widehat{E}\overline{k}$ of $\widehat{E}$ and $\overline{k}(T)$ inside Ω (set $T - t_0 = 1/T$ if $t_0 = \infty$), where $\widehat{E}$ denotes the Galois closure of E over $k(T)$ inside Ω. There are only finitely many branch points, denoted by $t_1, \dots, t_r$.

Suppose f is Galois and set $G = \mathrm{Gal}(E/k(T))$. Say that $E/k(T)$ is a *regular G-extension*.

Denote the k-fundamental group of $\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}$ by $\pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_k$, where $t \in \mathbb{P}^1(\overline{k}) \setminus \{t_1, \dots, t_r\}$ is a base point. To the regular k-G-cover $f : X \to \mathbb{P}^1$ corresponds an epimorphism $\phi : \pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_k \to G$ whose restriction to the $\overline{k}$-fundamental group $\pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_{\overline{k}}$ remains surjective.

Every $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$ yields a section $s_{t_0} : \mathrm{G}_k \to \pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_k$ to the exact sequence

$$1 \to \pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_{\overline{k}} \to \pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_k \to \mathrm{G}_k \to 1,$$

which is uniquely defined up to conjugation by an element of $\pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_{\overline{k}}$. The homomorphism $\phi \circ s_{t_0} : \mathrm{G}_k \to G$ is denoted by f_{t_0} and called the *specialization morphism* of f at t_0. The fixed field in $\overline{k}$ of $\ker(f_{t_0})$ is the residue field at some prime ideal $\mathfrak{p}$ lying over the prime ideal of $k[T - t_0]$ generated by $T - t_0$ in the extension $E/k(T)$.[4] We denote it by E_{t_0} and call the extension E_{t_0}/k the *specialization* of $E/k(T)$ at t_0. The Galois group of E_{t_0}/k is the decomposition group of $E/k(T)$ at a prime $\mathfrak{p}$ as above.

Let us define the following two sets:

$$\mathrm{Sp}(f) = \{f_{t_0} : \mathrm{G}_k \to G : t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}\},$$
$$\mathrm{Sp}(E) = \{E_{t_0}/k : t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}\}.$$

As a special case of Definition 2.1, say that $d \in [0, 1]$ is the *density* of the set $\mathrm{Sp}(f)$ if

$$\frac{|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G, x)|}{|\overline{\mathcal{S}}(G, x)|}$$

tends to d as x tends to ∞. We define analogously the density of the set $\mathrm{Sp}(E)$. Note that the set $\mathrm{Sp}(f)$ is of density 0 if and only if the set $\mathrm{Sp}(E)$ is.

Recall that $E/k(T)$ is *parametric* if every G-extension of k lies in the set $\mathrm{Sp}(E)$, and that $E/k(T)$ is *generic* if $Ek'/k'(T)$ is parametric for every overfield $k' \supseteq k$.

2.2.2. Ramification in specializations. We review a well-known result relating the ramification of f to that of its specializations. Keep the notation from § 2.2.1 and take $k = \mathbb{Q}$.

[4] This does not depend on the choice of $\mathfrak{p}$ as the extension $E/k(T)$ is Galois.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

The *minimal polynomial* of $t = [a : b] \in \mathbb{P}^1(\overline{\mathbb{Q}})$ is the unique (up to sign) homogeneous polynomial $P(U, V) \in \mathbb{Z}[U, V]$ defined as follows. If $b = 0$, set $P(U, V) = V$. Otherwise, let $P(U, V)$ be the homogenization of the irreducible polynomial in $\mathbb{Z}[U]$ with root a/b. Given a prime number p, say that t is *p-integral* if p divides neither the coefficient of the leading U-term nor of the leading V-term of $P(U, V)$. If t_0 is in $\mathbb{P}^1(\mathbb{Q}) \setminus \{t\}$, set $t_0 = [a' : b']$ with a' and b' coprime integers. Define $I_p(t_0, t)$ as the p-adic valuation of $P(a', b')$ (if t is p-integral).

The theorem below is an immediate consequence of a fundamental result of Beckmann [1, Proposition 4.2] (see also [33, § 2.2]):

Theorem 2.2. *For every prime number p, not in some finite set $\mathcal{S}_{\text{exc}}$ depending only on f, and every $t_0 \in \mathbb{P}^1(\mathbb{Q}) \setminus \{t_1, \dots, t_r\}$, the following two conclusions hold.*

(a) *If p ramifies in the specialization $E_{t_0}/\mathbb{Q}$, then $I_p(t_0, t_i) > 0$ for some (necessarily unique up to $\mathbb{Q}$-conjugation) $i \in \{1, \dots, r\}$.*

(b) *If $I_p(t_0, t_i) > 0$, then the inertia group of $E_{t_0}/\mathbb{Q}$ at p is conjugate in G to $\langle \tau_i^{I_p(t_0,t_i)} \rangle$, with τ_i a generator of an inertia subgroup of $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(T)$ at the prime ideal generated by $T - t_i$.*

2.3. Superelliptic curves

Let n and N be integers with $n \geqslant 2$ and $N \geqslant 1$. Set $N = qn + r$, with $q \geqslant 0$ and $0 \leqslant r \leqslant n - 1$. Let $P(T) = a_0 + a_1 T + \cdots + a_{N-1} T^{N-1} + a_N T^N$ be in $\mathcal{P}(n, N)$.

2.3.1. The case where n divides N. First, assume $r = 0$. Consider this equivalence relation on $\overline{\mathbb{Q}}^3 \setminus \{(0, 0, 0)\}$: $(y_1, t_1, z_1) \sim (y_2, t_2, z_2)$ iff $(y_2, t_2, z_2) = (\lambda^{N/n} y_1, \lambda t_1, \lambda z_1)$ for some $\lambda \in \overline{\mathbb{Q}} \setminus \{0\}$. The quotient space $(\overline{\mathbb{Q}}^3 \setminus \{(0, 0, 0)\})/\sim$ is a weighted projective space, denoted by $\mathbb{P}_{N/n,1,1}(\overline{\mathbb{Q}})$. Given $(y, t, z) \in \overline{\mathbb{Q}}^3 \setminus \{(0, 0, 0)\}$, the corresponding point in $\mathbb{P}_{N/n,1,1}(\overline{\mathbb{Q}})$ is denoted by $[y : t : z]$. Set

$$P(T, Z) = a_0 Z^N + a_1 Z^{N-1} T + \cdots + a_{N-1} Z T^{N-1} + a_N T^N.$$

The equation $Y^n = P(T, Z)$ in $\mathbb{P}_{N/n,1,1}(\overline{\mathbb{Q}})$ is *the superelliptic*[5] *curve associated with* $P(T)$; we denote it by $C_{P(T)}$. The set of all $\mathbb{Q}$-rational points on $C_{P(T)}$, i.e., the set of all elements $[y : t : z] \in \mathbb{P}_{N/n,1,1}(\overline{\mathbb{Q}})$ such that $(y, t, z) \in \mathbb{Q}^3 \setminus \{(0, 0, 0)\}$ and $y^n = P(t, z)$, is denoted by $C_{P(T)}(\mathbb{Q})$. A point $[y : t : z] \in C_{P(T)}(\mathbb{Q})$ is *trivial* if $y = 0$, and *non-trivial* otherwise. Equivalently, $[y : t : z] \in C_{P(T)}(\mathbb{Q})$ is trivial if $z \neq 0$ and $P(t/z) = 0$.

2.3.2. The case where n does not divide N. Now, we consider the case $r \geqslant 1$, which is in fact similar to the previous one. However, to avoid confusion, we state it in details.

Consider this equivalence relation on $\overline{\mathbb{Q}}^3 \setminus \{(0, 0, 0)\}$: $(y_1, t_1, z_1) \sim (y_2, t_2, z_2)$ if and only if $(y_2, t_2, z_2) = (\lambda^{(N+n-r)/n} y_1, \lambda t_1, \lambda z_1)$ for some $\lambda \in \overline{\mathbb{Q}} \setminus \{0\}$. The quotient space $(\overline{\mathbb{Q}}^3 \setminus \{(0, 0, 0)\})/\sim$ is a weighted projective space, denoted by $\mathbb{P}_{(N+n-r)/n,1,1}(\overline{\mathbb{Q}})$. Given

[5] Here and in § 2.3.2, say *hyperelliptic* if $n = 2$.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

$(y, t, z) \in \overline{\mathbb{Q}}^3 \setminus \{(0,0,0)\}$, the corresponding point in $\mathbb{P}_{(N+n-r)/n,1,1}(\overline{\mathbb{Q}})$ is denoted by $[y : t : z]$. Set

$$P(T, Z) = a_0 Z^{(q+1)n} + a_1 Z^{(q+1)n-1} T + \cdots + a_{N-1} Z^{n-r+1} T^{N-1} + a_N Z^{n-r} T^N.$$

The equation $Y^n = P(T, Z)$ in $\mathbb{P}_{(N+n-r)/n,1,1}(\overline{\mathbb{Q}})$ is *the superelliptic curve associated with* $P(T)$; we denote it by $C_{P(T)}$. The set of all $\mathbb{Q}$-rational points on $C_{P(T)}$, i.e., the set of all points $[y : t : z] \in \mathbb{P}_{(N+n-r)/n,1,1}(\overline{\mathbb{Q}})$ such that $(y, t, z) \in \mathbb{Q}^3 \setminus \{(0,0,0)\}$ and $y^n = P(t, z)$, is denoted by $C_{P(T)}(\mathbb{Q})$. A point $[y : t : z] \in C_{P(T)}(\mathbb{Q})$ is *trivial* if $y = 0$, and *non-trivial* otherwise. Equivalently, $[y : t : z] \in C_{P(T)}(\mathbb{Q})$ is trivial if either $z = 0$ (this point, which is $[0 : 1 : 0]$, is the point at ∞) or $z \neq 0$ and t/z is a root of $P(T)$.

2.3.3. Extra notation. We use the following notation:

(a) $\mathcal{N}_n(P(T))$: subset of $\mathcal{N}_n$ defined by the extra condition that the 'twisted' superelliptic curve $C_{d \cdot P(T)} : y^n = d \cdot P(t)$ has a non-trivial $\mathbb{Q}$-rational point;

(b) $\mathcal{N}_n(P(T), x) = \mathcal{N}_n(P(T)) \cap \mathcal{N}_n(x)$ $(x \geqslant 1)$.

2.4. On the quadratic case

The following elementary proposition, which gives an explicit description of the set of branch points and characterizes specializations of a given regular $\mathbb{Z}/2\mathbb{Z}$-extension of $\mathbb{Q}(T)$, will be needed in the sequel. See, e.g., [26, § 8] for a proof.

Proposition 2.3. *Let $N \geqslant 1$ be an integer and $P(T) \in \mathcal{P}(2, N)$. Denote the roots of $P(T)$ by $t_1, \ldots, t_N$ and the field $\mathbb{Q}(T)(\sqrt{P(T)})$ by E.*

(a) *The set of branch points of $E/\mathbb{Q}(T)$ is either the set $\{t_1, \ldots, t_N\}$ (if N is even) or the set $\{t_1, \ldots, t_N\} \cup \{\infty\}$ (if N is odd).*

(b) *Let d be in $\mathcal{N}_2$. Then the $\mathbb{Z}/2\mathbb{Z}$-extension $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is in $\mathrm{Sp}(E)$ if and only if the twisted hyperelliptic curve $C_{d \cdot P(T)} : y^2 = d \cdot P(t)$ has a non-trivial $\mathbb{Q}$-rational point.*

Given an indeterminate T, there is a natural bijection f between the set of all regular $\mathbb{Z}/2\mathbb{Z}$-extensions of $\mathbb{Q}(T)$ and the set of all separable polynomials $P(T) \in \mathbb{Z}[T]$ with squarefree content. Then define the *height* of a given regular $\mathbb{Z}/2\mathbb{Z}$-extension $E/\mathbb{Q}(T)$ as the height of the associated polynomial $P_E(T)$. Moreover, by Proposition 2.3(a), if r is a positive even integer, then $E/\mathbb{Q}(T)$ has r branch points if and only if $P_E(T)$ has degree r or $r - 1$.

Given positive integers r and H with r even, we use the following notation:

(a) $\mathcal{E}(r)$: set of all regular $\mathbb{Z}/2\mathbb{Z}$-extensions of $\mathbb{Q}(T)$ with r branch points;

(b) $\mathcal{E}(r, H)$: subset of $\mathcal{E}(r)$ defined by the extra condition that the height is at most H.

Proposition 2.4. *Given an even positive integer r, there exists a constant $\alpha(r) > 0$ such that*

$$|\mathcal{E}(r, H)| \sim |\mathcal{P}_2(2, r, H)| \sim \alpha(r) \cdot H^{r+1}, \quad H \to \infty, \tag{2.1}$$

$$\frac{|\mathcal{E}(r, H)| - |\mathcal{P}_2(2, r, H)|}{|\mathcal{E}(r, H)|} = O\left(\frac{1}{H}\right), \quad H \to \infty. \tag{2.2}$$

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Proof. Given $H \geqslant 1$, Proposition 2.3(a) shows that

$$|\mathcal{E}(r, H)| = |\mathcal{P}_2(2, r, H)| + |\mathcal{P}_2(2, r-1, H)| \tag{2.3}$$

By [34, Lemma 5.8], one has

$$|\mathcal{P}_2(2, r, H)| \sim \alpha(r) \cdot H^{r+1}, \quad H \to \infty, \tag{2.4}$$

for some positive constant $\alpha(r)$ and, clearly, one has

$$|\mathcal{P}_2(2, r-1, H)| = O(H^r), \quad H \to \infty. \tag{2.5}$$

It then remains to combine (2.3), (2.4), and (2.5) to get (2.1) and (2.1), as needed. □

3. Conditional results

This section is devoted to our conditional results which assert that the specialization set of a regular $\mathbb{Q}$-G-cover of $\mathbb{P}^1$ with sufficiently many branch points has density zero.

We need some notation, in addition to that from § 2. Let G be a non-trivial finite group and $f : X \to \mathbb{P}^1$ a regular $\mathbb{Q}$-G-cover. We denote the associated regular G-extension by $E/\mathbb{Q}(T)$. Let $S = \{t_1, \dots, t_r\} \subseteq \mathbb{P}^1(\overline{\mathbb{Q}})$ be a non-empty subset of the set of all branch points of f, closed under the action of $\mathrm{G}_{\mathbb{Q}}$. Denote the ramification index of t_i by e_i, $i = 1, \dots, r$, and set $e_0 = \min\{e_1, \dots, e_r\}$. Let q_0 be the smallest prime dividing one of the e_i's and p the smallest prime divisor of $|G|$.

3.1. A conditional upper bound

This more precise version of Theorem 1.2 gives an upper bound for $|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G, x)|$, provided r is large enough and the abc-conjecture holds:

Theorem 3.1. *Assume the abc-conjecture holds and*

$$r > 2 + \frac{2}{q_0 - 1}. \tag{3.1}$$

Then, for every $\epsilon > 0$ and every sufficiently large integer x, one has

$$|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G, x)| \leqslant x^{e+\epsilon},$$

where

$$e = 2 \cdot |G|^{-1} \cdot \left(1 - \frac{1}{e_0}\right)^{-1} \cdot \left(r - 2 - \frac{2}{q_0 - 1}\right)^{-1}. \tag{3.2}$$

Remark 3.2. (a) The set S, which is implicit in Theorem 3.1 as well as in the next result can most conveniently be chosen to be the set of all branch points of f. However, in some situations, proper subsets yield stronger conclusions, notably if there are many branch points with large ramification index. From the proof of Theorem 3.1 (see § 3.4), considering several subsets at the same time (with the corresponding notation for each subset) can sometimes yield even stronger results. We refrain from explicitly stating such a version of Theorem 3.1, to avoid unnecessarily complicated notation.
(b) Condition (3.1) holds if and only if one of these conditions is satisfied:

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

(1) $r \geqslant 5$;

(2) $r \geqslant 4$ and $q_0 \geqslant 3$;

(3) $r \geqslant 3$ and $q_0 \geqslant 5$.

3.2. Explicit examples

We now explain how deriving several explicit results with the conclusion that the set $\mathrm{Sp}(f)$ has density zero.

First, we combine the lower bound given by the Malle conjecture and the upper bound from Theorem 3.1 to obtain the following more precise version of Theorem 1.3:

Corollary 3.3. *Assume the lower bound (1.2) is fulfilled for the group G, the abc-conjecture holds, and the following condition is satisfied:*

$$r > 2\left(\frac{q_0}{q_0-1} + \frac{(p-1)e_0}{p(e_0-1)}\right), \tag{3.3}$$

Then one has $e < \alpha(G)$, where e and $\alpha(G)$ are defined in (3.2) and (1.3), respectively, and, for every $\epsilon > 0$ and every sufficiently large x, one has

$$\frac{|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G,x)|}{|\overline{\mathcal{S}}(G,x)|} = O(x^{e-\alpha(G)+\epsilon}). \tag{3.4}$$

In particular, the set $\mathrm{Sp}(f)$ has density 0.

Proof. First, note that (3.3) $\Rightarrow$ (3.1) as

$$2\left(\frac{q_0}{q_0-1} + \frac{(p-1)e_0}{p(e_0-1)}\right) > \frac{2q_0}{q_0-1} = 2 + \frac{2}{q_0-1}.$$

Then, by Theorem 3.1 and since (1.2) has been assumed to hold, (3.4) holds. To complete the proof, it suffices to check $e < \alpha(G)$. Clearly, this holds if and only if (3.3) is satisfied. □

Remark 3.4. Making use of the inequalities $2 \leqslant p \leqslant q_0 \leqslant e_0$, one sees that (3.3) holds as soon as one of the following conditions is satisfied:

(a) $r \geqslant 7$;

(b) $r = 6$ and $e_0 \geqslant 3$;

(c) $r = 5$, $q_0 \geqslant 3$, and $(e_0, q_0, p) \neq (3,3,3)$;

(d) $r = 4$ and $q_0 > 2p$.

Conversely, since the right-hand side of (3.3) is bounded from below by 3, Corollary 3.3 in its present form cannot yield conclusions about covers with 3 branch points.

Moreover, by the Riemann–Hurwitz formula, the cover f has at least 7 branch points, provided X is of genus at least $2|G|-1$. Consequently, we have this conditional statement:

The specialization set of a given regular $\mathbb{Q}$-G-cover of $\mathbb{P}^1$ of genus at least $2|G|-1$ is of density 0, under the abc-conjecture and the lower bound (1.2).

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

In Corollary 3.5, we give several explicit situations where the conclusion of Corollary 3.3 holds, independently of the ramification data of f:

Corollary 3.5. *Suppose the abc-conjecture holds and one of these conditions is satisfied:*

(a) *G has rank at least 6 and (1.2) holds for the group G;*

(b) *G has a cyclic quotient of order $\notin \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$ and G fulfills (1.2);*

(c) *G is nilpotent of order divisible by a prime number $\geqslant 7$.*

Then the density of $\mathrm{Sp}(f)$ *is 0.*

Proof. First, assume G has rank $\geqslant 6$ and (1.2) holds. Then, by the first condition and the *Riemann existence theorem*, f has at least 7 branch points. Applying Corollary 3.3 and Remark 3.4 (with S the set of all branch points of f) provides the desired conclusion.

Now, assume G has a cyclic quotient of order $\notin \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$ and G fulfills (1.2). We shall make use of the following easy claim:

Let n be a positive integer $\notin \{1, 2, 3, 4, 5, 6, 8, 10, 12\}$. Then every regular $\mathbb{Q}$-$\mathbb{Z}/n\mathbb{Z}$-cover of $\mathbb{P}^1$ has either at least 8 branch points or at least 6 branch points of ramification index $\geqslant 3$.

Under the claim, we may apply Corollary 3.3 and Remark 3.4 to get the desired conclusion.

We now prove the claim. If p_0 is a prime number and $m \geqslant 1$, recall that, as a classical consequence of the *Branch Cycle lemma* (see [19] and [41, Lemma 2.8]), every regular $\mathbb{Q}$-$\mathbb{Z}/p_0^m\mathbb{Z}$-cover of $\mathbb{P}^1$ has at least $p_0^m - p_0^{m-1}$ branch points of ramification index p_0^m.[6] Consequently, the claim already holds if n is divisible by 16, 9, 25 or a prime number $p_0 \geqslant 7$. For the case $n = 15$, let g be a regular $\mathbb{Q}$-$\mathbb{Z}/15\mathbb{Z}$-cover of $\mathbb{P}^1$. Then either g has no branch point of ramification index 15, in which case g has at least 6 branch points of ramification index $\geqslant 3$ (at least 2 coming from the subcover of degree 3 and at least 4 from that of degree 5), or g has at least one branch point of ramification index 15, in which case g has in fact at least 8 such branch points by the Branch Cycle Lemma. In particular, the claim holds if n is divisible by 15. As to the remaining cases $n = 20, 24, 40$, one treats them as the case $n = 15$.

Finally, (c) is a special case of (b). Indeed, if G is nilpotent of order divisible by a prime q, then G has a (cyclic) quotient group of order q, and G fulfills (1.2) by [30]. □

Remark 3.6. (a) More explicit examples derived from (b) could be given in (c). For example, the density zero conclusion also holds if G is nilpotent of order divisible by 15. We refrain from considering more applications of this kind, to avoid complicated case distinctions.

(b) By Corollary 3.5(c), if $q \geqslant 7$ is a prime number, then no regular $\mathbb{Z}/q\mathbb{Z}$-extension of $\mathbb{Q}(T)$ is parametric, under the abc-conjecture. The interest of this remark is that none of the methods from [26] and [27, § 7] applies to finite groups of prime order.

[6] Indeed, at least one such branch point must exist since the inertia groups at branch points generate $\mathbb{Z}/p_0^m\mathbb{Z}$. By the Branch Cycle Lemma, we obtain at least $\varphi(p_0^m) = p_0^m - p_0^{m-1}$ such branch points, where φ denotes the Euler totient function. See, e.g., [12, Proposition 3.1.19] for more details.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

More generally, by the above, no regular G-extension of $\mathbb{Q}(T)$ with $r \geqslant 7$ branch points is parametric, under the abc-conjecture and, possibly, the lower bound (1.2). In Appendix A, we discuss the situation where r is 2 or 3. The case $r \in \{4, 5, 6\}$ remains open in general.

3.3. Variants

We provide below two variants of Corollary 3.3.

The first one asserts that one can remove the assumption that the lower bound (1.2) holds, at the cost of making (3.3) less explicit:

Theorem 3.7. *There exists a positive constant $r_0(G)$ such that if $r \geqslant r_0(G)$ and if the abc-conjecture holds, then the set $\mathrm{Sp}(f)$ has density 0.*

Proof. Without loss, we may assume G is a regular Galois group over $\mathbb{Q}$.[7] Then, by [13, Theorem 1.1], there exists a positive constant $\beta(G)$ such that the following holds for every sufficiently large x (up to an explicit multiplicative constant depending on G):

$$x^{\beta(G)} \leqslant |\overline{\mathcal{S}}(G, x)|.$$

Hence, by Theorem 3.1 and Remark 3.2(b), if $r \geqslant 5$, it suffices to check $e < \beta(G)$ (with e as in (3.2)), which can be guaranteed if r is sufficiently large (depending on G). □

Remark 3.8. In fact, [13, Theorem 1.1 and § 4.1] provides the following:

Let $f_1 : X_1 \to \mathbb{P}^1$ be a regular $\mathbb{Q}$-G-cover with r_1 branch points. Then, for all sufficiently large x, one has $x^{a(G)/r_1} \leqslant |\mathrm{Sp}(f_1) \cap \overline{\mathcal{S}}(G, x)|$, where $a(G)$ may be chosen as $(|G| - 1) \cdot |G|^{-1} \cdot (3|G|^4 \log(|G|))^{-1}$.

Combination with our Theorem 3.1 then gives

$$x^{a(G)/r} \leqslant |\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G, x)| \leqslant x^{b(G)/r},$$

where $b(G) > a(G)$ is an explicit positive constant depending only on G, under the abc-conjecture. In particular, if $f_2 : X_2 \to \mathbb{P}^1$ is another regular $\mathbb{Q}$-G-cover with $r_2 > (b(G)/a(G)) \cdot r_1$ branch points, then this inequality holds for every sufficiently large x, under the abc-conjecture:

$$|\mathrm{Sp}(f_2) \cap \overline{\mathcal{S}}(G, x)| < |\mathrm{Sp}(f_1) \cap \overline{\mathcal{S}}(G, x)|.$$

As a consequence, the constant $r_0(G)$ in Theorem 3.7 can be made explicit. Namely, if G is not a regular Galois group over $\mathbb{Q}$, one can arbitrarily take $r_0(G) = 1$. Otherwise, take any $r_0(G) > (b(G)/a(G)) \cdot r_1(G)$, where $r_1(G)$ is the smallest number of branch points of a regular $\mathbb{Q}$-G-cover of $\mathbb{P}^1$.

For our second variant, we need to recall beforehand the statements of the uniformity conjecture and the upper bound from the Malle conjecture.

[7] The definition of a regular Galois group over $\mathbb{Q}$ is recalled in § 1.2.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

The uniformity conjecture. *Let $g \geqslant 2$ be an integer. Then there exists a positive integer B, depending only on g, such that the set of all $\mathbb{Q}$-rational points on any given smooth curve defined over $\mathbb{Q}$ with genus g has cardinality at most B.*

The Malle conjecture (upper bound). *For every $\epsilon > 0$, one has*

$$|\mathcal{S}(G, x)| \leqslant c_2(G, \epsilon) \cdot x^{\alpha(G)+\epsilon} \tag{3.5}$$

for some constant $c_2(G, \epsilon) > 0$ and every sufficiently large x, where $\alpha(G)$ is defined in (1.3).

Theorem 3.9. *Suppose the uniformity conjecture holds and G has a normal subgroup H such that the following three conditions are satisfied:*

(a) *for every regular $\mathbb{Q}$-G/H-cover $X \to \mathbb{P}^1$, the genus of X is at least 2;*

(b) *p does not divide the order of G/H;*

(c) *(1.2) and (3.5) hold for the groups G and G/H, respectively.*

Then the set $\mathrm{Sp}(f)$ has density 0.

Remark 3.10. (a) By [7, Theorem 1.1], the uniformity conjecture holds under the Lang conjecture, which asserts that the set of all $\mathbb{Q}$-rational points on any variety of general type defined over $\mathbb{Q}$ is not Zariski dense.

(b) By [26, Proposition 7.3], Condition (a) of Theorem 3.9 holds if G/H is neither solvable of even order nor of order 3.

Proof. As noted in § 2.2.1, it suffices to show that the set $\mathrm{Sp}(E)$ has density zero.

Let $E_1/\mathbb{Q}(T), \dots, E_s/\mathbb{Q}(T)$ be the subextensions of $E/\mathbb{Q}(T)$ of group G/H. For $i \in \{1, \dots, s\}$, let g_i be the genus of X_i, where $X_i \to \mathbb{P}^1$ is the regular $\mathbb{Q}$-G/H-cover associated with $E_i/\mathbb{Q}(T)$. Also, let q be the smallest prime divisor of the order of G/H. One then has

$$\alpha(G/H) = \frac{|G|^{-1}}{|H|^{-1}}\left(1 - \frac{1}{q}\right)^{-1}.$$

Let $F/\mathbb{Q}$ be a G-extension in $\mathrm{Sp}(E)$ and $t_0 \in \mathbb{P}^1(\mathbb{Q})$ such that $F = E_{t_0}$. By [26, Lemma 3.2], $(E_1)_{t_0}/\mathbb{Q}, \dots, (E_s)_{t_0}/\mathbb{Q}$ are the distinct subextensions of $E_{t_0}/\mathbb{Q}$ with Galois group G/H. Hence, there exists $i \in \{1, \dots, s\}$ such that $F^H/\mathbb{Q}$ is the specialization of $E_i/\mathbb{Q}(T)$ at t_0. Let $g_0 = \max(g_1, \dots, g_s)$. By (a) and as the uniformity conjecture holds, one may apply [26, Proposition 2.5] to get that there exists a positive constant $B = B(|G/H|, g_0)$ such that, for each $i \in \{1, \dots, s\}$, there exist at most B points $t_0 \in \mathbb{P}^1(k)$ with $F^H/\mathbb{Q} = (E_i)_{t_0}/\mathbb{Q}$. Moreover, if d_F and d_{F^H} denote the absolute discriminants of the number fields F and F^H, respectively, then one has $|d_{F^H}| \leqslant |d_F|^{1/|H|}$. Conclude that this inequality holds for every positive integer x:

$$|\mathrm{Sp}(E) \cap \mathcal{S}(G, x)| \leqslant Bs \cdot |\mathcal{S}(G/H, x^{1/|H|})|. \tag{3.6}$$

By (b), one has $p < q$, that is, $(1/|H|) \cdot \alpha(G/H) < \alpha(G)$. Let $\epsilon > 0$ be such that

$$\alpha(G/H) + \epsilon < \alpha(G) \cdot |H|. \tag{3.7}$$

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Combining (3.6) and the assumption that (3.5) holds for the group G/H then provides

$$|\mathrm{Sp}(E) \cap \mathcal{S}(G, x)| \leqslant Bs \cdot c_2(G/H, \epsilon) \cdot x^{(\alpha(G/H)+\epsilon)/|H|} \tag{3.8}$$

for some positive constant $c_2(G/H, \epsilon)$ and every $x \geqslant x(G/H, \epsilon)$. On the other hand, since (1.2) has been assumed to hold for the group G, one has

$$|\mathcal{S}(G, x)| \geqslant c_1(G) \cdot x^{\alpha(G)} \tag{3.9}$$

for some positive constant $c_1(G)$ and every $x \geqslant x(G, \epsilon)$. Combine (3.8) and (3.9) to get

$$\frac{|\mathrm{Sp}(E) \cap \mathcal{S}(G, x)|}{|\mathcal{S}(G, x)|} = O(x^{(\alpha(G/H)+\epsilon)/|H|-\alpha(G)}), \quad x \to \infty. \tag{3.10}$$

It then remains to combine (3.7) and (3.10) to conclude that the set $\mathrm{Sp}(E)$ has density 0. □

Corollary 3.11. *Suppose the uniformity conjecture holds, the group G is nilpotent, and one of the following two conditions is satisfied:*

(a) *G is of even order but $|G| \notin \{2^a 3^b : a \geqslant 1,\ b \in \{0, 1\}\}$;*

(b) *G is of odd order and $|G|$ has at least two distinct prime factors.*

Then the set $\mathrm{Sp}(f)$ has density 0.

For example, Corollary 3.11 applies to the groups $\mathbb{Z}/10\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Note that these groups have covers with four branch points and our results under the abc-conjecture cannot (*a priori*) apply to them.

Proof. As the group G is nilpotent, [30] may be used to show that the entire Malle conjecture holds for every quotient of G. By Theorem 3.9, it then suffices to find a quotient of G for which Conditions (a) and (b) of that theorem hold.

Set $G = P_1 \times \cdots \times P_s$ where $s \geqslant 1$ and P_i is a non-trivial p_i-group for each $i \in \{1, \ldots, s\}$. We assume $p_1 \leqslant \cdots \leqslant p_s$ and $|P_i| \leqslant |P_j|$ if $p_i = p_j$ $(i, j \in \{1, \ldots, s\})$. If (a) holds, then $p_s \geqslant 5$ or ($p_s = 3$ and $|P_s| \geqslant 9$) or ($p_s = 3$ and $P_s \times P_{s-1} \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$). Then either $G/(P_1 \times \cdots \times P_{s-1})$ (in the first two cases) or $G/(P_1 \times \cdots \times P_{s-2})$ (in the third case) has odd order and it is not $\mathbb{Z}/3\mathbb{Z}$. In particular, Conditions (a) and (b) of Theorem 3.9 are fulfilled (see Remark 3.10(b)). If (b) holds, then $p_1 < p_s$ and $p_s \geqslant 5$, and one concludes as in (a). □

3.4. Proof of Theorem 3.1

The proof relies on this consequence of the abc-conjecture, due to Elkies, Langevin, and Granville (see, e.g., [23, Theorem 5]):

Theorem 3.12. *Let $P(U, V) \in \mathbb{Z}[U, V]$ be a homogeneous polynomial of degree d without any repeated factors. Assume the abc-conjecture holds. Then, for every $\epsilon > 0$ and every couple (u, v) of coprime integers, one has*

$$\mathrm{rad}(P(u, v)) \geqslant c_1 \cdot \max\{|u|, |v|\}^{d-2-\epsilon},$$

where c_1 is a positive constant depending only on P and ϵ.

We break the proof of Theorem 3.1 into three parts.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

3.4.1. Controlling the ramification of specializations of f. The first part requires associating a homogeneous polynomial controlling the ramification behavior in specializations of f, which is done via Theorem 2.2.

For each $i \in \{1, \dots, r\}$, let $P_i(U, V) \in \mathbb{Z}[U, V]$ be the minimal polynomial of the branch point t_i. Set

$$P(U, V) = \prod_{i \in I} P_i(U, V),$$

where the t_i's, $i \in I$, build a set of representatives of $t_1, \dots, t_r$ modulo the action of $\mathrm{G}_{\mathbb{Q}}$. Moreover, set $a_i = |G|(1 - 1/e_i)$, where e_i is as before the ramification index of t_i, for each $i \in I$ (so a_i is the index of an inertia group generator at t_i, viewed as a permutation in the regular permutation action of G).[8] For $t_0 \in \mathbb{Q}$, set $t_0 = u/v$, with u and v coprime integers, and denote the absolute discriminant of E_{t_0} by d_{t_0}.

Let ℓ be a prime number, not contained in the finite exceptional set $\mathcal{S}_{\mathrm{exc}}$ from Theorem 2.2. By that theorem, ℓ is (tamely) ramified in $E_{t_0}/\mathbb{Q}$ with ramification index e_i if ℓ divides $P_i(u, v)$ with positive multiplicity at most $q_i - 1$, where q_i is the smallest prime divisor of e_i. In that case, the exponent of ℓ in d_{t_0} equals a_i. Therefore, we get the following lower bound:

$$|d_{t_0}| \geqslant \prod_{i \in I} \prod_{\ell} \ell^{|G|(1-1/e_i)},$$

where, given $i \in I$, the second product is over all prime numbers ℓ which are not in $\mathcal{S}_{\mathrm{exc}}$ and which divide $P_i(u, v)$ with positive multiplicity at most $q_i - 1$. As the finitely many elements of the set $\mathcal{S}_{\mathrm{exc}}$, as well as the numbers q_i, $i \in I$, are fixed and depend only on f, we have

$$|d_{t_0}| \geqslant c_0 \cdot \prod_{i \in I} \prod_{\ell} \ell^{|G|(1-1/e_i)}, \tag{3.11}$$

for some positive constant c_0 depending only on f, and where, given $i \in I$, the second product is over *all* prime numbers ℓ which divide $P_i(u, v)$ with positive multiplicity at most $q_i - 1$. Combining (3.11) and the definitions of e_0 and q_0 (see the beginning of § 3) yields the following lower bound:

$$|d_{t_0}| \geqslant c_0 \cdot \prod_{\ell} \ell^{|G|(1-1/e_0)}, \tag{3.12}$$

where the product is over all primes dividing $P(u, v)$ with positive multiplicity at most $q_0 - 1$.

3.4.2. Applying Theorem 3.12. The second part consists in estimating the product of all prime numbers dividing a given value of $P(U, V)$ with positive multiplicity at most $q_0 - 1$.

Let u, v be coprime integers and set $n = \max\{|u|, |v|\}$. Given $\epsilon > 0$, since the abc-conjecture has been assumed to hold, we may apply Theorem 3.12 to get this lower bound:

$$\mathrm{rad}(P(u, v)) \geqslant c_1 \cdot n^{\deg(P)-2-\epsilon} = c_1 \cdot n^{r-2-\epsilon}, \tag{3.13}$$

[8] Recall that the *index* of a permutation $\sigma \in S_d$ is defined as d minus the number of orbits of $\langle \sigma \rangle$.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

where c_1 depends only on $P(U, V)$ and ϵ. For $m \geqslant 1$, let B_m be the product of all prime numbers dividing $P(u, v)$ exactly m times. Setting $t_0 = u/v$, (3.12) can be rewritten as

$$|d_{t_0}| \geqslant c_0 \cdot \left(\prod_{m=1}^{q_0-1} B_m \right)^{|G|(1-1/e_0)}. \tag{3.14}$$

Now, let $B_{\geqslant q_0}$ be the product of all B_m's with $m \geqslant q_0$. Since $\mathrm{rad}(P(u, v))$ is the product of all B_m's with $m \geqslant 1$, one has

$$\mathrm{rad}(P(u, v)) \leqslant \frac{|P(u, v)|}{\prod_{m=q_0}^{\infty} B_m^{m-1}} \leqslant \frac{|P(u, v)|}{B_{\geqslant q_0}^{q_0-1}}. \tag{3.15}$$

As $|P(u, v)| \leqslant c_2 \cdot n^r$, with $c_2 = c_2(P)$, the combination of (3.13) and (3.15) then yields

$$\frac{c_2 \cdot n^r}{B_{\geqslant q_0}^{q_0-1}} \geqslant c_1 \cdot n^{r-2-\epsilon},$$

that is,

$$B_{\geqslant q_0} \leqslant c_3 \cdot n^{(2+\epsilon)/(q_0-1)} \tag{3.16}$$

for some positive constant c_3 depending only on f and ϵ. Combining (3.13), (3.14), and (3.16) then provides the following bound (up to replacing ϵ by $\epsilon|G|^{-1}(1-1/e_0)^{-1}(q_0-1)/q_0$):

$$|d_{t_0}| \geqslant c_0 \cdot \left(\frac{\mathrm{rad}(P(u, v))}{B_{\geqslant q_0}} \right)^{|G|(1-1/e_0)} \geqslant c_4 \cdot n^{|G|(1-1/e_0)(r-2-2/(q_0-1))-\epsilon}, \tag{3.17}$$

where c_4 is some positive constant depending only on f and ϵ.

3.4.3. Conclusion. Finally, we use the estimate (3.17) to bound $|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G, x)|$ from above.

Let δ be any real number such that

$$\delta > \frac{r}{r-2-2/(q_0-1)}.$$

By (3.1), δ is well defined and positive. Let ϵ be a positive real number. By (3.17), for every couple (u, v) of coprime integers, one has

$$|d_{u/v}| \geqslant c_4 \cdot \max\{|u|, |v|\}^{r \cdot |G|(1-1/e_0) \cdot \delta^{-1} - \epsilon}. \tag{3.18}$$

Let n be a sufficiently large integer (depending on ϵ). The lower bound (3.18) then allows to conclude that all specializations $E_{t_0}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ with $t_0 \in \mathbb{Q}$ and such that

$$|d_{t_0}| \leqslant n^{r \cdot |G|(1-1/e_0) \cdot \delta^{-1}}$$

must come from values $t_0 = u/v$ with $\max\{|u|, |v|\} \leqslant n$. Setting $x = n^{r \cdot |G|(1-1/e_0) \cdot \delta^{-1}}$, we find that all specializations $E_{t_0}/\mathbb{Q}$ of $E/\mathbb{Q}(T)$ with $t_0 \in \mathbb{Q}$ and such that $|d_{t_0}| \leqslant x$ must come from values $t_0 = u/v$ with

$$\max\{|u|, |v|\} \leqslant x^{\delta \cdot (r|G|(1-1/e_0))^{-1}}.$$

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

In particular, choosing

$$\delta = \frac{r}{r-2-2/(q_0-1)} + \frac{\epsilon}{2} \cdot r \cdot |G| \cdot \left(1 - \frac{1}{e_0}\right)$$

and using the definition of our exponent e given in (3.2), we obtain

$$\max\{|u|, |v|\} \leqslant x^{(e+\epsilon)/2}.$$

As there are at most $4 \cdot x^{e+\epsilon}$ such pairs of integers (u, v), this concludes the proof.

4. Unconditional results

The aim of this section is to show unconditionally that the set of specializations of almost all regular $\mathbb{Q}$-G-covers of $\mathbb{P}^1$, where $G = \mathbb{Z}/2\mathbb{Z}$ or S_3, has density zero.

4.1. The quadratic case

We start with the case $G = \mathbb{Z}/2\mathbb{Z}$ and, for simplicity, use the function field extension language, which is strictly identical to the cover point of view.

4.1.1. Main result. The following statement is a more precise version of Theorem 1.4 from the introduction. Note that the unconditional upper bound in (b) is expectedly weaker than the one provided by Theorem 3.1 under the abc-conjecture. Recall that the sets $\mathcal{E}(r)$ and $\mathcal{E}(r, H)$, which occur in the statement below, are defined in § 2.4.

Theorem 4.1. *Let r be an even positive integer. Then there exists a subset S of $\mathcal{E}(r)$ which satisfies the following two conclusions.*

(a) *One has*

$$\frac{|S \cap \mathcal{E}(r, H)|}{|\mathcal{E}(r, H)|} = 1 - O\left(\frac{\log(H)}{\sqrt{H}}\right), \quad H \to \infty.$$

In particular, the set S has density 1.

(b) *For every extension $E/\mathbb{Q}(T)$ in S, there exists a positive constant $\alpha < 1$ such that*

$$|\mathrm{Sp}(E) \cap \mathcal{S}(\mathbb{Z}/2\mathbb{Z}, x)| = O(x \cdot \log^{-\alpha}(x)), \quad x \to \infty.$$

In particular, the set of specializations of every extension of $\mathbb{Q}(T)$ in S has density 0.

4.1.2. Proof of Theorem 4.1. Our main tool is the case $n = 2$ of the following diophantine result, which has its own interest and which shows that almost all twists of almost all superelliptic curves over $\mathbb{Q}$ have only trivial $\mathbb{Q}$-rational points, under a suitable assumption on the degree. Recall that the sets $\mathcal{P}(n, N)$ and $\mathcal{P}(n, N, H)$, and the sets $\mathcal{N}_n(P(T))$ and $\mathcal{N}_n(P(T), x)$, which occur in the statement below, are defined in § 2.1 and § 2.3.3, respectively.

Theorem 4.2. *Given two positive integers n and N such that $2 \leqslant n$ and n divides N, there exists a subset S' of $\mathcal{P}(n, N)$ such that the following two conclusions are satisfied.*

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

(a) *One has*

$$\frac{|S' \cap \mathcal{P}(n, N, H)|}{|\mathcal{P}(n, N, H)|} = 1 - O\left(\frac{\log(H)}{\sqrt{H}}\right), \quad H \to \infty. \tag{4.1}$$

In particular, the set S' has density 1.

(b) *For each $P(T) \in S'$, there exists a positive constant $\alpha < 1$ such that*

$$|\mathcal{N}_n(P(T), x)| = O(x \cdot \log^{-\alpha}(x)), \quad x \to \infty. \tag{4.2}$$

In particular, for each $P(T) \in S'$, the density of the subset $\mathcal{N}_n(P(T))$ of $\mathcal{N}_n$ is 0.

Proof of Theorem 4.1 under Theorem 4.2. Let S' be a subset of $\mathcal{P}(2, r)$ as in Theorem 4.2 and $\overline{S'} = \mathcal{P}(2, r) \setminus S'$. Let S be the subset of $\mathcal{E}(r)$ consisting of all regular $\mathbb{Z}/2\mathbb{Z}$-extensions of $\mathbb{Q}(T)$ with r branch points and whose associated polynomial lies in the set $S' \cap \mathcal{P}_2(2, r)$.[9]

First, we prove (a). For every positive integer H, one has

$$\begin{aligned}
1 - \frac{|S \cap \mathcal{E}(r, H)|}{|\mathcal{E}(r, H)|} &= 1 - \frac{|S' \cap \mathcal{P}_2(2, r, H)|}{|\mathcal{E}(r, H)|} \\
&= 1 - \frac{|\mathcal{P}_2(2, r, H)|}{|\mathcal{E}(r, H)|} + \frac{|\overline{S'} \cap \mathcal{P}_2(2, r, H)|}{|\mathcal{E}(r, H)|} \\
&\leqslant 1 - \frac{|\mathcal{P}_2(2, r, H)|}{|\mathcal{E}(r, H)|} + \frac{|\overline{S'} \cap \mathcal{P}(2, r, H)|}{|\mathcal{E}(r, H)|} \\
&= 1 - \frac{|\mathcal{P}_2(2, r, H)|}{|\mathcal{E}(r, H)|} + \frac{|\mathcal{P}(2, r, H)|}{|\mathcal{E}(r, H)|} - \frac{|S' \cap \mathcal{P}(2, r, H)|}{|\mathcal{E}(r, H)|} \\
&= 1 - \frac{|\mathcal{P}_2(2, r, H)|}{|\mathcal{E}(r, H)|} + \frac{|\mathcal{P}(2, r, H)| - |S' \cap \mathcal{P}(2, r, H)|}{|\mathcal{P}(2, r, H)|} \cdot \frac{|\mathcal{P}(2, r, H)|}{|\mathcal{E}(r, H)|}.
\end{aligned}$$

By Theorem 4.2(a), one has

$$\frac{|\mathcal{P}(2, r, H)| - |S' \cap \mathcal{P}(2, r, H)|}{|\mathcal{P}(2, r, H)|} = O\left(\frac{\log(H)}{\sqrt{H}}\right), \quad H \to \infty.$$

Moreover, by Proposition 2.4 and as $|\mathcal{P}(2, r, H)| \sim 2^{r+1} \cdot H^{r+1}$ as H tends to ∞, one has

$$1 - \frac{|\mathcal{P}_2(2, r, H)|}{|\mathcal{E}(r, H)|} = O\left(\frac{1}{H}\right) \quad \text{and} \quad \frac{|\mathcal{P}(2, r, H)|}{|\mathcal{E}(r, H)|} = O(1)$$

as H tends to ∞. Hence, one has

$$1 - \frac{|S \cap \mathcal{E}(r, H)|}{|\mathcal{E}(r, H)|} = O\left(\frac{1}{H}\right) + O\left(\frac{\log(H)}{\sqrt{H}}\right) \cdot O(1) = O\left(\frac{\log(H)}{\sqrt{H}}\right), \quad H \to \infty.$$

Now, we prove (b). Given $E/\mathbb{Q}(T) \in S$, there is a unique polynomial $P_E(T)$ in S' with

$$E = \mathbb{Q}(T)(\sqrt{P_E(T)}).$$

[9] The set $\mathcal{P}_2(2, r)$ is defined in § 2.1.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

By Theorem 4.2(b), there is a constant $\alpha \in]0,1[$ with

$$|\mathcal{N}_2(P_E(T),x)| = O(x\cdot\log^{-\alpha}(x))$$

as x tends to ∞. By applying Proposition 2.3(b), we get that $|\mathcal{N}_2(P_E(T),x)|$ is the cardinality of the subset of $\mathcal{N}_2(x)$ (see § 2.1) defined by the extra condition that $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is in $\mathrm{Sp}(E)$. As the absolute discriminant of the number field $\mathbb{Q}(\sqrt{d})$ is d or $4d$ ($d \in \mathcal{N}_2$), we get

$$|\mathrm{Sp}(E)\cap\mathcal{S}(\mathbb{Z}/2\mathbb{Z},x)| \leqslant |\mathcal{N}_2(P_E(T),x)| = O(x\cdot\log^{-\alpha}(x))$$

as x tends to ∞. It then remains to use that

$$|\mathcal{S}(\mathbb{Z}/2\mathbb{Z},x)| \geqslant |\mathcal{N}_2(x/4)| \sim \frac{x}{4\cdot\zeta(2)}$$

as x tends to ∞ to get the desired density zero conclusion. □

Comments on proof of Theorem 4.2. The proof is similar to the arguments given in [34, § 3.2 and § 4.2], which yield Theorem 4.2 with the weaker conclusion that almost all superelliptic curves over $\mathbb{Q}$ have at least one twist with only trivial $\mathbb{Q}$-rational points. For the convenience of the reader, we offer in Appendix B.1 a full proof of Theorem 4.2 with the necessary adjustments to get the desired stronger conclusion. □

In Appendix B.2, we give two variants of Theorem 4.2 where we relax the assumption that n divides N, at the cost of making the conclusion in (b) weaker.

4.2. Symmetric groups

The aim of this subsection is to give evidence that, given $n \geqslant 2$, almost all regular $\mathbb{Q}$-S_n-covers of $\mathbb{P}^1$ have a specialization set of density 0, thus generalizing the conclusion of Theorem 4.1. We count those covers via degree n polynomials with Galois group S_n over $\mathbb{Q}(T)$. For $n = 3$, we obtain an unconditional result, given in Theorem 4.7.

4.2.1. Preliminaries. First, we explain our way of counting covers via polynomials. Given $n \geqslant 2$, if $E/\mathbb{Q}(T)$ denotes the function field extension associated with a regular $\mathbb{Q}$-S_n-cover of $\mathbb{P}^1$, then E is the splitting field over $\mathbb{Q}(T)$ of a degree n polynomial

$$Y^n + a_{n-1}(T)Y^{n-1} + \cdots + a_1(T)Y + a_0(T),$$

with $a_0(T),\dots,a_{n-1}(T) \in \mathbb{Z}[T]$. A natural way of counting covers is then to count the corresponding polynomials up to a bounded T-degree and bounded height.

Given $n \geqslant 2$ and $D \geqslant 1$, we therefore consider the set $\mathcal{Q}(n,D)$ of all polynomials $P(T,Y) \in \mathbb{Z}[T][Y]$ which are monic and of degree n in Y, and which are also of degree at most D in T. Given $i \in \{0,\dots,n-1\}$ and $j \in \{0,\dots,D\}$, let $a_{i,j} \in \mathbb{Z}$ denote the coefficient at T^j of $a_i(T)$. We then count covers by fixing an integer $H \geqslant 1$ and considering the set

$$\mathcal{Q}(n,D,H) = \{P(T,Y) \in \mathcal{Q}(n,D) : |a_{i,j}| \leqslant H \text{ for all } i,j\}.$$

4.2.2. Main result. Our eventual goal is to prove Theorem 4.7, which is a statement about Galois covers with group S_3. Since most of the ingredients in the proof are not specific to the case $n = 3$, we try to retain generality as long as possible.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Lemma 4.3. *Given $n \geqslant 2$ and $D \geqslant 1$, let $U_{n-1,D}, \dots, U_{n-1,0}, \dots, U_{1,D}, \dots, U_{1,0}, U_{0,D}, \dots, U_{0,0}$ be algebraically independent indeterminates, and denote by $\underline{U}$ the vector consisting of these variables. Let $\Delta(T) \in \mathbb{Q}[\underline{U}][T]$ be the discriminant (with respect to Y) of the polynomial*

$$F(\underline{U}, T, Y) = Y^n + \left(\sum_{j=0}^{D} U_{n-1,j} T^j\right) Y^{n-1} + \cdots + \left(\sum_{j=0}^{D} U_{1,j} T^j\right) Y + \sum_{j=0}^{D} U_{0,j} T^j.$$

Then $\Delta(T)$ is irreducible over $\mathbb{Q}(\underline{U})$.

Proof. It is well known that the discriminant of the polynomial

$$Y^n + U_{n-1,0} Y^{n-1} + \cdots + U_{1,0} Y + U_{0,0}$$

is irreducible as an element of $\mathbb{Q}[U_{0,0}, U_{1,0}, \dots, U_{n-1,0}]$ (see, e.g., [21, page 15]). The polynomial $F(\underline{U}, T, Y)$ arises from this polynomial after applying the map sending $U_{i,0}$ to

$$U_{i,0} + (U_{i,1} T + U_{i,2} T^2 + \cdots + U_{i,D} T^D)$$

for each $i \in \{0, \dots, n-1\}$ and fixing all other indeterminates. Since this corresponds to an automorphism of the ring $\mathbb{Q}[\underline{U}, T, Y]$, the discriminant $\Delta(T)$ must still be irreducible as an element of $\mathbb{Q}[\underline{U}, T]$, and hence also inside $\mathbb{Q}(\underline{U})[T]$ by Gauss' lemma. □

Lemma 4.4. *Given $n \geqslant 2$ and $D \geqslant 1$, consider the set S consisting of all polynomials*

$$P(T, Y) = Y^n + a_{n-1}(T) Y^{n-1} + \cdots + a_1(T) Y + a_0(T)$$

in $\mathcal{Q}(n, D)$ fulfilling the following three conditions:

(a) *$P(T, Y)$ has Galois group S_n over $\mathbb{Q}(T)$;*

(b) *the discriminant $\Delta(T) \in \mathbb{Z}[T]$ of $P(T, Y)$ is irreducible;*

(c) *the polynomial*

$$a_{n-1,D} Y^{n-1} + a_{n-2,D} Y^{n-2} + \cdots + a_{0,D}$$

has degree $n-1$ and is irreducible over $\mathbb{Q}$, where $a_{i,D}$ denotes the coefficient of $a_i(T)$ at T^D for each $i \in \{0, \dots, n-1\}$.

Then one has

$$\frac{|S \cap \mathcal{Q}(n, D, H)|}{|\mathcal{Q}(n, D, H)|} = 1 - O\left(\frac{\log(H)}{\sqrt{H}}\right), \quad H \to \infty.$$

In particular, the set S has density 1.

Proof. We estimate the size of the complement $\mathcal{Q}(n, D) \setminus S$. Let $S_{(1)}$ (respectively, $S_{(2)}$, $S_{(3)}$) be the subset of $\mathcal{Q}(n, D)$ which consists of all polynomials $P(T, Y)$ which do not fulfill (a) (respectively, (b), (c)). It is enough to show that

$$\frac{|S_{(j)} \cap \mathcal{Q}(n, D, H)|}{|\mathcal{Q}(n, D, H)|} = O\left(\frac{\log(H)}{\sqrt{H}}\right), \quad H \to \infty, \tag{4.3}$$

for each $j \in \{1, 2, 3\}$. This is mainly obtained by making use of a sufficiently precise version of Hilbert's irreducibility theorem (namely, [9, Theorem 2.1]).

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Given algebraically independent indeterminates $T_0, \dots, T_{n-1}$, the polynomial

$$Y^n + T_{n-1}Y^{n-1} + \cdots + T_1 Y + T_0$$

has Galois group S_n over $\mathbb{Q}(T_0, T_1, \dots, T_{n-1})$. Apply [9, Theorem 2.1] to get that the number of tuples $(t_0, t_1, \dots, t_{n-1})$ of integers of absolute value at most H such that

$$Y^n + t_{n-1}Y^{n-1} + \cdots + t_1 Y + t_0$$

does not have Galois group S_n over $\mathbb{Q}$ is $O(H^{n-1/2} \cdot \log(H))$ as H tends to ∞. Combine this and the fact that if $P(T, Y)$ is such that $P(0, Y)$ has Galois group S_n over $\mathbb{Q}$, then $P(T, Y)$ has Galois group S_n over $\mathbb{Q}(T)$ to get that (4.3) holds for $j = 1$. In the same way, (4.3) also holds if $j = 2$ (use Lemma 4.3), and if $j = 3$. □

Lemma 4.5. *Let $n \geqslant 2$ and $D \geqslant 1$ be integers. Let S' be the subset of $\mathcal{Q}(n, D)$ which consists of all polynomials $P(T, Y)$ fulfilling the following two conditions:*

(a) *$P(T, Y)$ defines a regular $\mathbb{Q}$-S_n-cover $f : X \to \mathbb{P}^1$ of branch points $t_1, \dots, t_r$;*

(b) *$t_1, \dots, t_r$ are algebraically conjugate.*

Then one has

$$\frac{|S' \cap \mathcal{Q}(n, D, H)|}{|\mathcal{Q}(n, D, H)|} = 1 - O\left(\frac{\log(H)}{\sqrt{H}}\right), \quad H \to \infty.$$

In particular, the set S' has density 1.

Proof. It suffices to show that the set S provided by Lemma 4.4 is a subset of S'. Let $P(T, Y)$ be in S and $\Delta(T) \in \mathbb{Z}[T]$ its discriminant. By Condition (b) of Lemma 4.4, $\Delta(T)$ cannot be a square in $\overline{\mathbb{Q}}(T)$, i.e., the Galois group $\overline{G}$ of $P(T, Y)$ over $\overline{\mathbb{Q}}(T)$ is not contained in A_n. Since $\overline{G} \trianglelefteq S_n$ (by Condition (a) of Lemma 4.4), we can conclude that $\overline{G} = S_n$, thus leading to (a). As for (b), it suffices to show that ∞ is not a branch point of f (by the second part of Condition (b) of Lemma 4.4), since every finite branch point of f is a root of $\Delta(T)$.

Setting $U = 1/T$, consider the polynomial

$$Q(U, Y) = U^D P(1/U, Y) = U^D Y^n + b_{n-1}(U)Y^{n-1} + \cdots + b_1(U)Y + b_0(U),$$

where $b_i(U) = a_i(1/U)U^D$, $i \in \{0, \dots, n-1\}$. Since $Q(0, Y)$ is separable (even irreducible) of degree $n-1$ (by Condition (c) of Lemma 4.4), $U = 0$ has n distinct preimages under the degree n regular $\mathbb{Q}$-cover of $\mathbb{P}^1$ defined by $P(T, Y)$ (namely, $n-1$ distinct points with finite Y-coordinate, and one more infinite point). It is therefore unramified at $U = 0$, as is its Galois closure f. This concludes the proof. □

Lemma 4.6. *Let $E/\mathbb{Q}(T)$ be a regular G-extension all of whose branch points are algebraically conjugate. Then there exists a positive density set $\mathcal{S}_0$ of prime numbers such that all specializations of $E/\mathbb{Q}(T)$ are unramified at all the primes in $\mathcal{S}_0$.*

Proof. Let $R(T) \in \mathbb{Q}[T]$ be the minimal polynomial over $\mathbb{Q}$ of the branch points of $E/\mathbb{Q}(T)$, F the splitting field of $R(T)$ over $\mathbb{Q}$, and $G = \mathrm{Gal}(F/\mathbb{Q})$. Then G is transitive, and so there exists an element σ of G fixing no branch point of $E/\mathbb{Q}(T)$. Let $\mathcal{S}_0$ denote the

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

set of all prime numbers p such that the Frobenius associated with p in $F/\mathbb{Q}$ is conjugate in G to σ. By the Chebotarev density theorem, $\mathcal{S}_0$ has density $\alpha = |C_\sigma|/|G| \in]0, 1[$, with C_σ the conjugacy class of σ in G. Moreover, by the definition of $\mathcal{S}_0$, no prime number $p \in \mathcal{S}_0$ (possibly up to finitely many exceptions) is a *prime divisor* of $R(T)$, that is, there exist no $t_0 \in \mathbb{Q}$ such that $v_p(R(t_0)) > 0$. Theorem 2.2 then yields that, for every prime number $p \in \mathcal{S}_0$ (possibly up to finitely many exceptions), no specialization of $E/\mathbb{Q}(T)$ ramifies at p. □

A 'moral' implication of Lemma 4.6 is that, for covers f as in Lemma 4.5, the set $\mathrm{Sp}(f)$ cannot be too large. Turning this into a precise statement depends on precise knowledge about the distribution of S_n-extensions of $\mathbb{Q}$, which, in general, is a very difficult problem. For the special case $n = 3$, however, we have the following result:

Theorem 4.7. *Given a positive integer D, consider the set S of all polynomials $P(T, Y) \in \mathcal{Q}(3, D)$ fulfilling the following two conditions:*

(a) *$P(T, Y)$ defines a regular $\mathbb{Q}$-S_3-cover $f : X \to \mathbb{P}^1$;*

(b) *there exists a positive constant α such that*

$$\frac{|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(S_3, x)|}{|\overline{\mathcal{S}}(S_3, x)|} = O(\log^{-\alpha}(x))$$

as x tends to ∞ (in particular, the set $\mathrm{Sp}(f)$ has density 0).

Then one has

$$\frac{|S \cap \mathcal{Q}(3, D, H)|}{|\mathcal{Q}(3, D, H)|} = 1 - O\left(\frac{\log(H)}{\sqrt{H}}\right)$$

as H tends to ∞. In particular, the set S has density 1.

Proof. We choose S' as in Lemma 4.5 in the case $n = 3$. Given $P(T, Y) \in S'$, it suffices to show that (b) holds for the regular $\mathbb{Q}$-S_3-cover $f : X \to \mathbb{P}^1$ defined by $P(T, Y)$. Indeed, one then has $S' \subseteq S$ and the desired conclusion then follows from Lemma 4.5. Let $\mathcal{S}_0$ be the set of prime numbers provided by Lemma 4.6. Given $x \geqslant 1$, denote by $\mathcal{S}'(S_3, x)$ the set of all extensions $F/\mathbb{Q}$ in $\mathcal{S}(S_3, x)$ which ramify only at prime numbers not in $\mathcal{S}_0$. The asymptotic behavior of the ratio

$$\frac{|\mathcal{S}'(S_3, x)|}{|\mathcal{S}(S_3, x)|}$$

depends on the Bhargava principle (see [2]), which has been established for S_3-extensions of $\mathbb{Q}$ in [3]. A consequence of the mass formulas featuring in the principle is that, given a prime number p, the set of S_3-extensions ramifying tamely at p is (either empty or)[10] of density at least c/p, for some positive constant c not depending on p. Furthermore, the principle implies that the probabilities of local behaviors of S_3-extensions at any given

[10]This first case clearly does not happen, as every prime number ramifies tamely in a suitable S_3-extension.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

finite set of prime numbers are independent. This yields

$$\frac{|\mathcal{S}'(S_3,x)|}{|\mathcal{S}(S_3,x)|} = O\Big(\prod_{\substack{p\leqslant x\\ p\in\mathcal{S}_0}}\Big(1-\frac{1}{p}\Big)\Big), \quad x\to\infty.$$

Then, by Lemma 4.6 and [37, théorème 2.3], there exists some constant $\alpha>0$ such that

$$\frac{|\mathrm{Sp}(E)\cap\mathcal{S}(S_3,x)|}{|\mathcal{S}(S_3,x)|} \leqslant \frac{|\mathcal{S}'(S_3,x)|}{|\mathcal{S}(S_3,x)|} = O(\log^{-\alpha}(x)), \quad x\to\infty,$$

where $E/\mathbb{Q}(T)$ denotes the regular S_3-extension associated with the cover f. Since the map from $\mathrm{Sp}(f)$ to $\mathrm{Sp}(E)$, mapping a morphism to the fixed field of its kernel, has finite fibers of bounded cardinality (with the bound depending only on the order of the underlying Galois group, which is 6 here), conclude that (b) holds. □

Remark 4.8. The above way of counting covers is not canonical, since the map between polynomials and covers is not 1-to-1. It does however allow natural generalizations. In particular, assume a family of regular $\mathbb{Q}$-G-covers $X\to\mathbb{P}^1$ is parameterized by an irreducible polynomial $P(T_1,\dots,T_k,T,Y)$ with algebraically independent indeterminates $T_1,\dots,T_k$. Such a situation occurs whenever the Hurwitz space of covers of a given ramification type happens to be a rational variety. If, in addition, the branch points of such covers can be chosen such that some element of $\mathrm{G}_{\mathbb{Q}}$ permutes them *without fixed point*, then our arguments apply in the same way. This idea was used in [31] to show that most rational translates of a fixed regular $\mathbb{Q}$-G cover of $\mathbb{P}^1$ have a smaller specialization set than the original cover.

5. On a local–global principle for specializations

This section deals with our local–global principle for specializations, as alluded to in § 1.5.

5.1. Statement of the main result

We first need some terminology and notation.

Given a prime $\mathfrak{p}$ (possibly infinite) of a number field k, denote the restriction map $\mathrm{G}_{k_\mathfrak{p}}\to\mathrm{G}_k$ by $\mathrm{res}_\mathfrak{p}$ (with $k_\mathfrak{p}$ the completion of k at $\mathfrak{p}$). Given a finite group G and an epimorphism $\varphi:\mathrm{G}_k\to G$, the composed map $\varphi\circ\mathrm{res}_\mathfrak{p}:\mathrm{G}_{k_\mathfrak{p}}\to G$ is denoted by $\varphi_\mathfrak{p}$.

Definition 5.1. Let $f:X\to\mathbb{P}^1$ be a regular $\mathbb{Q}$-G-cover and $\varphi:\mathrm{G}_{\mathbb{Q}}\to G$ an epimorphism.

(a) Say that φ is a specialization morphism of f *everywhere locally* if φ_p is a specialization morphism of $f\otimes_{\mathbb{Q}}\mathbb{Q}_p$ for every prime p.

(b) Say that (f,φ) *fulfills the local–global principle* if the following implication holds:

$$\varphi\in\mathrm{Sp}(f)^{\mathrm{loc}} \Longrightarrow \varphi\in\mathrm{Sp}(f),$$

where $\mathrm{Sp}(f)^{\mathrm{loc}}$ denotes the set of all epimorphisms $\mathrm{G}_{\mathbb{Q}}\to G$ as in (a).

The existence of an epimorphism $\varphi:\mathrm{G}_{\mathbb{Q}}\to G$ such that (f,φ) does not fulfill the local–global principle means that φ does not occur as a specialization morphism of f but

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

this cannot be detected by local considerations. Moreover, note that a similar principle for specializations of regular G-extensions of $\mathbb{Q}(T)$ could be defined.

This theorem is our main contribution to our local–global principle for specializations:

Theorem 5.2. *Let $f : X \to \mathbb{P}^1$ be a regular $\mathbb{Q}$-G-cover with branch points $t_1, \dots, t_r$. Assume the inertia group at some t_i intersects the center of G non-trivially. Let q be the least prime number such that a central element of order q lies in the inertia group at some t_i, and let*

$$\beta = \frac{q}{(q-1)|G|}. \tag{5.1}$$

Then the following three conclusions hold.

(a) *This inequality holds for some positive constant $C(f)$ and every sufficiently large x:*

$$|\mathrm{Sp}(f)^{\mathrm{loc}} \cap \overline{\mathcal{S}}(G,x)| \geqslant C(f) \cdot x^{\beta} \cdot \log^{-1}(x).$$

(b) *Assume the abc-conjecture holds and $r \geqslant 8$. Then one has*

$$\lim_{x\to\infty} \frac{|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G,x)|}{|\mathrm{Sp}(f)^{\mathrm{loc}} \cap \overline{\mathcal{S}}(G,x)|} = 0.$$

In particular, for some positive constant $C'(f)$ and every sufficiently large integer x, the number of epimorphisms $\varphi \in \overline{\mathcal{S}}(G,x)$ such that (f,φ) does not fulfill the local–global principle is at least $C'(f) \cdot x^{\beta} \cdot \log^{-1}(x)$.

(c) *Assume the abc-conjecture and (3.3) hold (with S equal to the set of all branch points of f), and that the inertia group at some t_i contains a central element of order equal to the least prime divisor of $|G|$. Then one has $\beta = \alpha(G)$, where $\alpha(G)$ is defined in (1.3),*[11] *and*

$$\lim_{x\to\infty} \frac{|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G,x)|}{|\mathrm{Sp}(f)^{\mathrm{loc}} \cap \overline{\mathcal{S}}(G,x)|} = 0.$$

In particular, for some positive constant $C'(f)$ and every sufficiently large integer x, the number of epimorphisms $\varphi \in \overline{\mathcal{S}}(G,x)$ such that (f,φ) does not fulfill the local–global principle is at least $C'(f) \cdot x^{\alpha(G)} \cdot \log^{-1}(x)$.

5.2. Proof of Theorem 5.2

We break the proof into four parts.

5.2.1. Preliminaries. The proof is based on the investigation of the local behavior of specializations of the regular G-extension of $\mathbb{Q}(T)$ associated with f. We shall make use of the following general result, stemming from the two papers [16] and [27]:

Proposition 5.3. *Let k be a number field, G a finite group, $g : X \to \mathbb{P}^1$ a regular k-G-cover, $E/k(T)$ the regular G-extension associated with g, and $t_1, \dots, t_r$ the branch points of g. For $1 \leqslant i \leqslant r$, let $(E(t_i))_{t_i}/k(t_i)$ bethe residue extension of $E(t_i)/k(t_i)(T)$ at the prime*

[11] In the general case, one has $\alpha(G) \geqslant \beta > 1/|G| \geqslant \alpha(G)/2$.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

ideal generated by $T - t_i$. Then there exists a finite set $\mathcal{S}_{\mathrm{exc}}$ of prime ideals of the ring of integers of k, containing those prime ideals dividing $|G|$, such that, for every prime ideal $\mathfrak{p}$ not contained in $\mathcal{S}_{\mathrm{exc}}$ and every epimorphism $\varphi : \mathrm{G}_k \to G$, the following conclusions hold.

(a) *If $\varphi_{\mathfrak{p}}$ is unramified, then $g \otimes_k k_{\mathfrak{p}}$ specializes to $\varphi_{\mathfrak{p}}$.*

(b) *If $\varphi_{\mathfrak{p}}$ is totally ramified with image equal to the inertia group at some t_i and if $\mathfrak{p}$ splits completely in the extension $(E(t_i))_{t_i}/k$, then $g \otimes_k k_{\mathfrak{p}}$ specializes to some homomorphism $\varphi'(\mathfrak{p}) : \mathrm{G}_{k_{\mathfrak{p}}} \to G$ such that $\varphi_{\mathfrak{p}}$ and $\varphi'(\mathfrak{p})$ have the same kernels.*

Proof. (a) follows directly from [16, Theorem 1.2]. As for (b), it is a special case of [27, Theorem 4.4] (namely, with the assumption $N^{(\mathfrak{p})} = k_{\mathfrak{p}}$ in the notation there). Note that specialization is worded in terms of fields rather than morphisms in [27], hence the above conclusion replacing $\varphi_{\mathfrak{p}}$ by some other morphism with the same kernel. □

We need some notation. Denote the regular G-extension of $\mathbb{Q}(T)$ associated with f by $E/\mathbb{Q}(T)$. For $1 \leqslant i \leqslant r$, let $(E(t_i))_{t_i}/\mathbb{Q}(t_i)$ be the residue extension of $E(t_i)/\mathbb{Q}(t_i)(T)$ at the prime ideal generated by $T - t_i$.

Let $t_0 \in \mathbb{P}^1(\mathbb{Q}) \setminus \{t_1, \dots, t_r\}$ be such that the specialization morphism $f_{t_0} : \mathrm{G}_{\mathbb{Q}} \to G$ is surjective; such a t_0 exists by Hilbert's irreducibility theorem. The general idea of the proof is to construct, by slightly changing the epimorphism f_{t_0}, sufficiently many epimorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ that occur as a specialization morphism of f everywhere locally. More precisely, our epimorphisms φ will have only one more ramified prime number, compared to f_{t_0}. In order to reach the required amount of epimorphisms of bounded discriminant, the newly ramified prime number furthermore needs to have 'small' ramification index. Let $i \in \{1, \dots, r\}$ and g an element of the center of G of order q, where q is defined in Theorem 5.2, such that g is contained in the inertia group at t_i.

5.2.2. Construction of suitable epimorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$. Let $\mathcal{S}_{\mathrm{exc}}$ be the finite set of prime numbers provided by Proposition 5.3, when applied to the $\mathbb{Q}$-G-cover f, $\mathcal{S}$ an arbitrary finite set of prime numbers containing $\mathcal{S}_{\mathrm{exc}}$, $\mathcal{S}_1$ the set of all prime numbers which ramify in $E_{t_0}/\mathbb{Q}$, and p a prime number satisfying the following three properties (which depend on $\mathcal{S}$):

(i) $p \notin \mathcal{S} \cup \mathcal{S}_1$;

(ii) p splits completely in the extension $(E(t_i))_{t_i}/\mathbb{Q}$;

(iii) p splits completely in $F(\{\sqrt[q]{\ell} | \ell \in \mathcal{S} \cup \mathcal{S}_1\})/\mathbb{Q}$, where $F = \begin{cases} E_{t_0}(e^{2i\pi/q}) \text{ if } q \geqslant 3 \\ E_{t_0}(i) \text{ if } q = 2 \end{cases}$.

In particular, one has $p \equiv 1 \bmod q$ due to (iii).

Let $\varphi(p) : \mathrm{G}_{\mathbb{Q}} \to \langle g \rangle$ be an epimorphism such that if $L_{(p)}$ denotes the fixed field of the kernel of $\varphi(p)$ in $\overline{\mathbb{Q}}$, then $L_{(p)}$ is the unique degree q subfield of $\mathbb{Q}(e^{2i\pi/p})$. Note that the field $L_{(p)}$ embeds into $\mathbb{R}$ and the extension $L_{(p)}/\mathbb{Q}$ ramifies only at p.[12]

[12] In the case $q = 2$, we use the fact that p splits in $\mathbb{Q}(i)/\mathbb{Q}$ to ensure that 2 is unramified in $L_{(p)}/\mathbb{Q}$.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Since the ramification loci of $E_{t_0}/\mathbb{Q}$ and $L_{(p)}/\mathbb{Q}$ are disjoint (by (i)), the fields E_{t_0} and $L_{(p)}$ are linearly disjoint over $\mathbb{Q}$. We can therefore consider the direct product homomorphism $\psi(p) = f_{t_0} \times \varphi(p)$; this is an epimorphism from $\mathrm{G}_{\mathbb{Q}}$ onto $G \times \langle g \rangle$. Let Δ be the diagonal subgroup of $G \times \langle g \rangle$ generated by (g, g). Note that Δ is normal as g lies in the center of G. Consider the composed map $\mathrm{pr} \circ \psi(p)$, with pr the canonical projection from $G \times \langle g \rangle$ onto $(G \times \langle g \rangle)/\Delta$. As this quotient group equals G up to canonical isomorphism $g' \mapsto (g', 1) \cdot \Delta$, one obtains an epimorphism $\varphi'(p) : \mathrm{G}_{\mathbb{Q}} \to G$.

This lemma asserts that, up to choosing a suitable set $\mathcal{S}$ and a suitable epimorphism $\varphi(p)$, the above epimorphism $\varphi'(p)$ occurs as a specialization morphism of f everywhere locally:

Lemma 5.4. *For some finite set $\mathcal{S} \supseteq \mathcal{S}_{\mathrm{exc}}$ of prime numbers, depending only on f, the following holds. Let p be a prime number satisfying* (i), (ii), *and* (iii). *Then there exists an epimorphism $\varphi(p) : \mathrm{G}_{\mathbb{Q}} \to \langle g \rangle$ with fixed field $L_{(p)}$ as above, and for which the associated epimorphism $\varphi'(p) : \mathrm{G}_{\mathbb{Q}} \to G$ is such that $f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ specializes to $\varphi'(p)_\ell$ for every prime ℓ.*

5.2.3. Proof of Theorem 5.2 under Lemma 5.4. Let $\mathcal{S}$ be a finite set of prime numbers as given by Lemma 5.4. To prove (a), we estimate the number of epimorphisms $\varphi'(p) : \mathrm{G}_{\mathbb{Q}} \to G$ provided by Lemma 5.4, when p runs through the set of all prime numbers satisfying (i), (ii), and (iii). Let p be such a prime number. Since E_{t_0} and $L_{(p)}$ are linearly disjoint over $\mathbb{Q}$ and as the discriminants $d_{E_{t_0}}$ and $d_{L_{(p)}}$ of E_{t_0} and $L_{(p)}$, respectively, are coprime, one has

$$|d_{E_{t_0} L_{(p)}}| = |d_{E_{t_0}}|^q \cdot |d_{L_{(p)}}|^{|G|}.$$

Moreover, as $L_{(p)}/\mathbb{Q}$ is Galois of degree q and ramifies only at p, one has $|d_{L_{(p)}}| = p^{q-1}$. Combine this equality and the fact that g has order q to get that if $L'_{(p)}$ denotes the fixed field of $\ker(\varphi'(p))$ in $\overline{\mathbb{Q}}$, then

$$|d_{L'_{(p)}}| \leqslant C_1 \cdot p^{\frac{q-1}{q}|G|},$$

where $C_1 = |d_{E_{t_0}}|$ depends only on f. Furthermore, as $L'_{(p)}/\mathbb{Q}$ ramifies at p (with ramification index q) and is unramified outside $\mathcal{S}_1 \cup \{p\}$, one has $L'_{(p_1)} \neq L'_{(p_2)}$ for distinct prime numbers p_1 and p_2 as above. Finally, as the set of all prime numbers p fulfilling (i), (ii), and (iii) is a positive density subset of the set of all prime numbers, there are asymptotically at least $C_2 \cdot x \cdot \log^{-1}(x)$ such epimorphisms $\varphi'(p)$ with $p \leqslant x$, for some positive constant C_2 depending only on f. In total, the number of such epimorphisms $\varphi'(p)$ with $|d_{L'_{(p)}}| \leqslant x$ is then asymptotically at least

$$C_3 \cdot x^{\beta} \cdot \log^{-1}(x),$$

where C_3 is a positive constant depending only on f. This completes the proof of (a).

As for (b), suppose the abc-conjecture holds and $r \geqslant 8$. From the latter assumption and the definition of β, the exponent e defined in (3.2) (with S equal to the set of all

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

branch points of f) satisfies $e < \beta(G)$. Pick $\epsilon > 0$ with $e + \epsilon < \beta(G)$. Then combine (a) and Theorem 3.1 to obtain that

$$\frac{|\mathrm{Sp}(f) \cap \overline{\mathcal{S}}(G,x)|}{|\mathrm{Sp}(f)^{\mathrm{loc}} \cap \overline{\mathcal{S}}(G,x)|} = O(\log(x) \cdot x^{e+\epsilon-\beta(G)}) = o(1), \quad x \to \infty.$$

Finally, under the assumptions in (c), q is the smallest prime divisor of $|G|$ and one has $\beta = \alpha(G)$. Moreover, in this case, it suffices to check $e < \alpha(G)$ in the proof of (b) above to get the desired conclusion. As seen in the proof of Corollary 3.3, this inequality holds if and only if (3.3) holds.

5.2.4. Proof of Lemma 5.4. We first prove the following statement:

Lemma 5.5. *Fix a finite set $\mathcal{S}$ of prime numbers containing $\mathcal{S}_{\mathrm{exc}}$, a prime number p satisfying* (i), (ii), *and* (iii), *and an epimorphism $\varphi(p) : \mathrm{G}_{\mathbb{Q}} \to \langle g \rangle$ with fixed field $L_{(p)}$ as in § 5.2.2. Then the associated epimorphism $\varphi'(p) : \mathrm{G}_{\mathbb{Q}} \to G$ is such that $\varphi'(p)_\ell$ is a specialization morphism of $f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ for every prime $\ell \neq p$.*

Proof. Let ℓ be a prime $\neq p$. First, assume ℓ is finite and $\ell \notin \mathcal{S} \cup \mathcal{S}_1$. By our construction, ℓ is unramified in $E_{t_0}L_{(p)}/\mathbb{Q}$, and the same holds in the subextension $L'_{(p)}/\mathbb{Q}$. Therefore, by Proposition 5.3(a) (which can be applied as $\mathcal{S}$ contains $\mathcal{S}_{\mathrm{exc}}$), $f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ specializes to $\varphi'(p)_\ell$.

Second, assume ℓ is infinite or $\ell \in \mathcal{S} \cup \mathcal{S}_1$. Then $\varphi(p)_\ell$ is trivial. Indeed, for $\ell = \infty$, this is clear since $L_{(p)} \subseteq \mathbb{R}$ by construction. Assume then that ℓ is finite. If $q = 2$, then it follows from (iii) and the quadratic reciprocity that ℓ is totally split in the extension $\mathbb{Q}(\sqrt{p})/\mathbb{Q} = L_{(p)}/\mathbb{Q}$. One may then assume that q is odd. By (iii), $Y^q - \ell$ splits completely in $\mathbb{Q}_p$. This means that ℓ is a qth power in $\mathbb{Q}_p$. In other words, the multiplicative order of ℓ in $\mathbb{F}_p$ is a divisor of $(p-1)/q$. Consequently, the Frobenius of $\mathbb{Q}(e^{2i\pi/p})/\mathbb{Q}$ at ℓ is of order dividing $(p-1)/q$. As the elements of $\mathrm{Gal}(\mathbb{Q}(e^{2i\pi/p})/\mathbb{Q})$ of order dividing $(p-1)/q$ act trivially on $L_{(p)}$, we get that the Frobenius of $L_{(p)}/\mathbb{Q}$ at ℓ is trivial, thus proving the claim. Therefore, one has $(f_{t_0})_\ell = \psi(p)_\ell = \varphi'(p)_\ell$. In particular, $f \otimes_{\mathbb{Q}} \mathbb{Q}_\ell$ specializes to $\varphi'(p)_\ell$. □

We now proceed to the proof of Lemma 5.4. By Lemma 5.5, it suffices to show that $f \otimes_{\mathbb{Q}} \mathbb{Q}_p$ specializes to $\varphi'(p)_p$, under a suitable choice of $\mathcal{S}$ and $\varphi(p)$. This is done by reducing to Proposition 5.3(b). At this stage, choose $\mathcal{S}$ and $\varphi(p)$ arbitrary as above.

By the definition of $\varphi(p)$ and (i), the induced epimorphism $\varphi(p)_p : \mathrm{G}_{\mathbb{Q}_p} \to \langle g \rangle$ is totally (tamely) ramified. Its image $\langle g \rangle$ is not necessarily the inertia group at some branch point of f. However, this holds for a suitable pullback of f.

Indeed, up to applying a change of variable at the beginning of § 5.2, we may assume $\infty \notin \{t_1, \ldots, t_r\}$. With $U = 1/(T - t_i)$, one sees that ∞ is a branch point of $E(t_i)/\mathbb{Q}(t_i)(U)$ but 0 is not. Let e_i be the ramification index at t_i and $V = U^{q/e_i}$. Since the extensions $E\overline{\mathbb{Q}}/\overline{\mathbb{Q}}(U)$ and $\overline{\mathbb{Q}}(V)/\overline{\mathbb{Q}}(U)$ have only one common branch point (namely, ∞), the fields $E\overline{\mathbb{Q}}$ and $\overline{\mathbb{Q}}(V)$ are linearly disjoint over $\overline{\mathbb{Q}}(U)$. Thus, $E\overline{\mathbb{Q}}(V)/\overline{\mathbb{Q}}(V)$ is still a regular G-extension, and the same holds, in particular, for $E(t_i)(V)/\mathbb{Q}(t_i)(V)$. Let $f' : X' \to \mathbb{P}^1$ be the associated regular $\mathbb{Q}(t_i)$-G-cover. By Abhyankar's lemma, $\langle g \rangle$ is the inertia group of f' at ∞.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Set $k = (E(t_i))_{t_i}$ and denote the cover $f' \otimes_{\mathbb{Q}(t_i)} k$ by f''. If $\mathfrak{p}$ is any prime ideal lying over p in $k/\mathbb{Q}$, then the completion $k_{\mathfrak{p}}$ is equal to $\mathbb{Q}_p$, due to the splitting assumption in (ii). Moreover, as p is totally split in $E_{t_0}/\mathbb{Q}$ (by (iii)), the restriction $(f_{t_0})_p$ is trivial, that is, $\varphi(p)_p = \psi(p)_p = \varphi'(p)_p$. Hence, since every specialization morphism of $f'' \otimes_k \mathbb{Q}_p$ (at a point $t \in \mathbb{P}^1(\mathbb{Q}_p)$) is a specialization morphism of $f \otimes_{\mathbb{Q}} \mathbb{Q}_p$ (namely, at $1/t^{e_i/q} + t_i$), it suffices to show that $f'' \otimes_k \mathbb{Q}_p$ specializes to $\varphi(p)_p$.

Choose $\mathcal{S}$ as the set of all prime numbers ℓ which are in the already defined set $\mathcal{S}_{\mathrm{exc}}$ or such that some prime ideal lying over ℓ in the extension $k/\mathbb{Q}$ belongs to the exceptional set provided by Proposition 5.3, when applied to the cover f''. By Proposition 5.3(b), $f'' \otimes_k \mathbb{Q}_p$ specializes to some homomorphism $\varphi''(p) : \mathrm{G}_{\mathbb{Q}_p} \to G$ such that $\varphi(p)_p$ and $\varphi''(p)$ have the same kernels. In particular, the image of $\varphi''(p)$ is equal to $\langle g \rangle$ and $\varphi''(p) = \sigma \circ \varphi(p)_p$ for some automorphism $\sigma : \langle g \rangle \to \langle g \rangle$. Then consider the epimorphism $\sigma \circ \varphi(p) : \mathrm{G}_{\mathbb{Q}} \to \langle g \rangle$. The fixed field of the kernel of this epimorphism is equal to that of $\varphi(p)$ and $f'' \otimes_k \mathbb{Q}_p$ specializes to $(\sigma \circ \varphi(p))_p$, as $(\sigma \circ \varphi(p))_p = \sigma \circ \varphi(p)_p = \varphi''(p)$. Conclude that the lemma holds.

5.3. On the assumptions of Theorem 5.2

We exhibit below several explicit situations where covers as in Theorem 5.2 can be constructed.

5.3.1. Abelian groups. If G is an arbitrary finite abelian group, then the condition on inertia groups in Theorem 5.2(c) is satisfied for every regular $\mathbb{Q}$-G cover f of $\mathbb{P}^1$, as the inertia groups at the branch points of f generate G. Moreover, if f has at least 7 branch points, then (3.3) holds (see Remark 3.4). Hence, the conclusion of Theorem 1.7 follows from Theorem 5.2(c).

5.3.2. Extension to some non-abelian groups. In fact, the same applies for some non-abelian groups G as well. Here are some examples:

(a) $G = H \times \mathbb{Z}/2^k\mathbb{Z}$, where H is an arbitrary finite group, and 2^k is strictly larger than the highest 2-power occurring as an element order in H;

(b) $G = Q_8^n \times H$, where Q_8 is the quaternion group, $n \geqslant 1$, and H is abelian.

Indeed, for (a), if $(h_1, g_1), \ldots, (h_r, g_r)$ generate G, with $h_1, \ldots, h_r \in H$ and $g_1, \ldots, g_r \in \mathbb{Z}/2^k\mathbb{Z}$, then we may assume g_1 is of order 2^k. Thanks to our assumption on k, there exists $m \geqslant 1$ with $h_1^{2^{k-1}+m2^k} = 1$. As for (b), suppose $(g_1, h_1), \ldots, (g_r, h_r)$ generate G, with $g_1, \ldots, g_r \in Q_8^n$ and $h_1, \ldots, h_r \in H$. We may assume g_1 is of order 4. Then (g_1^2, h_1^2) has even order, say $2m$ with $m \geqslant 1$. Hence, (g_1^{2m}, h_1^{2m}) has order 2 and is in the center of G.

5.3.3. Regular Galois groups over $\mathbb{Q}$ with non-trivial center. Let G be a regular Galois group over $\mathbb{Q}$ with non-trivial center. Then there exists a regular $\mathbb{Q}$-G-cover of $\mathbb{P}^1$ whose inertia group at some branch point intersects the center of G non-trivially.

Indeed, let $f : X \to \mathbb{P}^1$ be a regular $\mathbb{Q}$-G-cover, g an element of the center of G of prime order, and $f' : X' \to \mathbb{P}^1$ a regular $\mathbb{Q}$-$\langle g \rangle$-cover. Up to applying a suitable change of variable, we may assume that the sets of branch points of f and f' are disjoint. Denote

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

the function field extensions of the covers f and f' by $E/\mathbb{Q}(T)$ and $E'/\mathbb{Q}(T)$, respectively. Then the fields $E\overline{\mathbb{Q}}$ and $E'\overline{\mathbb{Q}}$ are linearly disjoint over $\overline{\mathbb{Q}}$, that is, the extension $EE'/\mathbb{Q}(T)$ is a regular $(G \times \langle g \rangle)$-extension. If E'' denotes the fixed field of $\langle g \rangle \times \langle g \rangle$ in EE', then $E''/\mathbb{Q}(T)$ is a regular G-extension, each branch point t of $E'/\mathbb{Q}(T)$ is a branch point of $E''/\mathbb{Q}(T)$, and the inertia group of $E''/\mathbb{Q}(T)$ at t is equal to $\langle g \rangle$. Consequently, the regular $\mathbb{Q}$-G-cover f'' of $\mathbb{P}^1$ associated with the extension $E''/\mathbb{Q}(T)$ satisfies the desired conclusion.

We note for later use that we can simultaneously require that no branch point of f'' is $\mathbb{Q}$-rational and the total number of branch points of f'' is arbitrarily large (in particular, at least 8). Indeed, up to replacing f by a suitable pullback of f, we may assume no branch point of f is $\mathbb{Q}$-rational. Moreover, as a consequence of the rigidity method, we may assume the same holds for the cover f' and the number of branch points of f' is arbitrarily large.

6. Diophantine aspects

In this section, we discuss diophantine aspects of our results, as already alluded to in § 1.6.

6.1. Preliminaries

Our first aim is to briefly recall the definition and the main properties of the twisted cover from [11]. See, e.g., [16, § 2.2] for more details. We use below the notation introduced in § 2.2.

Let k be a field of characteristic zero, $\overline{k}$ an algebraic closure of k, G a finite group, $f : X \to \mathbb{P}^1$ a regular k-G-cover of branch points $t_1, \dots, t_r$, and $\varphi : \mathrm{G}_k \to G$ a homomorphism. Denote the right-regular (respectively, left-regular) representation of G by $\delta : G \to S_{|G|}$ (respectively, by $\gamma : G \to S_{|G|}$). Define $\varphi^* : \mathrm{G}_k \to G$ by $\varphi^*(\sigma) = \varphi(\sigma)^{-1}$ $(\sigma \in \mathrm{G}_k)$. Denote the restriction map $\pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_k \to \mathrm{G}_k$ by res and the multiplication in $S_{|G|}$ by $\times$.

If $\phi : \pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_k \to G$ is the epimorphism corresponding to f, consider

$$\widetilde{\phi}^{\varphi} : \begin{cases} \pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_k & \longrightarrow \quad S_{|G|} \\ \theta & \longmapsto \ \widetilde{\phi}^{\varphi}(\theta) = \gamma \circ \phi(\theta) \times \delta \circ \varphi^* \circ \mathrm{res}(\theta). \end{cases}$$

Then the map $\widetilde{\phi}^{\varphi}$ is a homomorphism with the same restriction to $\pi_1(\mathbb{P}^1 \setminus \{t_1, \dots, t_r\}, t)_{\overline{k}}$ as ϕ, hence corresponds to a regular k-cover (not Galois in general), denoted by $\widetilde{f}^{\varphi} : \widetilde{X}^{\varphi} \to \mathbb{P}^1$ and called the *twisted cover* of f by φ, which satisfies $f \otimes_k \overline{k} = \widetilde{f}^{\varphi} \otimes_k \overline{k}$. In particular, the covers f and $\widetilde{f}^{\varphi}$ have the same branch points.

The following proposition (see [16, Twisting Lemma 2.1]) contains the main property of the twisted cover:

Proposition 6.1. *For every $t_0 \in \mathbb{P}^1(k) \setminus \{t_1, \dots, t_r\}$, the following conditions are equivalent:*

(a) *there exists a k-rational point x_0 on $\widetilde{X}^{\varphi}$ such that $\widetilde{f}^{\varphi}(x_0) = t_0$;*

(b) *there exists $\omega \in G$ such that the specialization morphism f_{t_0} equals* $\mathrm{conj}(\omega) \circ \varphi$.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Furthermore, the twisting operation commutes with extension of scalars: if $k' \supseteq k$, then the twisted cover of $f \otimes_k k'$ by the restriction of φ to $\mathrm{G}_{k'}$[13] is the regular k'-cover $\widetilde{f^{\varphi}} \otimes_k k'$.

Condition (a) of Proposition 6.1 leads us to the following terminology:

Definition 6.2. Let $f : X \to \mathbb{P}^1$ be a regular k-cover. Say that a k-rational point x on X is *trivial* if $f(x)$ is a (k-rational) branch point of f, and *non-trivial* otherwise.

Example 6.3. Let $f : X \to \mathbb{P}^1$ be a regular $\mathbb{Q}$-$\mathbb{Z}/2\mathbb{Z}$-cover and $P(T) \in \mathbb{Z}[T]$ separable such that X is the hyperelliptic curve $C_{P(T)} : y^2 = P(t)$. Then the set of all epimorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to \mathbb{Z}/2\mathbb{Z}$ is in 1-to-1 correspondence with the set $\mathcal{N}_2$ of all squarefree integers. Given such an integer d, the associated twisted curve $\widetilde{X}^{\varphi}$ is the hyperelliptic curve $C_{d \cdot P(T)} : y^2 = d \cdot P(t)$. Moreover, trivial points in the sense of Definition 6.2 correspond to those defined in § 2.3, and Proposition 2.3(b) corresponds to the quadratic case of Proposition 6.1.

6.2. Global aspects

Let G be a finite group and $f : X \to \mathbb{P}^1$ a regular $\mathbb{Q}$-G-cover. By § 6.1, the set $\mathrm{Sp}(f)$ is the set of all homomorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ such that the twisted curve $\widetilde{X}^{\varphi}$ has a non-trivial $\mathbb{Q}$-rational point. Hence, Theorem 3.1 can be rephrased as follows:

Theorem 6.4. *Let $S \subseteq \mathbb{P}^1(\overline{\mathbb{Q}})$ be a non-empty subset of the set of branch points of f, closed under the action of $\mathrm{G}_{\mathbb{Q}}$. Assume the abc-conjecture and (3.1) hold. Then, for every $\epsilon > 0$ and every sufficiently large x, the number $h(x)$ of all epimorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ in $\overline{\mathcal{S}}(G, x)$ such that the twisted curve $\widetilde{X}^{\varphi}$ has a non-trivial $\mathbb{Q}$-rational point satisfies*

$$h(x) \leqslant x^{e+\epsilon},$$

where e is defined in (3.2).

Similarly, all other results from §§ 3 and 4 with a density zero conclusion can be rewritten with the above diophantine flavor. We leave this to the interested reader.

In the case $G = \mathbb{Z}/2\mathbb{Z}$, Theorem 6.4 yields this corollary, which is [24, Corollary 1]:

Corollary 6.5. *Let $P(T) \in \mathbb{Z}[T]$ be a separable polynomial of degree $\geqslant 5$ and g the genus of the hyperelliptic curve $C_{P(T)} : y^2 = P(t)$. Assume the abc-conjecture holds. Then, for every $\epsilon > 0$ and every sufficiently large x, the number $h(x)$ of all squarefree integers $d \in [\![-x, x]\!]$[14] such that the twisted curve $C_{d \cdot P(T)} : y^2 = d \cdot P(t)$ has a non-trivial $\mathbb{Q}$-rational point satisfies*

$$h(x) \leqslant x^{(1/(g-1))+\epsilon}.$$

Proof. Let $f : X \to \mathbb{P}^1$ be the regular $\mathbb{Q}$-$\mathbb{Z}/2\mathbb{Z}$-cover given by the polynomial $Y^2 - P(T)$. By Proposition 2.3(a), f has $r \geqslant 6$ branch points. Hence, by Remark 3.2(b), Example 6.3, and Theorem 6.4, it suffices to show that the exponent e (with S the set of all branch points of f) is equal to $1/(g-1)$. By (3.2), one has $e = 2/(r-4)$. Moreover, one has $2(g-1) = r-4$ by the Riemann–Hurwitz formula. Conclude that the desired equality holds. □

[13] That is, by the homomorphism $\varphi \circ \mathrm{res}' : \mathrm{G}_{k'} \to G$, where $\mathrm{res}' : \mathrm{G}_{k'} \to \mathrm{G}_k$ is the restriction map.

[14] Recall that $[\![-x, x]\!]$ denotes the set of all integers between $-x$ and x.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

6.3. On the local–global principle for specializations

For a regular $\mathbb{Q}$-G-cover $f : X \to \mathbb{P}^1$, §6.1 shows that the set $\mathrm{Sp}(f)^{\mathrm{loc}} \setminus \mathrm{Sp}(f)$, with $\mathrm{Sp}(f)^{\mathrm{loc}}$ introduced in Definition 5.1, is the set of all epimorphisms $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ such that the twisted curve $\widetilde{X}^{\varphi}$ has a non-trivial $\mathbb{Q}_p$-rational point for every prime p but only trivial $\mathbb{Q}$-rational points. As above, Theorem 5.2 may be worded with this diophantine flavor. We leave this to the interested reader.

Let us rather give an application of our result to the Hasse principle. Recall that a curve C over $\mathbb{Q}$ fulfills the Hasse principle if the following implication holds:

$$C \text{ has a } \mathbb{Q}_p\text{-rational point for every prime } p \implies C \text{ has a } \mathbb{Q}\text{-rational point.}$$

The sole difference between the Hasse principle and the diophantine analog of our local–global principle for specializations is that, since we are interested in covers rather than just abstract curves, we have to disallow rational points extending branch points. However, if we start with a cover with no $\mathbb{Q}$-rational branch point, then the twisted curves provided by (the diophantine version of) Theorem 5.2 do not fulfill the Hasse principle.

For example, by combining Theorem 5.2 and §§5.3.1–5.3.2, we obtain Corollary 6.6, which makes Theorem 1.8 more precise:

Corollary 6.6. *Let G be a finite abelian group or a finite group as in §5.3.2, and let $f : X \to \mathbb{P}^1$ be a regular $\mathbb{Q}$-G cover with no $\mathbb{Q}$-rational branch point. Assume the abc-conjecture holds and f has at least 7 branch points. Then, for some positive constant $C(f)$ and every sufficiently large x, the number of epimorphisms $\varphi \in \overline{\mathcal{S}}(G, x)$ such that $\widetilde{X}^{\varphi}$ does not fulfill the Hasse principle is at least*

$$C(f) \cdot x^{\alpha(G)} \cdot \log^{-1}(x),$$

where $\alpha(G)$ is defined in (1.3).

In the special case $G = \mathbb{Z}/2\mathbb{Z}$, we have this corollary, which is [8, Theorem 2] and which follows from Corollary 6.6 as Corollary 6.5 follows from Theorem 6.4:

Corollary 6.7. *Let $P(T) \in \mathbb{Z}[T]$ be a separable polynomial of even degree at least 8 and without any root in $\mathbb{Q}$. Suppose the abc-conjecture holds. Then there exists a positive constant C, depending only on $P(T)$, which satisfies the following. For every sufficiently large x, the number of all squarefree integers $d \in [\![-x, x]\!]$ such that the twisted hyperelliptic curve $C_{d \cdot P(T)} : y^2 = d \cdot P(t)$ does not fulfill the Hasse principle is at least $C \cdot x \cdot \log^{-1}(x)$.*

Remark 6.8. If $P(T)$ is of odd degree, then the conclusion fails trivially as the trivial point $[0 : 1 : 0]$ lies on every quadratic twist of $C_{P(T)}$. This actually gives an example where the Hasse principle holds but our local–global principle fails.

Namely, consider a separable polynomial $P(T) \in \mathbb{Z}[T]$ of odd degree. Then $C_{P(T)} : y^2 = P(t)$ has a non-trivial $\mathbb{Q}_p$-rational point for every prime p (an easy consequence of Hensel's lemma). Consequently, if d denotes an arbitrary squarefree integer, then the twisted hyperelliptic curve $C_{d \cdot P(T)} : y^2 = d \cdot P(t)$ has a non-trivial $\mathbb{Q}_p$-rational point for every prime p. However, by Corollary 6.5, if $P(T)$ has degree at least 7 and the abc-conjecture holds, then $C_{d \cdot P(T)}$ has only trivial $\mathbb{Q}$-rational points for almost

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

all squarefree integers d. Note that this last conclusion does hold unconditionally for infinitely many squarefree integers d in some situations (see, e.g., the upcoming Proposition B.2).

Even though the above situation seems like an artificial creation of a failure of Hasse principle (by disallowing trivial points), it is important from our point of view of specializations, since it yields a case of a regular $\mathbb{Q}$-G-cover $f : X \to \mathbb{P}^1$ where *every* epimorphism $\varphi : \mathrm{G}_{\mathbb{Q}} \to G$ is a specialization morphism of f everywhere locally, but not all such φ's occur as specialization morphisms of f. In particular, it provides a conditional example where the ratio (1.5) tends to 0, whereas the ratio in (1.4) does not.

In fact, Corollary 6.6 holds if f an arbitrary regular $\mathbb{Q}$-G-cover of $\mathbb{P}^1$ with 8 branch points or more, none of them is $\mathbb{Q}$-rational, and such that some geometric inertia group contains a non-trivial central element.[15] In particular, this corollary, which relies on § 5.3.3, allows to conditionally generate many more curves over $\mathbb{Q}$ failing the Hasse principle:

Corollary 6.9. *Let G be a regular Galois group over $\mathbb{Q}$ with non-trivial center. Assume the abc-conjecture holds. Then there exist a curve C over $\mathbb{Q}$, with a regular $\mathbb{Q}$-G-cover to $\mathbb{P}^1$, and 'many' $\mathbb{Q}$-curves C', which are isomorphic to C up to base change from $\mathbb{Q}$ to $\overline{\mathbb{Q}}$ and which do not fulfill the Hasse principle.*

Note that our arguments indeed yield infinitely many pairwise non-isomorphic (over $\mathbb{Q}$) such curves C'. This is because isomorphic curves over $\mathbb{Q}$ have isomorphic function fields, whereas it is easy to see that twists $\widetilde{f}^{\varphi_1}$ and $\widetilde{f}^{\varphi_2}$ of the same cover f have non-isomorphic function fields as soon as the kernels of φ_1 and φ_2 have distinct fixed fields.

Acknowledgements. The first author was supported by the National Research Foundation of Korea (NRF Grant no. 2019002665). The authors also wish to thank Arno Fehm for his help with Lemma 4.3.

Appendix A. Parametric extensions with few branch points

The aim of this section is to use various tools from previous papers to prove the following conditional result about parametric extensions with at most three branch points:

Theorem A.1. *Let G be a non-trivial finite group and let $E/\mathbb{Q}(T)$ be a regular G-extension with $r \leqslant 3$ branch points.*

(a) *Suppose $r = 2$. Then the following three conditions are equivalent:*
   (1) *the extension $E/\mathbb{Q}(T)$ is generic;*
   (2) *the extension $E/\mathbb{Q}(T)$ is parametric;*
   (3) *either $E = \mathbb{Q}(\sqrt{T})$, up to applying a change of variable (that is, $G = \mathbb{Z}/2\mathbb{Z}$ and each branch point of $E/\mathbb{Q}(T)$ is $\mathbb{Q}$-rational), or $G = \mathbb{Z}/3\mathbb{Z}$.*

[15] At the cost of replacing $\alpha(G)$ by the smaller constant β defined in (5.1).

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

(b) *Suppose all finite groups occur as Galois groups over* $\mathbb{Q}$ *and* $r = 3$. *Then the following three conditions are equivalent:*

(1) *the extension* $E/\mathbb{Q}(T)$ *is generic;*

(2) *the extension* $E/\mathbb{Q}(T)$ *is parametric;*

(3) *the field* E *is equal to the splitting field over* $\mathbb{Q}(T)$ *of the polynomial* $Y^3 + TY + T$ *(in which case* $G = S_3$*), up to applying a change of variable.*

Proof. (a) First, assume $r = 2$. By the Riemann existence theorem, one has $G = \mathbb{Z}/n\mathbb{Z}$ for some $n \geqslant 2$. As in the proof of Corollary 3.5, the Branch Cycle Lemma yields $2 = r \geqslant \varphi(n)$, where φ denotes the Euler totient function, that is, $n \in \{2, 3, 4, 6\}$. First, assume $n = 2$. Then $E/\mathbb{Q}(T)$ is parametric if and only if each branch point is $\mathbb{Q}$-rational [32, Proposition 3.1], and it is clear that $E/\mathbb{Q}(T)$ is generic if the latter holds. Now, assume $n = 3$. Then, as a consequence of, e.g., [17, Proposition 5.3], the extension $E/\mathbb{Q}(T)$ is generic. Finally, assume $n \in \{4, 6\}$. Then, by the Branch Cycle Lemma, none of the branch points of $E/\mathbb{Q}(T)$ is $\mathbb{Q}$-rational. In particular, there exist infinitely many prime numbers which ramify in no specialization of $E/\mathbb{Q}(T)$; see Lemma 4.6. However, for all prime numbers p, there are $\mathbb{Z}/n\mathbb{Z}$-extensions of $\mathbb{Q}$ which ramify at p. Conclude that $E/\mathbb{Q}(T)$ is not parametric.

(b) Now, we suppose $r = 3$. As all finite groups have been assumed to be Galois groups over $\mathbb{Q}$, one may use [29, Proposition 1] to get that there exists a totally real G-extension of $\mathbb{Q}$. By [15, Proposition 1.2], such a G-extension of $\mathbb{Q}$ cannot occur as a specialization of $E/\mathbb{Q}(T)$, unless G is dihedral of order $2n$ with $n \in \{2, 3, 4, 6\}$.

First, assume G is dihedral of order $2n$ with $n \in \{2, 4, 6\}$. In each case, G has a non-cyclic abelian subgroup (namely, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$). Then recall that, in this situation, [27, Theorem 6.2] shows that the extension $E/\mathbb{Q}(T)$ cannot be 'locally parametric'. That is, for infinitely many prime numbers p, there exists a finite Galois extension $F_p/\mathbb{Q}_p$ whose Galois group embeds into G and which does not occur as a specialization of $E\mathbb{Q}_p/\mathbb{Q}_p(T)$. Since G is dihedral, up to dropping finitely many such primes, such a Galois extension $F_p/\mathbb{Q}_p$ can be lifted to a G-extension $F/\mathbb{Q}$, that is, the field F_p is the completion of F at p; see [18, Theorem 1.1]. In particular, the extension $F/\mathbb{Q}$ cannot occur as a specialization of $E/\mathbb{Q}(T)$.

Now, assume $G = S_3$. One easily checks that the ramification indices of the branch points of $E/\mathbb{Q}(T)$ are 2, 2, and 3, i.e., the inertia groups of the branch points are generated by a 2-cycle, a 2-cycle, and a 3-cycle. Let C_2 (respectively, C_3) be the conjugacy class in S_3 of the 2-cycles (respectively, of the 3-cycles). If the first two branch points are not $\mathbb{Q}$-rational, then, by (a), the quadratic subextension of $E/\mathbb{Q}(T)$ is not parametric. Since every quadratic number field embeds into an S_3-extension of $\mathbb{Q}$, this implies that $E/\mathbb{Q}(T)$ cannot be parametric either. So all three branch points can be assumed to be $\mathbb{Q}$-rational. Since (C_2, C_2, C_3) is a rigid triple of rational conjugacy classes of the centerless group S_3, there is only one regular S_3-extension of $\mathbb{Q}(T)$ with 3 $\mathbb{Q}$-rational branch points, up to change of variable. See, e.g., [38, Chapters 7 and 8] for more details. Let E' be the splitting field of $Y^3 + TY + T$ over $\mathbb{Q}(T)$. Since $E'/\mathbb{Q}(T)$ is a regular S_3-extension and its set of branch points is $\{0, \infty, -27/4\}$,it is the only regular S_3-extension of $\mathbb{Q}(T)$ with 3

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

$\mathbb{Q}$-rational branch points. As this extension is known to be generic (see, e.g., [25, § 2.1] or [17, Proposition 5.3]), we are done. □

Remark A.2. (a) We do not know whether the equivalence between '$E/\mathbb{Q}(T)$ parametric' and '$E/\mathbb{Q}(T)$ generic' holds without assuming the number of branch points is at most 3 and every finite group occurs as a Galois group over $\mathbb{Q}$.[16] Note that this result would imply that only the subgroups of S_3 have a parametric extension over $\mathbb{Q}$, since this last conclusion holds with 'parametric' replaced by 'generic'; see [25] and [17, Corollary 5.4]. (b) Given a finite group G, every regular G-extension of $\mathbb{Q}(T)$ of genus 0 has at most 3 branch points (by the Riemann–Hurwitz formula). Hence, Theorem A.1 shows that, under a positive answer to the inverse Galois problem, any given regular G-extension $E/\mathbb{Q}(T)$ of genus 0 which is parametric is generic. This weaker conclusion actually holds unconditionally.

Indeed, denote the number of branch points of $E/\mathbb{Q}(T)$ by r. Since $E/\mathbb{Q}(T)$ has genus 0, one of these conditions holds:

(1) G is cyclic of order $n \in \{2, 3, 4, 6\}$ and $r = 2$;

(2) G is dihedral of order $2n$ with $n \in \{2, 3, 4, 6\}$ and $r = 3$;

(3) $G = A_4$ and $r = 3$;

(4) $G = S_4$ and $r = 3$.[17]

If (1) holds, then $E/\mathbb{Q}(T)$ is generic if it is parametric, by Theorem A.1(a). If (2) (with $n \neq 3$) or (3) or (4) holds, then G has a non-cyclic abelian subgroup. One then shows as in the proof of Theorem A.1(b) that $E/\mathbb{Q}(T)$ is not parametric. Finally, if (2) holds with $n = 3$, then one sees as above that $E/\mathbb{Q}(T)$ is non-parametric or E is the splitting field over $\mathbb{Q}(T)$ of $Y^3 + TY + T$, up to change of variable.

Appendix B. Twists of superelliptic curves without rational points

B.1. Proof of Theorem 4.2

Let S' be the subset of $\mathcal{P}(n, N)$ consisting of all polynomials $P(T)$ satisfying this condition:

(∗) *$P(T)$ is separable and $\bigcup_{j=1}^{N} \mathrm{Gal}(L/\mathbb{Q}(t_j)) \neq \mathrm{Gal}(L/\mathbb{Q})$, where $t_1, \ldots, t_N$ and L are the roots and the splitting field over $\mathbb{Q}$ of $P(T)$, respectively.*

[16] Over larger number fields k, examples of regular G-extensions of $k(T)$ which are parametric but not generic are known, under the Birch and Swinnerton-Dyer conjecture. See [17, § 5.4] for more details.

[17] Indeed, since $E/\mathbb{Q}(T)$ is of genus 0, the group G embeds into $\mathrm{PGL}_2(\overline{\mathbb{Q}})$ and, by [36, Chapter I, Theorem 6.2], we get that one of the following five conditions holds: (1) G is cyclic and $r = 2$, (2) G is dihedral and $r = 3$, (3) $G = A_4$ and $r = 3$, (4) $G = S_4$ and $r = 3$, and (5) $G = A_5$ and $r = 3$. First, as in the proof of Theorem A.1(a), (1) can happen only if $n \in \{2, 3, 4, 6\}$, by the Branch Cycle Lemma. Now, (5) cannot happen. Indeed, the ramification indices of the branch points of $E/\mathbb{Q}(T)$ should be 2, 3, and 5 (see [36, Chapter I, Theorem 6.2]); thus violating the Branch Cycle Lemma since A_5 has two conjugate conjugacy classes of 5-cycles. Finally, in the case of dihedral groups, similar arguments show that (2) can happen only if $n \in \{2, 3, 4, 6\}$.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

First, an element $P(T)$ of $\mathcal{P}(n, N)$ is in S' if its Galois group over $\mathbb{Q}$, viewed as a permutation group of the roots, is isomorphic to S_N. One then shows as in the proof of Lemma 4.4 that the estimate (4.1) holds. Moreover, if $P(T) \in S'$, then, as in the proof of Lemma 4.6, there is a set $\mathcal{S}$ of prime numbers of positive density α such that no prime number $p \in \mathcal{S}$ is a prime divisor of $P(T)$.[18] Set $P(T) = a_0 + a_1 T + \cdots + a_N T^N$. As condition $(*)$ holds, $P(T)$ has no root in $\mathbb{Q}$. In particular, one has $a_0 \neq 0$. Up to dropping finitely many prime numbers, we may assume $v_p(a_0) = 0$ and $v_p(a_N) = 0$ for each prime number $p \in \mathcal{S}$.

Next, let d be an arbitrary n-free number which is divisible by at least one prime number $p \in \mathcal{S}$. Suppose $C_{d \cdot P(T)}$ has a (non-trivial) $\mathbb{Q}$-rational point $[y : t : z]$. If $z = 0$, one has

$$y^n = d \cdot a_N t^N. \tag{B 1}$$

In particular, one has $y \neq 0$ and $t \neq 0$. By the condition $v_p(a_N) = 0$ and (B 1), one has

$$n \cdot v_p(y) = v_p(d) + N \cdot v_p(t).$$

As n divides N, we get that n divides $v_p(d)$, which cannot happen. One then has $z \neq 0$. Up to replacing (y, t, z) by $(y/z^{N/n}, t/z, 1)$, we may assume $z = 1$. Hence, one has

$$y^n = d \cdot P(t). \tag{B 2}$$

If $v_p(P(t)) = 0$, (B 2) gives $n \cdot v_p(y) = v_p(d)$. Then $n | v_p(d)$, which cannot happen. Hence,

$$v_p(P(t)) \neq 0. \tag{B 3}$$

If $t = 0$, (B 2) gives $y^n = d \cdot a_0$. Since $v_p(a_0) = 0$, we get $n | v_p(d)$, a contradiction. Hence, $t \neq 0$. If $v_p(t) \geqslant 0$, then $v_p(P(t)) \geqslant 0$. By (B 3), this yields $v_p(P(t)) > 0$. Then p is a prime divisor of $P(T)$, a contradiction. Hence, $v_p(t) < 0$. Using that $v_p(a_N) = 0$, we get

$$v_p(P(t)) = v_p(t^N) = N \cdot v_p(t). \tag{B 4}$$

Combining (B 2) and (B 4) then provides $n \cdot v_p(y) = v_p(d) + N \cdot v_p(t)$. As $n | N$, we get that n divides $v_p(d)$, which cannot happen. One then has $C_{d \cdot P(T)}(\mathbb{Q}) = \emptyset$.

Finally, let $\mathcal{N}_{\mathcal{S}}$ be the set of all integers d which are divisible by no prime number in $\mathcal{S}$. By the above, one has $|\mathcal{N}_n(P(T), x)| \leqslant |\mathcal{N}_{\mathcal{S}} \cap [\![-x, x]\!]|$ for every positive integer x. Moreover, by [37, théorème 2.3], one has $|\mathcal{N}_{\mathcal{S}} \cap [\![-x, x]\!]| \sim \beta \cdot x \cdot \log^{-\alpha}(x)$ as x tends to ∞ (for some constant $\beta > 0$). Conclude that (4.2) and the desired density zero conclusion hold (as $\mathcal{N}_n$ has positive density), thus ending the proof of Theorem 4.2.

B.2. Variants of Theorem 4.2

As before, we refer to § 2.1 and § 2.3.3 for the definitions of the sets $\mathcal{P}(n, N)$, $\mathcal{P}(n, N, H)$, $\mathcal{N}_n$, $\mathcal{N}_n(P(T))$, $\mathcal{N}_n(x)$, and $\mathcal{N}_n(P(T), x)$.

[18] The definition of a prime divisor of a polynomial is recalled in the proof of Lemma 4.6.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

Proposition B.1. *Let n and N be integers such that $n \geqslant 2$, n is not a prime number, and $N \geqslant 5$. Let $P(T)$ be a separable polynomial in $\mathcal{P}(n, N)$ and let n_1 be the smallest prime divisor of n. Then there exists a positive constant c such that*

$$|\mathcal{N}_n(x)| - |\mathcal{N}_n(P(T), x)| \geqslant c \cdot x^{1/n_1}, \quad x \to \infty. \tag{B 5}$$

Proof. For $\alpha \in \mathcal{N}_2$, consider the n-free integer $d_\alpha = 2\alpha^{n_1}$ (note that $n_1 \notin \{n-1, n\}$ as n is not a prime and $n_1 \mid n$). We show below that there are only finitely many squarefree integers α such that the twisted superelliptic curve $C_{d_\alpha \cdot P(T)} : y^n = d_\alpha \cdot P(t)$ has a non-trivial $\mathbb{Q}$-rational point, thus providing (B 5).

Set $n = n_1 n_2$. Given $\alpha \in \mathcal{N}_2$, let $[y_\alpha : t_\alpha : z_\alpha]$ be a non-trivial $\mathbb{Q}$-rational point on $C_{d_\alpha \cdot P(T)}$. If $z_\alpha \neq 0$, then $[y_\alpha : t_\alpha : z_\alpha] = [y'_\alpha : t_\alpha / z_\alpha : 1]$, where y'_α is y_α divided by some power of z_α. One may then assume $z_\alpha = 0$ or $z_\alpha = 1$. In each case, one sees that $[y_\alpha^{n_2}/\alpha : t_\alpha : z_\alpha]$ is a non-trivial $\mathbb{Q}$-rational point on $C_{2 \cdot P(T)} : y^{n_1} = 2 \cdot P(t)$.

Now, given $\alpha \neq \beta \in \mathcal{N}_2$, suppose $[y_\alpha^{n_2}/\alpha : t_\alpha : z_\alpha] = [y_\beta^{n_2}/\beta : t_\beta : z_\beta]$. First, if $z_\alpha = z_\beta = 0$ (which implies that n divides N), then $y_\alpha^{n_2}/\alpha = \lambda^{N/n_1} y_\beta^{n_2}/\beta$ for some $\lambda \in \mathbb{Q} \setminus \{0\}$. Since n_2 divides N/n_1, this implies that $\alpha/\beta \neq 1$ is a n_2th power in $\mathbb{Q}$, which cannot happen. Now, if $z_\alpha = z_\beta = 1$, then $y_\alpha^{n_2}/\alpha = y_\beta^{n_2}/\beta$ and one gets a contradiction as in the first case.

Hence, if $C_{d_\alpha \cdot P(T)}$ has a non-trivial $\mathbb{Q}$-rational point for infinitely many $\alpha \in \mathcal{N}_2$, then $|C_{2 \cdot P(T)}(\mathbb{Q})| = \infty$. However, due to our assumptions that $P(T)$ is separable and $N \geqslant 5$, this superelliptic curve has genus at least 2 and Faltings' theorem then yields a contradiction. □

Proposition B.2. *Let N be a positive integer such that $N \equiv 3 \pmod 4$. Then there exists a subset S of $\mathcal{P}(2, N)$ which satisfies the following two conclusions.*

(a) *One has*

$$\frac{|S \cap \mathcal{P}(2, N, H)|}{|\mathcal{P}(2, N, H)|} = 1 - O\left(\frac{\log(H)}{\sqrt{H}}\right), \quad H \to \infty. \tag{B 6}$$

In particular, the set S has density 1.

(b) *The complement $\mathcal{N}_2 \setminus \mathcal{N}_2(P(T))$ is infinite for every polynomial $P(T) \in S$.*

Proof. See, e.g., the survey paper [39] for more details on the terminology we use below.

First, given $N \geqslant 1$ odd and a polynomial $P(T) \in \mathcal{P}(2, N)$, suppose there exists an infinite subset $\mathcal{S}$ of $\mathcal{N}_2$ such that the 2-Selmer group $\mathrm{Sel}_2(J(C_{d \cdot P(T)}))$ of the Jacobian $J(C_{d \cdot P(T)})$ of $C_{d \cdot P(T)} : y^2 = d \cdot P(t)$ is trivial for each $d \in \mathcal{S}$. For such a d, denote the Mordell–Weil rank of $J(C_{d \cdot P(T)})$ by r_d and the 2-torsion subgroup of $J(C_{d \cdot P(T)})(\mathbb{Q})$ by $J(C_{d \cdot P(T)})(\mathbb{Q})[2]$. Then

$$r_d \leqslant \dim_{\mathbb{F}_2} \mathrm{Sel}_2(J(C_{d \cdot P(T)})) - \dim_{\mathbb{F}_2} J(C_{d \cdot P(T)})(\mathbb{Q})[2] = -\dim_{\mathbb{F}_2} J(C_{d \cdot P(T)})(\mathbb{Q})[2].$$

See [39, § 3] for more details. Consequently, one has $r_d = \dim_{\mathbb{F}_2} J(C_{d \cdot P(T)})(\mathbb{Q})[2] = 0$. Moreover, up to dropping finitely many elements of $\mathcal{S}$, we may assume that

$$J(C_{d \cdot P(T)})(\mathbb{Q})[\mathrm{tors}] = J(C_{d \cdot P(T)})(\mathbb{Q})[2]$$

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

for each $d \in \mathcal{S}$, with $J(C_{d\cdot P(T)})(\mathbb{Q})[\mathrm{tors}]$ the set of torsion points of $J(C_{d\cdot P(T)})(\mathbb{Q})$. We refer to [4, Theorem 2.1] for more details. Hence, every $\mathbb{Q}$-rational point on $J(C_{d\cdot P(T)})$ is of order 1. In particular, for each $d \in \mathcal{S}$, the set $C_{d\cdot P(T)}(\mathbb{Q})$ is reduced to $[0:1:0]$.

Now, given N such that $N \equiv 3 \pmod 4$, consider the subset S of $\mathcal{P}(2, N)$ defined by the extra condition that the Galois group over $\mathbb{Q}$ is S_N or A_N. As in the proof of Theorem 4.2, one shows that the set S fulfills (B 6). Moreover, by [42, Theorem 3], for every $P(T) \in S$, there exist infinitely many $d \in \mathcal{N}_2$ such that the 2-Selmer group of the Jacobian of $C_{d\cdot P(T)}$ is trivial. It then remains to apply the first part of the proof to conclude. □

Remark B.3. (a) If $N = 3$, one can take $S = \mathcal{P}(2, N)$. Indeed, for $P(T) \in \mathcal{P}(2, 3)$, it is known that the Mordell–Weil rank of $C_{d\cdot P(T)}$ is 0 for infinitely many $d \in \mathcal{N}_2$, and that, for all but finitely many $d \in \mathcal{N}_2$, every torsion $\mathbb{Q}$-rational point on $C_{d\cdot P(T)}$ is trivial. See, e.g., [10] and [22, Proposition 1] for more details and references. Moreover, for some $P(T) \in \mathcal{P}(2, 3)$, the density of $\mathcal{N}_2 \setminus \mathcal{N}_2(P(T))$ is known to be positive (unconditionally). See [10] for references.
(b) Given $r \geqslant 2$ even, the density of the subset $\mathcal{E}^\infty(r)$ of $\mathcal{E}(r)$ (see § 2.4), which consists of all regular $\mathbb{Z}/2\mathbb{Z}$-extensions of $\mathbb{Q}(T)$ with exactly r branch points and with ∞ as a branch point, is easily seen to be 0 by Proposition 2.4. Consequently, elements of $\mathcal{E}^\infty(r)$ which are contained in a set S as in Theorem 4.1 are only a negligible part of S. However, if r is divisible by 4, Proposition B.2 shows that there is a density 1 subset S of $\mathcal{E}^\infty(r)$ such that there exist infinitely many quadratic extensions of $\mathbb{Q}$ which do not belong to the specialization set of a given extension of $\mathbb{Q}(T)$ in S. The precise statement and the proof, which is very similar to that of Theorem 4.1 under Theorem 4.2, are left to the interested reader.

References

1. S. Beckmann, On extensions of number fields obtained by specializing branched coverings, *J. Reine Angew. Math.* **419** (1991), 27–53.
2. M. Bhargava, Mass formulae for extensions of local fields, and conjectures on the density of number field discriminants, *Int. Math. Res. Not. IMRN* **2007**(17) (2007), Art. ID rnm052, 20 pp.
3. M. Bhargava and M. Wood, The density of discriminants of S_3-sextic number fields, *Proc. Amer. Math. Soc.* **136**(5) (2008), 1581–1587.
4. A. Bourdon, P. Clark and J. Stankewicz, Torsion points on CM elliptic curves over real number fields, *Trans. Amer. Math. Soc.* **369**(12) (2017), 8457–8496.
5. D. Byeon, Ranks of quadratic twists of an elliptic curve, *Acta Arith.* **114**(4) (2004), 391–396.
6. D. Byeon, D. Jeon and C. H. Kim, Rank-one quadratic twists of an infinite family of elliptic curves, *J. Reine Angew. Math.* **633** (2009), 67–76.
7. L. Caporaso, J. Harris and B. C. Mazur, Uniformity of rational points, *J. Amer. Math. Soc.* **10**(1) (1997), 1–35.
8. P. Clark and L. Watson, ABC and the Hasse principle for quadratic twists of hyperelliptic curves, *C. R. Math. Acad. Sci. Paris* **356**(9) (2018), 911–915.
9. S. D. Cohen, The distribution of Galois groups and Hilbert's irreducibility theorem, *Proc. Lond. Math. Soc. (3)* **43**(2) (1981), 227–250.

https://doi.org/10.1017/S1474748019000537 Published online by Cambridge University Press

10. A. Dabrowski, On the proportion of rank 0 twists of elliptic curves, *C. R. Math. Acad. Sci. Paris* **346**(9–10) (2008), 483–486.
11. P. Dèbes, Galois covers with prescribed fibers: the Beckmann–Black problem, *Ann. Sc. Norm. Super. Pisa Cl. Sci. (4)* **28**(2) (1999), 273–286.
12. P. Dèbes, *Arithmétique des revêtements de la droite*, Lecture notes, (2009). At http://math.univ-lille1.fr/∼pde/ens.html.
13. P. Dèbes, On the Malle conjecture and the self-twisted cover, *Israel J. Math.* **218**(1) (2017), 101–131.
14. P. Dèbes, Groups with no parametric Galois realizations, *Ann. Sci. Éc. Norm. Supér. (4)* **51**(1) (2018), 143–179.
15. P. Dèbes and M. D. Fried, Rigidity and real residue class fields, *Acta Arith.* **56**(4) (1990), 291–323.
16. P. Dèbes and N. Ghazi, Galois covers and the Hilbert–Grunwald property, *Ann. Inst. Fourier (Grenoble)* **62**(3) (2012), 989–1013.
17. P. Dèbes, J. König, F. Legrand and D. Neftin, Rational pullbacks of Galois covers. *Manuscript*, 2018. arXiv:1807.01937.
18. C. Demarche, G. L. Arteche and D. Neftin, The Grunwald problem and approximation properties for homogeneous spaces, *Ann. Inst. Fourier (Grenoble)* **67**(3) (2017), 1009–1033.
19. M. D. Fried, Fields of definition of function fields and Hurwitz families-groups as Galois groups, *Comm. Algebra* **5**(1) (1977), 17–82.
20. M. D. Fried and M. Jarden, *Field Arithmetic*, third edition, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], Volume 11 (Springer-Verlag, Berlin, 2008). Revised by Jarden. xxiv + 792 pp.
21. I. M. Gel'fand, M. M. Kapranov and A. V. Zelevinsky, *Discriminants, Resultants, and Multidimensional Determinants*, Mathematics: Theory & Applications (Birkhäuser Boston, Inc., Boston, MA, 1994). x+523 pp.
22. F. Q. Gouvêa and B. C. Mazur, The square-free sieve and the rank of elliptic curves, *J. Amer. Math. Soc.* **4**(1) (1991), 1–23.
23. A. Granville, ABC allows us to count squarefrees, *Int. Math. Res. Not. IMRN* **19** (1998), 991–1009.
24. A. Granville, Rational and integral points on quadratic twists of a given hyperelliptic curve, *Int. Math. Res. Not. IMRN* **2007**(8) (2007), Art. ID 027, 24 pp.
25. C. U. Jensen, A. Ledet and N. Yui, *Generic polynomials. Constructive Aspects of the Inverse Galois Problem*, Mathematical Sciences Research Institute Publications, Volume 45 (Cambridge University Press, 2002). x+258 pp.
26. J. König and F. Legrand, Non-parametric sets of regular realizations over number fields, *J. Algebra* **497** (2018), 302–336.
27. J. König, F. Legrand and D. Neftin, On the local behavior of specializations of function field extensions, *Int. Math. Res. Not. IMRN* **2019**(9) (2019), 2951–2980.
28. J. Klüners, Asymptotics of number fields and the Cohen–Lenstra heuristics, *J. Théor. Nombres Bordeaux* **18**(3) (2006), 607–615.
29. J. Klüners and G. Malle, A database for field extensions of the rationals, *LMS J. Comput. Math.* **4** (2001), 182–196.
30. J. Klüners and G. Malle, Counting nilpotent Galois extensions, *J. Reine Angew. Math.* **572** (2004), 1–26.
31. J. König, Non-parametricity of rational translates of regular Galois extensions, *Acta Arith.* **179**(3) (2017), 267–275.
32. F. Legrand, Parametric Galois extensions, *J. Algebra* **422** (2015), 187–222.

33. F. Legrand, Specialization results and ramification conditions, *Israel J. Math.* **214**(2) (2016), 621–650.
34. F. Legrand, Twists of superelliptic curves without rational points, *Int. Math. Res. Not. IMRN* **2018**(4) (2018), 1153–1176.
35. G. Malle, On the distribution of Galois groups, *J. Number Theory* **92**(2) (2002), 315–329.
36. G. Malle and B. H. Matzat, *Inverse Galois Theory*, second edition, Springer Monographs in Mathematics (Springer, Berlin, 2018). xvii+532 pp.
37. J.-P. Serre, Divisibilité de certaines fonctions arithmétiques, *Enseign. Math. (2)* **22**(3–4) (1976), 227–260.
38. J.-P. Serre, *Topics in Galois Theory*, Research Notes in Mathematics, Volume 1 (Jones and Bartlett Publishers, Boston, MA, 1992). Lecture notes prepared by Henri Darmon [Henri Darmon]. With a foreword by Darmon and the author. xvi+117 pp.
39. M. Stoll, Rational points on hyperelliptic curves: recent developments, in *Computeralgebra-Rundbrief 54* (Fachgruppe Computeralgebra, Berlin, 2014).
40. V. Vatsal, Rank-one twists of a certain elliptic curve, *Math. Ann.* **311**(4) (1998), 791–794.
41. H. Völklein, *Groups as Galois Groups. An Introduction*, Cambridge Studies in Advanced Mathematics, Volume 53 (Cambridge University Press, Cambridge, 1996). xviii+248 pp.
42. M. Yu, Selmer ranks of twists of hyperelliptic curves and superelliptic curves, *J. Number Theory* **160** (2016), 148–185.