THE GEOMETRIC BUNYAKOWSKY PROBLEM

EMMANUEL KOWALSKI

Abstract. We introduce a problem of algebraic geometry that can be interpreted as a geometric version of the Bunyakowsky problem of representing primes by values of an integral polynomial. We solve the simplest aspect of this geometric problem, which leads in particular to a "large finite field" statement that generalizes results concerning the Bunyakowsky Problem for polynomials of a fixed degree over large finite fields, due in particular to Entin.

1. The Bunyakowsky problem

The original *Bunyakowsky Problem* concerns the prime values $p = \mathrm{F}(n)$ taken by a fixed (irreducible and primitive) polynomial $\mathrm{F} \in \mathbf{Z}[\mathrm{X}]$ for integer values of n. It is a major open problem of analytic number theory to prove that this set of primes is infinite for any polynomial with degree $\geqslant 2$. On the other hand, in the context of polynomials over finite fields, much progress has been made in the analogue problem when the size of the base field grows.

Our goal in this note is to give a geometric interpretation of this version of the Bunyakowsky Problem. This leads to a rather natural and interesting generalization, that can be seen as a question of independent interest in algebraic geometry. We begin this section by introducing this problem, and in the next one, we will make precise the link with the original conjecture of Bunyakowsky.

Let k be a field, and C/k a smooth projective geometrically connected curve of genus $g \geqslant 0$ (for instance, the projective line over a finite field). For any effective divisor D on C, defined over k (for instance, the divisor $d(\infty)$), we wish to consider functions f on C with poles only at the points in the support of D, with poles of order corresponding to their multiplicity in D (for instance, polynomials of degree exactly d), and with distinct zeros (which would be squarefree polynomials of degree d in the previous example).

These functions form an algebraic family if $\deg(\mathrm{D}) \geqslant 2g+1$, which we assume from now on: there exists in that case a Riemann-Roch variety $\mathcal{H}_{\mathrm{D}}$ over k such that, for any field extension K/k, the points in $\mathcal{H}_{\mathrm{D}}(\mathrm{K})$ "are" the rational functions $f : \mathrm{C} \longrightarrow \mathbf{P}^1$, defined over K, with divisor of poles exactly D. The zeros of these functions are therefore all contained in the affine curve U which is the complement of the support of D in C. The algebraic variety $\mathcal{H}_{\mathrm{D}}$ is isomorphic to the affine space $\mathbf{A}^d$ where $d = \deg(\mathrm{D}) + 1 - g \geqslant g+2$ (see, e.g., [11, Lemma 5.0.6], where $\mathcal{H}_{\mathrm{D}}$ is the closure of the space $\mathrm{Fct}(\mathrm{C}, \deg(\mathrm{D}), \mathrm{D}, \emptyset)$, which contains functions with $\deg(\mathrm{D})$ distinct zeros, a condition we do not need to impose).

Key words and phrases. Schinzel Hypothesis, Bunyakowsky's conjecture, algebraic curves, Lefschetz pencils, Galois groups, function field arithmetic.

Partially supported by a DFG-SNF lead agency program grant (grant 200021L_153647).

For any function $f\colon \mathrm{U} \to \mathbf{A}^1$ on U, we denote by $\Gamma_f \subset \mathrm{U} \times \mathbf{A}^1$ the graph of f. Now, let $\mathrm{S} \subset \mathrm{U} \times \mathbf{A}^1$ be a fixed algebraic curve defined over k. We form the subscheme

$$\mathcal{Z}_{\mathrm{D}} \subset \mathcal{H}_{\mathrm{D}} \times \mathrm{U} \times \mathbf{A}^1$$

defined by

$$\begin{aligned}\mathcal{Z}_{\mathrm{D}} &= \{(f, x, y) \in \mathcal{H}_{\mathrm{D}} \times \mathrm{S} \mid (x, y) \in \mathrm{S} \cap \Gamma_f\} \\ &= \{(f, x, y) \in \mathcal{H}_{\mathrm{D}} \times \mathrm{U} \times \mathbf{A}^1 \mid (x, y) \in \mathrm{S} \text{ and } y = f(x)\},\end{aligned}$$

and the first projection $\mathcal{Z}_{\mathrm{D}} \longrightarrow \mathcal{H}_{\mathrm{D}}$. Thus the fiber of π_{D} over f is the intersection $\Gamma_f \cap \mathrm{S}$ of the graph of f with the fixed curve S. Restricting π_{D} to a suitable open dense subset $\mathcal{H}_{\mathrm{D,S}}$ of $\mathcal{H}_{\mathrm{D}}$, the induced projection

$$\pi_{\mathrm{D}}\colon \mathcal{Z}_{\mathrm{D,S}} \longrightarrow \mathcal{H}_{\mathrm{D,S}}$$

is finite étale (we will check this in detail in Lemma 10 below). We call this map the *Bunyakowsky covering* associated to $(\mathrm{C}, \mathrm{D}, \mathrm{S})$.

Definition (Bunyakowsky group)**.** The *Bunyakowsky group* of $\mathcal{Z}_{\mathrm{D}}$ over k is the geometric Galois group of the Galois closure of the covering $\mathcal{Z}_{\mathrm{D,S}} \longrightarrow \mathcal{H}_{\mathrm{D,S}}$, restricted to an open subset where it is an étale covering. Equivalently, for any prime ℓ different from the characteristic of k, it is the geometric monodromy group of the constructible $\bar{\mathbf{Q}}_\ell$-sheaf $\pi_{\mathrm{D},*}\bar{\mathbf{Q}}_\ell$, on any dense open subset of $\mathcal{H}_{\mathrm{D}}$ where it is lisse.

We will be interested in the following problem (the next section explains the choice of terminology):

Problem (Geometric Bunyakowsky problem)**.** What is the Bunyakowsky group of D and S? More generally, what are the geometric and topological properties of the Bunyakowsky covering $\mathcal{Z}_{\mathrm{D,S}} \longrightarrow \mathcal{H}_{\mathrm{D,S}}$?

In this paper, we answer the first question in fair generality.

Theorem 1. *Let k be a field of odd characteristic. Let C/k be a smooth projective algebraic curve of genus $g \geqslant 0$, let D be an effective k-rational divisor on C of degree $\geqslant 2g+1$, and let U be the open complement of the support of D. Let $\mathrm{S} \subset \mathrm{U} \times \mathbf{A}^1$ be a smooth curve defined over k. Assume that S is smooth, geometrically irreducible, and is not contained in a vertical line $\{x\} \times \mathbf{A}^1$ for some $x \in \mathrm{U}$. Let $\tilde{\mathrm{S}}$ be the smooth projective model of S. Let $\pi_{\mathrm{D}}\colon \mathcal{Z}_{\mathrm{D,S}} \to \mathcal{H}_{\mathrm{D,S}}$ be the associated Bunyakowsky covering.*

(1) For f in a dense open subset of $\mathcal{H}_{\mathrm{D}}$, the polar divisor of the function $(x, y) \mapsto y - f(x)$ on $\tilde{\mathrm{S}}$ is a fixed effective divisor E on $\tilde{\mathrm{S}}$, of degree $n \geqslant 1$, and the degree of π_{D} is equal to n.

(2) Assume that $\deg(\mathrm{D}) \geqslant 2g+3$ and that one of the following conditions holds:

- *the divisor E is coprime to the characteristic p of k, in the sense that all multiplicities of points in the support of E are coprime to p;*
- *or n is a prime number;*
- *or the genus of $\tilde{\mathrm{S}}$ is $\geqslant 1$ and $p \nmid n$.*

Then the Bunyakowsky group is maximal, i.e., it is isomorphic to $\mathfrak{S}_n$.

The result is particularly satisfactory in characteristic 0, since the condition on E is then vacuous. If k has characteristic $p > 0$, then the first condition concerning E is satisfied if p is "large enough" compared with the degree of D and the genus of $\tilde{\mathrm{S}}$. It is also true, of

course, in many other cases, and the condition can be efficiently checked in concrete cases. The last condition is true in many cases, for a fixed S (of genus $\geqslant 1$), if the support of D is fixed and the multiplicities of each point in its support increase, provided that the degree of the projection $\mathrm{S} \to \mathrm{U}$ is not divisible by p.

We will first discuss in the next section the arithmetic interpretation of the Bunyakowsky group, and explain the terminology. This will show that, when $\mathrm{C} = \mathbf{P}^1$ and D is supported at infinity, this theorem reduces (in most cases) to a theorem of Entin [7]. In Section 3, we consider separately the special case where $\mathrm{S} = \mathrm{U} \times \{0\}$ – in this case, the result is due to Katz [11] and has independent interest, generalizing the classical property that the "generic" Galois group of the splitting field of a polynomial is the symmetric group. The proof of the general case of the theorem is then found in Section 4. The main idea is an adaptation of *another* argument of Katz in [11], using Lefschetz pencils on curves, and techniques of Katz and Rains [13].

Remark 2. Our geometric Bunyakowsky problem admits many variants, including higher-dimensional generalizations. In fact, it can also be seen as a *specialization* of the very general constructions of "twists" by Katz in [11] and [13]. We illustrate this with one example related to twists of elliptic curves over functions fields. Consider a field k and let $\mathrm{C} = \mathbf{P}^1$ and $\mathrm{D} = d(\infty)$. Let W be the hypersurface

$$\mathrm{W} = \{(x, y, t, d) \in \mathbf{A}^4 \mid dy^2 = x(x-1)(x-t)\} \subset \mathbf{A}^4.$$

Form then the algebraic variety

$$\mathrm{V}_\mathrm{D} = \{(x, y, f, t) \in \mathbf{A}^2 \times \mathcal{H}_\mathrm{D} \times \mathrm{U} \mid (x, y, t, f(t)) \in \mathrm{W}\}$$

with its natural projection $\pi\colon \mathrm{V}_\mathrm{D} \to \mathcal{H}_\mathrm{D}$. Then the fiber over $f \in \mathcal{H}_\mathrm{D}(k)$ is, on the one hand, the intersection of the hypersurface W with $\mathbf{A}^2 \times \Gamma_f$, and on the other hand, it "is" the twisted Legendre curve

$$f(t)y^2 = x(x-1)(x-t)$$

as an elliptic curve over $k(t)$. The study of the (geometric) monodromy group of the sheaf $\mathrm{R}^1\pi_!\bar{\mathbf{Q}}_\ell$ is then the study of the variation of the L-functions of these elliptic curves.

Note however that the techniques developped by Katz in the books we cited do not directly address our Bunyakowsky problem, since they are tailored to the computation of monodromy groups that are "large" linear algebraic groups.

Acknowledgments. We would like to acknowledge the influence of A. Entin's work [7]. We also thank R. Pink for explaining some points of algebraic geometry and Z. Rudnick for his remarks and criticisms. Also thanks to L. Bary-Soroker for pointing out the paper [2] of Bender and Pollack.

2. Arithmetic interpretation

In this section, we will explain the terminology "Bunyakowsky group" and "Bunyakowsky problem".

We take $\mathrm{C} = \mathbf{P}^1$ over k and $\mathrm{D} = d(\infty)$ with $d \geqslant 1$. Then $\mathrm{U} = \mathbf{A}^1$ and $\mathcal{H}_\mathrm{D}$ "is" the space of polynomials of degree d (compare with [11, Remark 5.0.7]). It is isomorphic to $\mathbf{A}^{d+1}$ by mapping a polynomial to the sequence of its coefficients.

Assume that $\mathrm{S} \subset \mathbf{A}^1 \times \mathbf{A}^1$ is the affine curve given by the equation

$$\mathrm{S} \ : \ \mathrm{F}(x, y) = 0$$

where $\mathrm{F} \in k[\mathrm{X}, \mathrm{Y}]$ is a non-constant polynomial. Assume further that S is smooth and geometrically irreducible, so that we are in the context of the discussion in the introduction. The fiber of $\mathcal{Z}_{\mathrm{D}}$ over f in that case is the set

$$\{(x, y) \in \mathbf{A}^2 \ \mid \ y = f(x) \text{ and } \mathrm{F}(x, y) = 0\}.$$

Let A be the ring $\mathrm{A} = k[\mathrm{X}]$. Then this fiber can be identified via the first projection with

$$\{x \in \mathbf{A}^1 \ \mid \ \mathrm{F}(x, f(x)) = 0\} = \{x \in \mathbf{A}^1 \ \mid \ \mathrm{F}(f)(x) = 0\}$$

where we view F as a polynomial in $\mathrm{A}[\mathrm{Y}]$, and use the substitution $\mathrm{F}(f) \in \mathrm{A}[\mathrm{Y}] = k[\mathrm{X}, \mathrm{Y}]$. So the question is that of determining the Galois group $\mathrm{G}_{d,\mathrm{F}}$ of a "generic" polynomial of the form $\mathrm{F}(f)$ for $f \in k[\mathrm{X}]$ separable of degree d. Let n denote the degree of such a generic polynomial.

The relation with the function field version of Bunyakowsky's conjecture is revealed when we assume that k is a finite field. Let k_ν be the extension of k of degree $\nu \geqslant 1$ in $\bar{k}$. If the Galois group $\mathrm{G} = \mathrm{G}_{d,\mathrm{F}}$ as above is also the arithmetic Galois group (which is certainly true if G is the full symmetric group), then the Chebotarev density theorem applied to the covering π_{D} implies that for any conjugacy class $\mathrm{C} \subset \mathrm{G}_{d,\mathrm{F}}$, we have

$$\frac{1}{|k|^{\nu(d+1)}} |\{f \in \mathcal{H}_{\mathrm{D}}(k_\nu) \ \mid \ \mathrm{Fr}_{\mathrm{F}(f)} \in \mathrm{C}\}| \longrightarrow \frac{|\mathrm{C}|}{|\mathrm{G}_{d,\mathrm{F}}|}$$

as $\nu \to +\infty$, where $\mathrm{Fr}_{\mathrm{F}(f)}$ denotes the geometric Frobenius conjugacy class corresponding to the action of the Frobenius automorphism by permutation of the roots of $\mathrm{F}(f)$. Recall that this Frobenius action for a polynomial $g \in k_\nu[\mathrm{X}]$ of degree n is an n-cycle if and only if the polynomial g is irreducible. So, if the image of $\mathrm{G}_{d,\mathrm{F}}$ in $\mathfrak{S}_n$ contains n-cycles, then it follows that

$$\frac{1}{|k|^{\nu(d+1)}} |\{f \in \mathcal{H}_{\mathrm{D}}(k_\nu) \ \mid \ \mathrm{F}(f) \text{ is irreducible}\}| =$$

$$\frac{1}{|k|^{\nu(d+1)}} |\{f \in \mathcal{H}_{\mathrm{D}}(k_\nu) \ \mid \ \mathrm{Fr}_{\mathrm{F}(f)} \text{ is an } n\text{-cycle}\}| \longrightarrow \mu_{d,\mathrm{F}}$$

as $\nu \to +\infty$, where the constant $\mu_{d,\mathrm{F}} > 0$ is the proportion of elements of $\mathrm{G}_{d,\mathrm{F}}$ whosethe cycle decomposition in $\mathfrak{S}_n$ is an n-th cycle. This statement is a "large finite field" case of Bunyakowsky' conjecture for polynomials over function fields, and this explains our terminology for the general setting. (The reduction of irreducibility problems over finite fields to Galois-theoretic problems goes back at least to Cohen [4]).

In the particular case that the group $\mathrm{G}_{d,\mathrm{F}}$ is the full symmetric group $\mathfrak{S}_n$ (as in Theorem 1), we have $\mu_{d,\mathrm{F}} = 1/n$, the proportion of n-cycles in $\mathfrak{S}_n$.

This special case of the Bunyakowsky problem has been solved in many cases by Entin [7, Th. 1.1 and 1.4] (and in fact, in the greater generality involving a finite set of polynomials instead of the single polynomial F, which is known as the Schinzel or Bateman-Horn conjecture): if either F is monic and separable (as an element of $\mathrm{A}[\mathrm{Y}]$; Carmon has removed the requirement that F be monic in a recent preprint) or if p is "large enough" (in a precise sense depending on F). This followed a number of works by Hall [8], Pollack [16], Bary-Soroker [3], among others.

The precise result we obtain from (parts of) Theorem 1 is:

Corollary 3. *Let k be a finite field of odd characteristic p. Let $\mathrm{F} \in k[\mathrm{X}, \mathrm{Y}]$ be a polynomial such that the affine curve S defined by the equation $\mathrm{F}(x, y) = 0$ in $\mathbf{A}^1 \times \mathbf{A}^1$ is smooth, geometrically irreducible, and is not contained in a vertical line. Let $\tilde{\mathrm{S}}$ be the smooth projective model of S and denote its genus by $g \geqslant 0$.*

Let $d \geqslant 2g + 3$. Let n be the degree of the polynomial $\mathrm{F}(f)$ for a "generic" polynomial $f \in k[\mathrm{X}]$ of degree d. Assume that p does not divide n and that either n is a prime or $g \geqslant 1$.

For $\nu \geqslant 1$, we have

$$\frac{1}{|k|^{(d+1)\nu}} |\{f \in k_\nu[\mathrm{X}] \mid \mathrm{F}(f) \text{ is irreducible in } k_\nu[\mathrm{X}]\}| = \frac{1}{n} + \mathrm{O}(\mathrm{E}|k|^{-\nu/2}),$$

where the implied constant is absolute and

$$\mathrm{E} = 3 \cdot 2^{5+2n} \cdot (3 + (2 + 2n)\deg(\mathrm{F})(2n - 1))^{d+2n+3} \cdot n^{-1}.$$

The explicit error term is not particularly good, but it shows that it is possible to write down such a bound. (To the author's knowledge, the only previous explicit estimates in problems of this type is found in a paper of Bender and Pollack [2].) It is then possible to deduce, e.g., the existence of *some* irreducible specialization $\mathrm{F}(f)$ for a specific sufficiently large finite field k (with $\nu = 1$), even allowing the degree d to grow – very slowly, however: roughly speaking, since we have $n \ll d$ (for a fixed F) we obtain uniformity for

$$d \ll \frac{\log |k|}{\log\log |k|},$$

where the implied constant depends only on the degree of F.

Proof. With the weaker error term $\mathrm{O}(|k|^{-\nu/2})$, where the implied constant depends on F, this follows from Theorem 1 (applied to $\mathrm{C} = \mathbf{P}^1$ and $\mathrm{D} = d(\infty)$) and the Chebotarev Density Theorem as in [15, Th. 1] for instance.

To obtain the explicit error term, we denote by U the dense open subset of $\mathbf{A}^{d+1}$ corresponding to coefficients of polynomials f of degree d such that $\mathrm{F}(f)$ is squarefree of degree n. Then the covering π_{D} is étale (Lemma 10 below). Its Galois closure is the covering $\mathrm{V}_{\mathrm{D}} \to \mathrm{U}$ such that

$$\mathrm{V}_{\mathrm{D}} = \{(f, (x_1, y_1), \dots, (x_n, y_n)) \in \mathrm{U} \times \mathrm{S}^n \mid f(x_i) = y_i \text{ for } 1 \leqslant i \leqslant n\}. \tag{1}$$

We express the characteristic function f of n-cycles in $\mathfrak{S}_n$ in terms of irreducible characters: we have

$$f = \sum_{\varrho} \alpha(\varrho)\chi_\varrho,$$

where ϱ runs over the irreducible representations of $\mathfrak{S}_n$, with character χ_ϱ, which have Fourier coefficient $\alpha(\varrho)$ in the decomposition of f. We view ϱ as a $\bar{\mathbf{Q}}_\ell$-representation, acting on some $\bar{\mathbf{Q}}_\ell$-vector space V_ϱ.

We denote by $\mathrm{H}^i_c(\mathrm{U} \times \bar{k}, \varrho)$ the compactly supported étale cohomology groups with coefficient in the lisse sheaf $\varrho(\pi_{\mathrm{D},*}\bar{\mathbf{Q}}_\ell)$ on U corresponding to the homomorphism

$$\pi_1(\mathrm{U} \times \bar{k}, \bar{\eta}) \to \mathfrak{S}_n \to \mathrm{GL}(\mathrm{V}_\varrho).$$

Then, by the relation between irreducibility and Galois action recalled above, we obtain from [15, Proof of Th. 1] the relation

$$\frac{1}{|\mathrm{U}(k_\nu)|}|\{f \in \mathrm{U}(k_\nu) \mid \mathrm{F}(f) \text{ is irreducible in } k_\nu[\mathrm{X}]\}| = \frac{1}{n} + \mathrm{O}(\mathrm{E}_1|k|^{-\nu/2}), \tag{2}$$

where the implied constant is absolute, and

$$\mathrm{E}_1 = \sum_{\varrho} |\alpha(\varrho)| \sum_i \dim \mathrm{H}^i_c(\mathrm{U} \times \bar{k}, \varrho).$$

We recall that this relies ultimately on the general form of the Riemann Hypothesis over finite fields due to Deligne.

We have then

$$\mathrm{E}_1 \leqslant (\max_{\varrho} |\alpha(\varrho)|) \sum_{\varrho} \sum_i \dim \mathrm{H}^i_c(\mathrm{U} \times \bar{k}, \varrho).$$

From the explicit computation of the Fourier coefficients $\alpha(\varrho)$ (see, e.g, [1, Prop. 10]), we get

$$\max_{\varrho} |\alpha(\varrho)| = \frac{1}{n}.$$

Moreover, for any i and any representation ϱ, the space $\mathrm{H}^i_c(\mathrm{U} \times \bar{k}, \varrho)$ is isomorphic to the ϱ-isotypic component of $\mathrm{H}^i_c(\mathrm{V}_\mathrm{D} \otimes \bar{k}, \bar{\mathbf{Q}}_\ell)$. Hence

$$\mathrm{H}^i_c(\mathrm{V}_\mathrm{D} \otimes \bar{k}, \bar{\mathbf{Q}}_\ell) = \bigoplus_{\varrho} \mathrm{H}^i_c(\mathrm{U} \times \bar{k}, \varrho)$$

and

$$\mathrm{E}_1 \leqslant \frac{1}{n} \sum_i \dim \mathrm{H}^i_c(\mathrm{V}_\mathrm{D} \otimes \bar{k}, \bar{\mathbf{Q}}_\ell).$$

We proceed to estimate the sum of Betti numbers of V_D using the results of Katz [12]. For this purpose, we must represent V_D as a subvariety of $\mathbf{A}^\mathrm{N}$ defined by $\leqslant r$ equations of degree $\leqslant \delta$ for some parameters (N, r, δ).

We first express U in this way. Recall that U is the space of polynomials of degree d such that $\mathrm{F}(f)$ is squarefree of degree n. We represent U as a closed subscheme of $\mathbf{A}^{(d+1)+2}$ with extra variables to ensure that $\deg(\mathrm{F}(f)) = n$ and that $\mathrm{res}(\mathrm{F}(f), \mathrm{F}(f)') \neq 0$; in terms of the coefficients of f, the resultant $\mathrm{res}(\mathrm{F}(f), \mathrm{F}(f)')$ has degree $\leqslant \deg_\mathrm{Y}(\mathrm{F})(2n-1)$. So we can take parameters

$$(\mathrm{N}_1, r_1, \delta_1) = (d+3, 2, \deg_\mathrm{Y}(\mathrm{F})(2n-1))$$

to embed U in $\mathbf{A}^{\mathrm{N}_1}$ using at most r_1 equations of degree $\leqslant \delta_1$.

Recalling (1), we deduce that we can take parameters

$$(\mathrm{N}, r, \delta) = (\mathrm{N}_1 + 2n, r_1 + 2n, \max(\delta_1, \deg(\mathrm{F}), d))$$

(since $f(x_i) = y_i$ is a single equation of degree d, and $(x_i, y_i) \in \mathrm{S}$ is a single equation of degree $\deg(\mathrm{F})$). By [12, Cor. of Th. 1], it follows that

$$\sum_i \dim \mathrm{H}^i_c(\mathrm{V}_\mathrm{D} \otimes \bar{k}, \bar{\mathbf{Q}}_\ell) \leqslant 3 \cdot 2^{5+2n} \cdot (3 + (r_1 + 2n)\delta)^{\mathrm{N}_1 + 2n + 1}.$$

where $\delta = \max(d, \deg(\mathrm{F}), (2n-1)\deg_{\mathrm{Y}}(\mathrm{F})) \leqslant (2n-1)\deg(\mathrm{F})$. Comparing with (2), we obtain

$$\frac{1}{|\mathrm{U}(k_\nu)|}|\{f \in \mathrm{U}(k_\nu) \mid \mathrm{F}(f) \text{ is irreducible in } k_\nu[\mathrm{X}]\}| = \frac{1}{n} + \mathrm{O}(\mathrm{E}|k|^{-\nu/2}),$$

where E is the constant is the statement of the corollary, and the implied constant is absolute.

Moreover, we have similarly (by the point-counting formula)

$$|\mathrm{U}(k_\nu)| = |k|^{\nu(d+1)} + \mathrm{O}(\mathrm{E}_2|k|^{\nu(d+1/2)})$$

where the implied constant is absolute and

$$\mathrm{E}_2 = \sum_i \dim \mathrm{H}^i_c(\mathrm{U} \times \bar{k}, \bar{\mathbf{Q}}_\ell) \leqslant \mathrm{E}_1.$$

Hence the bound for U implies the result as stated. □

Remark 4. (1) For simplicity, we have not included the alternative of Theorem 1 where the divisor E is coprime to p.

(2) The degree n of the polynomial $\mathrm{F}(f)$ depends on the degree d of f and the precise monomials that occur in F. For instance, if d is large enough and the leading term of f with respect to Y is $a\mathrm{Y}^{\deg_{\mathrm{Y}}(\mathrm{F})}$, we will have $n = d\deg_{\mathrm{Y}}(\mathrm{F}) + \deg_{\mathrm{X}}(a)$.[1]

(3) One might also get bounds using the results of [14], which would be somewhat better, but the arguments there depend on tameness properties which are not a priori always true in this setting (they would be satisfied at least if $p > n$).

Example 5. Assume k has characteristic $\geqslant 5$. Consider $\mathrm{F}(\mathrm{X}, \mathrm{Y}) = \mathrm{Y}^2 - \mathrm{X}^3 - a\mathrm{X} - b$, with a and b such that the resulting cubic is smooth. Then the closure in $\mathbf{P}^2$ is smooth (an elliptic curve, with the single point at infinity, denoted 0, as origin). Then the degree of $\mathrm{F}(f)$ is 3 if $\deg(f) = 1$, and $2\deg(f)$ if $\deg(f) \geqslant 3$. Theorem 1 applies for $\deg(f) \geqslant 5$. However, experiments for $k = \mathbf{Q}$ (combined with Hilbert's irreducibility theorem) suggest that the result holds in that case for $\deg(f) \geqslant 1$, at least for most cubics.

Remark 6. The proof of Theorem 1 that we give hinges on two group-theoretic steps: (1) finding transpositions in the Bunyakowsky group; (2) showing that the Bunyakowsky group is primitive as a permutation group. In the context of this section, it may be noted that the second step could "almost" be replaced by the whimsical assumption that there exists *one* irreducible value of $\mathrm{F}(f)$ which is of the right degree n. Indeed, this will correspond to the existence of a cycle of length n in the Galois group, and although not all pairs of an n-cycle and a tranposition do generate $\mathfrak{S}_n$, this is often the case (and always so if n is prime). This fact suggests that the mechanisms at work seem very different than anything known or expected in the number field case (see also Remark 14).

3. Splitting fields of zeros of functions on curves

We come back to the general case of the Bunyakowsky problem for an arbitrary smooth projective curve C. We consider the special case $\mathrm{S} = \mathrm{U} \times \{0\} \subset \mathrm{U} \times \mathbf{A}^1$. The fiber of the projection π_{D} over $f \in \mathcal{H}_{\mathrm{D}}$ is then the scheme of zeros of the function f. The space $\mathcal{H}_{\mathrm{D}}$ is then the scheme $\mathrm{Fct}(\mathrm{C}, \deg(\mathrm{D}), \mathrm{D}, \emptyset)$ of Katz [11, Lemma 5.0.6].

[1] Note in particular, if $\deg_{\mathrm{Y}}(\mathrm{F})$ and $\deg_{\mathrm{X}}(a)$ are coprime, this will be prime infinitely often as d varies.

The following result of Katz computes the Bunyakowsky group in that case, in a stronger form than actually implied by the statement of Theorem 1 in that case.

Theorem 7 (Katz)**.** *Let k be a field. Let C/k be a smooth projective algebraic curve of genus $g \geqslant 0$, let D be an effective k-rational divisor on C of degree $\geqslant 2g+1$, and let U be the open complement of the support of D. Let $\mathrm{S} = \mathrm{U} \times \{0\}$. The Bunyakowsky group G is then isomorphic to $\mathfrak{S}_n$, where $n = \deg(\mathrm{D})$.*

Proof. We give two proofs, one by Katz from [11] and one based on results of Katz and Rains in [13], in this second case under the slightly more restrictive condition that $\deg(\mathrm{D}) \geqslant 2g+3$. Observe first that the monodromy group G is naturally isomorphic to a subgroup of $\mathfrak{S}_n$, since by construction of the scheme $\mathcal{H}_\mathrm{D}$, the fiber $\pi_\mathrm{D}^{-1}(f)$ over $f \in \mathcal{H}_\mathrm{D}$ is a finite set with $n = \deg(\mathrm{D})$ distinct elements, and G is naturally isomorphic to a permutation group of the generic fiber.

(1) The statement is simply a special case of [11, Cor. 9.2.3], after proper interpretation of the notation and terminology there (left to the reader, as this is not our main concern in this note).

(2) Alternatively, we note that it is enough to find a one-parameter family of functions in $\mathcal{H}_\mathrm{D}$ such that the pullback of $\pi_{\mathrm{D},*}\bar{\mathbf{Q}}_\ell$ along this family already has maximal geometric monodromy group $\mathfrak{S}_n$.

Assume that $\deg(\mathrm{D}) \geqslant 2g+3$. By [13, Th. 6.2.11, Cor. 6.2.15] (a result due to Katz and Rains), there exists $f_0 \in \mathcal{H}_\mathrm{D}$ such that the geometric monodromy group of (the restriction to a dense open set where it is lisse of) the sheaf $f_{0,*}\bar{\mathbf{Q}}_\ell$ is $\mathfrak{S}_n$, where we view the function f_0 as a morphism $f_0 \colon \mathrm{U} \to \mathbf{A}^1$.

We will show that this geometric monodromy group is the same as the geometric monodromy for the covering $\mathcal{Z}_\mathrm{D} \to \mathcal{H}_\mathrm{D}$ restricted to the one-parameter subfamily $t \mapsto f_0 - t$.

Precisely, let V be the subset of those $t \in \mathbf{A}^1$ with $f_0 - t \in \mathcal{H}_\mathrm{D}$. It is open in $\mathbf{A}^1$ (because $\mathcal{H}_\mathrm{D}$ is open in the space of functions with divisor D) and non-empty (since $0 \in \mathrm{V}$) hence dense. Consider the morphism

$$q \ : \ \begin{cases} \mathrm{V} \longrightarrow \mathcal{H}_\mathrm{D} \\ t \mapsto f_0 - t \end{cases},$$

and the pullback $q^*\mathcal{Z}_\mathrm{D} \to \mathrm{V}$ of $\mathcal{Z}_\mathrm{D} \longrightarrow \mathcal{H}_\mathrm{D}$ along q. We have

$$q^*\mathcal{Z}_\mathrm{D} = \{(t, f, x, 0) \in \mathrm{V} \times \mathcal{H}_\mathrm{D} \times \mathrm{U} \times \mathbf{A}^1 \mid f = f_0 - t, \quad f(x) = 0\}.$$

The morphism

$$\begin{cases} q^*\mathcal{Z}_\mathrm{D} \longrightarrow f_0^{-1}(\mathrm{V}) \subset \mathrm{C} \\ (t, f, x, 0) \mapsto x \end{cases}$$

is then an isomorphism, with inverse given by $x \mapsto (f_0(x), f_0 - f_0(x), x, 0)$. Under this isomorphism, the pullback to $q^*\mathcal{Z}_\mathrm{D}$ of the projection π_D corresponds to the morphism $f_0 \colon f_0^{-1}(\mathrm{V}) \to \mathrm{V}$. Hence we have an isomorphism

$$\pi_{\mathrm{D},*}\bar{\mathbf{Q}}_\ell \simeq f_{0,*}\bar{\mathbf{Q}}_\ell,$$

on V, and hence the result of Katz and Rains implies that the geometric monodromy group of $q^*\mathcal{Z}_\mathrm{D} \to \mathrm{V}$ is $\mathfrak{S}_n$. □

Remark 8. (1) In characteristic $\neq 2$ and if $\deg(\mathrm{D}) < p$, the most delicate part of the result of Katz and Rains can be avoided, even for $\deg(\mathrm{D}) \geqslant 2g+1$: one can then pick a function $f_0 \in \mathcal{H}_{\mathrm{D}}$ such that f_0 defines a Lefschetz pencil outside D by [11, Th. 2.2.6], and then it is a relatively simple fact (see [10, proof of Lemma 7.10.2.3] or [13, Th. 6.2.4 (2)]) that the monodromy group of $f_{0,*}\bar{\mathbf{Q}}_\ell$ is $\mathfrak{S}_n$ (the assumption $\deg(\mathrm{D}) < p$ and the fact that f_0 defines a Lefschetz pencil outside D in the sense of [10, Def. 2.0.13] are equivalent with saying that f_0 is a supermorse function on $\mathrm{U} = \mathrm{C} - \mathrm{D}$, in the sense of [10, 7.10.2.2]).

In particular, this argument gives an alternate approach in characteristic 0 to the proof in [11, Cor. 9.2.3].

(2) As Katz comments in [11, Chapter 9], this result is so classical in aspect that it might very well have been proved much earlier.

Here is a corollary that gives an arithmetic interpretation of this special case, somewhat different than the Bunyakowsky-type question of the previous section:

Corollary 9. *Let $\mathrm{C}/\mathbf{Q}$ be a smooth projective algebraic curve of genus $g \geqslant 0$, let D be an effective $\mathbf{Q}$-rational divisor on C of degree $\geqslant 2g+1$. Fix a $\mathbf{Q}$-basis of the vector space $\Gamma(\mathrm{C}, \mathcal{L}(\mathrm{D}))$ of functions with polar divisor $\leqslant \mathrm{D}$ on C, and define $\mathcal{H}_{\mathrm{D}}(\mathbf{Z})$ as the intersection of $\mathcal{H}_{\mathrm{D}}(\mathbf{Q})$ and of the lattice in $\Gamma(\mathrm{C}, \mathcal{L}(\mathrm{D}))$ spanned by this basis. Let H be a height function on $\mathcal{H}_{\mathrm{D}}(\mathbf{Z})$, e.g., define $\mathrm{H}(f)$ as the largest absolute value of a coefficient in a $\mathbf{Z}$-linear combination of the given basis that represents $f \in \mathcal{H}_{\mathrm{D}}(\mathbf{Z})$.*

For $\mathrm{N} \geqslant 1$, let

$$\mathrm{B}(\mathrm{N}) = |\{f \in \mathcal{H}_{\mathrm{D}}(\mathbf{Z}) \mid \mathrm{H}(f) \leqslant \mathrm{N}\}|.$$

Then for $\mathrm{N} \geqslant 1$, we have

$$\frac{1}{\mathrm{B}(\mathrm{N})}|\{f \in \mathcal{H}_{\mathrm{D}}(\mathbf{Z}) \mid \mathrm{H}(f) \leqslant \mathrm{N} \text{ and the Galois group of the splitting field of the divisor of zeros of } f \text{ is not } \mathfrak{S}_n\}| \ll \mathrm{N}^{-1/2}(\log \mathrm{N}).$$

Proof. This follows by combining the previous proposition and Hilbert's Irreducibility Theorem (see Serre's treatment in [17, §3.4]), followed by an estimate of Cohen [5] for the number of integral points of bounded size in a "thin" set (see the proof of [17, Th. 3.4.4] for the details). □

For instance, this gives the "generic" Galois group of the zeros of elliptic functions with (say) a pole at 0 of order $d \geqslant 3$ on an elliptic curve $\mathrm{E}/\mathbf{Q}$.

4. Geometric Bunyakowsky group

We will prove Theorem 1 by generalizing the second argument used in the proof of Theorem 7. We may assume that k is algebraically closed, since the statement of Theorem 1 is geometric. For the remainder of this section, we fix a smooth projective curve C of genus g over k, the effective divisor D on C with $\deg(\mathrm{D}) \geqslant 2g+1$, and the curve $\mathrm{S} \subset \mathrm{U} \times \mathbf{A}^1$. We assume that S is smooth and geometrically irreducible, and we denote by $\tilde{\mathrm{S}}$ its projective smooth model.

We denote by π_{D} the covering $\mathcal{Z}_{\mathrm{D}} \to \mathcal{H}_{\mathrm{D}}$ defined in the introduction. We first confirm that this is a finite étale covering over a dense open subset of $\mathcal{H}_{\mathrm{D}}$.

Lemma 10. *The morphism π_{D} is a finite étale covering over the dense open set $\mathcal{H}_{\mathrm{D,S}}$ of $\mathcal{H}_{\mathrm{D}}$ formed of those $f \in \mathcal{H}_{\mathrm{D}}$ where the intersection $\Gamma_f \cap \mathrm{S}$ is transverse.*

Proof. First, we check that $\mathcal{H}_{\mathrm{D,S}}$ is an open dense subset in $\mathcal{H}_{\mathrm{D}}$. This is a variant of [11, Lemma 5.0.6]. First, this set is open in $\mathcal{H}_{\mathrm{D}}$ by viewing it as union of subsets of $\mathcal{H}_{\mathrm{D}}$ where the zero divisor of $\mathrm{Y} - f$ is linearly equivalent to some divisor on $\tilde{\mathrm{S}}$ and has support in $\mathrm{U} \times \mathbf{A}^1$ with no multiplicity (compare with loc. cit.).

It is then enough to prove that there exists some $f_0 \in \mathcal{H}_{\mathrm{D}}$ for which the intersection is transverse. This condition is equivalent to saying that the function $(x, y) \mapsto y - f_0(x)$ has only zeros of order 1 on S. Fix some f_0. Then for any $c \in k$, the possible double zeros of $y - (f_0 + c)$ are located at the same points, namely the zeros of the differential form $dy - df_0$ on S. If the set of these zeros is finite, we can find c such that $y - (f_0 + c)$ is non-zero at these points, so that $f_0 + c$ satisfies the required condition.

To achieve the finiteness of the zeros of $dy - df_0$, observe that it holds for $f_0 = 0$ if S is not contained in a horizontal line. Otherwise, the existence of f_0 with $df_0 \neq 0$ is proved in [11, proof of Lemma 5.0.6].

Let $\Gamma \subset \mathcal{H}_{\mathrm{D,S}} \times \mathrm{C} \times \mathbf{A}^1$ denote the "universal graph" of a function in $\mathcal{H}_{\mathrm{D,S}}$. This is a smooth divisor. Similarly, $\mathcal{H}_{\mathrm{D,S}} \times \mathrm{S}$ is a smooth divisor in $\mathcal{H}_{\mathrm{D,S}} \times \mathrm{C} \times \mathbf{A}^1$, and we have

$$\mathcal{Z}_{\mathrm{D,S}} = \Gamma \cap (\mathcal{H}_{\mathrm{D,S}} \times \mathrm{S}) \subset \mathcal{H}_{\mathrm{D,S}} \times \mathrm{C} \times \mathbf{A}^1.$$

By definition, the intersection of these smooth divisors is transverse, and this translates exactly to the Jacobian criterion for the projection $\mathcal{Z}_{\mathrm{D,S}} \to \mathcal{H}_{\mathrm{D,S}}$ to be étale. □

We recall next that a function g on a smooth connected projective curve over k is said to define a Lefschetz pencil outside an effective divisor D, if the divisor of poles of g is contained in D and the differential dg has simple zeros, separated by g ([11, 2.0.13, 2.2.6]). Furthermore, it will be useful to make the following *ad-hoc* definition: g defines a *strong* Lefschetz pencil if, for any pole x of g, the differential dg has a pole at x. If k has characteristic 0, then g defines a strong Lefschetz pencil if and only if it defines a Lefschetz pencil.

The projections $\mathrm{S} \to \mathrm{U}$ and $\mathrm{S} \to \mathbf{A}^1$ extend to morphisms $\tilde{x} \colon \tilde{\mathrm{S}} \to \mathrm{C}$ and $\mathrm{Y} \colon \tilde{\mathrm{S}} \to \mathbf{P}^1$. For a function f on C, we still denote by $\tilde{f}$ the function $f \circ \tilde{x}$ on $\tilde{\mathrm{S}}$.

Lemma 11. *Assume that* S *is not contained in a vertical line $\{x\} \times \mathbf{A}^1$. There exists an effective divisor* E *on* $\tilde{\mathrm{S}}$ *with support contained in the support of $\tilde{x}^*\mathrm{D}$, and an open dense subset $\mathcal{H}^1_{\mathrm{D}}$ of $\mathcal{H}_{\mathrm{D}}$ such that, for all $f \in \mathcal{H}^1_{\mathrm{D}}$, the polar divisor of $\mathrm{Y} - \tilde{f}$ is equal to* E *and the zeros of $\mathrm{Y} - \tilde{f}$ are in* S.

Proof. Let $f \in \mathcal{H}_{\mathrm{D}}$ and let $g = \mathrm{Y} - \tilde{f}$. If $(x, y) \in \tilde{\mathrm{S}}$ is a pole of g, then either it is a pole of Y, or x is a pole of f. However, since S is not contained in a vertical line, the polar divisor of Y is contained in $\tilde{x}^*\mathrm{D}$, as one sees by considering a local equation of S at a point (x, y) in the polar divisor of Y. Hence the polar divisor of g is contained in $\tilde{x}^*\mathrm{D}$.

Let (x, y) be a point in the support of $\tilde{x}^*\mathrm{D}$. Let $\nu_1 \geqslant 0$ be the order of the pole of Y at (x, y) and let $\nu_2 \geqslant 1$ be the ramification index of π_1 at (x, y). Then by definition of $\mathcal{H}_{\mathrm{D}}$, the order of the pole of $\tilde{f}$ at (x, y) is $m\nu_2$, where m is the multiplicity of x in D. If $m\nu_2 \neq \nu_1$, then the order of the pole of g at (x, y) is always $\max(m\nu_2, \nu_1)$. If $m\mu_2 = \nu_1$, there is an open dense subset $\mathrm{U}_{x,y} \subset \mathcal{H}_{\mathrm{D}}$ such that the order of the pole of g at (x, y) is $m\mu_2$. Indeed, this happens if and only if the polar terms of order $m\nu_2 = \nu_1$ of Y and $\tilde{f}$ do not cancel; this

is an open condition, and if it fails to hold for f, then it holds for cf for any $c \neq 1$. We may therefore define

$$\mathrm{E} = \sum_{(x,y)\in \mathrm{Supp}(\tilde{x}^*\mathrm{D})} \max(\nu_1(x,y), m(x,y)\nu_2(x,y)) \cdot [(x,y)]$$

and take $\mathcal{H}^1_{\mathrm{D}}$ to be the intersection of the open dense sets $\mathrm{U}_{(x,y)}$. □

We denote by E the divisor given by this lemma.

Lemma 12. *Assume that there exists $f_0 \in \mathcal{H}^1_{\mathrm{D}}(k)$ such that the function $g = y - \tilde{f}_0$ on $\tilde{\mathrm{S}}$ defines a* strong *Lefschetz pencil outside* E*, and furthermore that either* $\deg(\mathrm{E})$ *is prime, or* E *is coprime to p, or $p \nmid \deg(\mathrm{E})$ and the genus of $\tilde{\mathrm{S}}$ is $\geqslant 1$. Then the Bunyakowsky group for* D *and* S *is maximal, i.e., it is $\mathfrak{S}_n$ where $n = \deg(\mathrm{E})$.*

Proof. The variation with $t \in \mathbf{A}^1$ of the solutions $(x,y) \in \mathrm{U} \times \mathbf{A}^1$ of $g(x,y) = y - f_0(x) = t$ correspond exactly (as in the proof of Proposition 7) to the variation of the solutions $(x,y) \in \mathrm{S}$ of $y = f_0(x) - t$, i.e, to the intersections $\mathrm{S} \cap \Gamma_{f_0 - t}$.

Precisely, let $\mathrm{V} \subset \mathbf{A}^1$ be the dense open set of those $t \in \mathbf{A}^1$ such that $f_0 - t \in \mathcal{H}_{\mathrm{D}}$. Consider $q\colon \mathrm{V} \to \mathcal{H}_{\mathrm{D}}$ defined by $t \mapsto f_0 - t$. The pullback $q^*\mathcal{Z}_{\mathrm{D}}$ over V is the variety

$$q^*\mathcal{Z}_{\mathrm{D}} = \{(t, f, x, y) \mid (x,y) \in \mathrm{S},\ f \in \mathcal{H}_{\mathrm{D}},\ f = f_0 - t\}$$

with projection $(t,f,x,y) \mapsto t$. But $(t,f,x,y) \mapsto (x,y)$ is an isomorphism $q^*\mathcal{Z}_{\mathrm{D}} \to g^{-1}(\mathrm{V}) \subset \tilde{\mathrm{S}}$, with inverse given by

$$(x,y) \mapsto (y - f_0(x), f_0 - (y - f_0(x)), x, y) = (g(x,y), f_0 - g(x,y), x, y).$$

Hence, by the variant of the result of Katz and Rains [13, Th. 6.2.15] proved in Theorem 15 below, we deduce that the Bunyakowsky group is maximal under the conditions we state. □

The following proposition, combined with Lemma 12 therefore implies Theorem 1. The conditions to ensure the existence of a strong Lefschetz pencil hint admiteddly at tinkering and lack elegance, and a more definitive statement should be true.

Proposition 13. *Let k be an algebraically closed field of odd characteristic. Assume that $\deg(\mathrm{D}) \geqslant 2g+2$ and that* S *is not contained in a vertical line $x = x_0$ in $\mathrm{U} \times \mathbf{A}^1$. In the space $\mathcal{H}^1_{\mathrm{D}}$ there exists a function f_0 such that $\mathrm{Y} - f_0$ is a strong Lefschetz pencil on $\tilde{\mathrm{S}}$ outside the divisor* E*.*

Proof. This is an application of the very general results of SGA 7 [6], with some tweaks similar to those in [11].

We already observed that the functions Y and $\tilde{f}$ for $f \in \Gamma(\mathrm{C}, \mathcal{L}(\mathrm{D}))$ belong to $\Gamma(\tilde{\mathrm{S}}, \mathcal{L}(\mathrm{E}))$. Let L be the vector space generated by these sections in $\Gamma(\tilde{\mathrm{S}}, \mathcal{L}(\mathrm{E}))$. This defines in the usual way (see [9, II, prop. 7.3] for instance) a closed embedding $i\colon \tilde{\mathrm{S}} \to \mathbf{P}(\mathrm{L})$. We first claim that this embedding is a *Lefschetz embedding* in the sense of [6, Exp. XVII, 2.3].

For the proof, we first note that (as in [11, 2.0.2, 2.2.5]) that the hyperplane sections associated to this embedding correspond to the subschemes on $\tilde{\mathrm{S}}$ of zeros of the non-zero elements $g \in \mathrm{L}$.

By [6, Exp. XVII, cor. 3.5.0 and prop. 3.3], it is enough to find a point $(x_0, y_0) \in \tilde{\mathrm{S}}$ and a hyperplane section of the embedding i through $i(x_0, y_0)$ such that this section has an ordinary double point at $i(x_0, y_0)$. Let (x_0, y_0) be any point in $\mathrm{U} \times \mathbf{A}^1$ (viewed as an open

set in $\tilde{\mathrm{S}}$) where the tangent is not a vertical line, i.e., any point such that a uniformizer ϖ on C at x_0 "is" a uniformizer (still denoted ϖ) on $\tilde{\mathrm{S}}$ at (x_0, y_0) – such points exist since $\tilde{\mathrm{S}}$ is not itself a vertical line. Let y be the image of the function Y in the local ring at (x_0, y_0). If we write

$$y = y_0 + c_1\varpi + c_2\varpi^2 + \cdots$$

then the ordinary double point condition for the hyperplane section corresponding to $\tilde{f} \in \mathrm{L}$ translates into

$$f = y_0 + c_1\varpi + c_2'\varpi^2 + \cdots$$

where $c_2' \neq c_2$ (in the completed local ring of C at x_0). We can find a function $f \in \mathrm{L}$ with this property if $\deg(\mathrm{D}) \geqslant 2g + 2$ since the Riemann-Roch theorem (on C) allows us to specifiy arbitrarily the terms up to ϖ^2 of functions in $\Gamma(\mathrm{C}, \mathcal{L}(\mathrm{D}))$ (compare [11, proof of Lemma 2.2.2]).

By the definition of Lefschetz embeddings [6, Exp. XVII, 2.3], it follows that there exists an open dense subset U of the space of lines in L such that any line $\ell \in \mathrm{U}$ is a Lefschetz pencil on $\tilde{\mathrm{S}}$ with respect to the closed embedding i ([6, Exp. XVII, 2.2]).

Arguing exactly as in [11, Prop. 2.0.11, (3)], in the space of lines through a given hyperplane H in $\mathbf{P}(\mathrm{L})$ for which the hyperplane intersection $i(\tilde{\mathrm{S}}) \cap \mathrm{H}$ is finite, there is an open dense subset U′ such that all lines $\ell \in \mathrm{U}'$ are Lefschetz pencils outside H. Any such line is defined by a single function $g \in \mathrm{L}$, so $g = c\mathrm{Y} - \tilde{f}$ for some $c \in k$ and $f \in \Gamma(\mathrm{C}, \mathcal{L}(\mathrm{D}))$; it cannot be the case that $c = 0$ for all g corresponding to lines in U′, since the subset where $c = 0$ is a proper closed subscheme of $\mathbf{P}(\mathrm{L})$. Taking then the intersection of $\mathcal{H}_{\mathrm{D}}$ with those g in U′ corresponding to $c \neq 0$, we obtain a dense open subset of $\mathcal{H}_{\mathrm{D}}$ such that $\mathrm{Y} - \tilde{f}$ is a Lefschetz pencil outside E.

Now we must finally check that there is also a dense open set of $\mathcal{H}_{\mathrm{D}}$ with elements defining a strong Lefschetz pencil. By [13, Lemma 6.2.7], there exists a dense open set U″ of $\mathcal{H}_{\mathrm{D}}$ such that if $f \in \mathrm{U}''$, then for any pole P of f of order $a \geqslant 1$, the differential df has a pole of order either $a+1$, if $p \nmid a$, or a, if $p \mid a$. We now show that if such a function f also belongs to the open dense subset $\mathcal{H}_{\mathrm{D}}^1$ (and possibly satisfies some further open conditions) then $g = \mathrm{Y} - \tilde{f}$ defines a strong Lefschetz pencil outside E, which will conclude the proof.

Let $(x, y) \in \tilde{\mathrm{S}}$ be a pole of g. Then x belongs to the support of D, so that f has a pole at x. Since $f \in \mathrm{U}''$, the differential df has a pole at x. It follows that $d\tilde{f} = \tilde{x}^* df$ has a pole at (x, y). It is an open condition that the (fixed) possible pole of $d\mathrm{Y}$ at (x, y) does not "cancel" this pole of $d\tilde{f}$, and this may be achieved by multiplying f by a suitable constant, so the resulting set of functions is still dense in L. Thus we obtain the result. □

Remark 14. (1) Note that from the point of view of number fields, the proof of Theorem 1 using Lefschetz pencils is quite strange, since it would amount to finding the right proportion of primes in a sequence by showing that there is the right proportion in a much *sparser* subsequence – usually a much harder problem!

(2) To define a Lefschetz pencil $g\colon \tilde{\mathrm{S}} \to \mathbf{P}^1$, two conditions are needed for a function g: (1) that the zeros of the differential be simple; (2) that the critical values of g be simple, in the sense that g separate the zeros of dg. Note that both statements are, for a polynomial, of the type "a polynomial is squarefree". Thus we have a somewhat mysterious statement of the kind: "if certain polynomials represent squarefree values sufficiently often, then some

cases of Bunyakowsky's Hypothesis hold", over function fields. This is again quite striking from the number field perspective.

5. Monodromy of Lefschetz pencils on curves

We will prove in this section the variant of the theorem of Katz and Rains that we used to prove Theorem 1.

Theorem 15. *Let k be an algebraically closed field of characteristic p. Let $\tilde{\mathrm{S}}$ be a smooth projective connected curve of genus $g \geqslant 1$ and $f\colon \tilde{\mathrm{S}} \to \mathbf{P}^1$ such that f has polar divisor some effective divisor D with $\deg(\mathrm{D}) \geqslant 2g+3$ and such that f defines a strong Lefschetz pencil outside D. Assume either that $p \nmid \deg(f)$, or that $\deg(f)$ is prime, or that D is coprime with p. Then the geometric monodromy group of $f_*\bar{\mathbf{Q}}_\ell$ is $\mathfrak{S}_n$ for $\ell \neq p$.*

Proof. This follows closely the proof of Katz and Rains [13, Th. 6.2.11]. Let G denote the geometric monodromy group of $f_*\bar{\mathbf{Q}}_\ell$. It is naturally seen as a subgroup of $\mathfrak{S}_n$ acting in its n-dimensional permutation representation. If D is coprime with p, then $\mathrm{G} = \mathfrak{S}_n$ by [13, Th. 6.2.4], so we may assume that one of the other two conditions holds.

The group-theoretic criterion that is used to show that $\mathrm{G} = \mathfrak{S}_n$ is that a primitive subgroup of $\mathfrak{S}_n$ containing a transposition is equal to $\mathfrak{S}_n$ (see [13, Lemma 6.3.2]).

Step 1. We first show that G contains a transposition. As in [13, 6.3.7, 6.3.8], it is enough to prove that $f_*\bar{\mathbf{Q}}_\ell$ has at least one singularity in $\mathbf{A}^1$ (the Lefschetz condition implies that the inertia group at such a singularity gives a transposition in G). The singularities of $f_*\bar{\mathbf{Q}}_\ell$ in $\mathbf{A}^1$ are the critical values of f in $\mathbf{A}^1$. Since f is a strong Lefschetz pencil, df has poles at all points in the support of D, hence all zeros of df are outside D. Since f is Lefschetz, it induces a bijection between zeros of df and critical values of f in $\mathbf{A}^1$. The number of singularities of $f_*\bar{\mathbf{Q}}_\ell$ in $\mathbf{A}^1$ is therefore the number of distinct zeros of df. Writing $(df)_0$ (resp. $(df)_\infty$) the divisor of zeros (resp. poles) of df, we get as in [13, (6.3.8.1)] the relations

$$\deg((df)_0) = 2g - 2 + \deg((df)_\infty) \geqslant \deg((df)_\infty)$$

since $g \geqslant 1$. The function f has at least one pole, and hence the strong Lefschetz condition implies that df has at least one pole. This means that $\deg((df)_0) \geqslant 1$, hence there is at least one finite singularity, hence at least one transposition in G.

Step 2. We next show that G is primitive as a subgroup of $\mathfrak{S}_n$. As in [13, 6.3.10–6.3.11], this is equivalent to proving that there is no factorization $f = h \circ \phi$ with

$$\tilde{\mathrm{S}} \xrightarrow{\phi} \mathrm{C}_1 \xrightarrow{h} \mathbf{P}^1,$$

where C_1 is a smooth projective curve of genus $g_1 \geqslant 0$, and ϕ (resp. h) is a morphism of degree $\deg(\phi) \geqslant 2$ (resp. $\deg(h) \geqslant 2$). This already shows that if $\deg(f)$ is prime, then G is primitive, in which case we are done. We therefore assume now that $p \nmid \deg(f)$.

Assume then that there is such a decomposition. Using only the Lefschetz property of f, the morphism h is first shown to be finite étale over $\mathbf{A}^1$ (see [13, 6.3.12]).

Now let $\mathrm{D}_1 = \sum_i e_i \mathrm{Q}_i$ be the polar divisor of h, with distinct Q_i's and $e_i \geqslant 1$. The polar divisor D_2 of dh has support contained in that of D_1. We claim first that the support of dh is the same as that of D_1, so that $\mathrm{D}_2 = \sum_i f_i \mathrm{Q}_i$ with $f_i \geqslant 1$. Indeed, since $f = h \circ \phi$, we have $df = \phi^* dh$, and since df has a pole at all poles of f by the strong Lefschetz assumption, it must be the case that dh has a pole at all poles of h.

We can now follow the lines of [13, 6.3.14]: since h is étale over $\mathbf{A}^1$, the divisor of dh is $-\mathrm{D}_2$. Hence

$$2g_1 - 2 = -\sum_i f_i < 0$$

since $f_i \geqslant 1$ and h must have poles. Therefore $g_1 = 0$ and

$$\sum_i f_i = 2.$$

Since $f_i \geqslant 1$, this means that either $\mathrm{D}_2 = \mathrm{Q}_1 + \mathrm{Q}_2$ with $\mathrm{Q}_1 \neq \mathrm{Q}_2$ or $\mathrm{D}_2 = 2\mathrm{Q}_1$.

In the first case, it must be the case that $p \mid e_1$ and $p \mid e_2$. Then p divides $e_1 + e_2 = d_1$, so p divides $\deg(f)$, which is a contradiction to our assumption on f. In the second case, either $p \mid e_1 = d_1 \mid \deg(f)$, which provides the same contradiction, or $d_1 = e_1 = 1$, another contradiction. □

References

[1] J. Bellaïche: *Théorème de Chebotarev et complexité de Littlewood*, Annales Sci. ENS (to appear).

[2] A.O. Bender and P. Pollack: *On quantitative analogues of the Goldbach and twin prime conjectures over* $\mathbf{F}_q[t]$, arXiv:0912.1702.

[3] L. Bary-Soroker: *Irreducible values of polynomials*, Adv. Math., 229 (2012), 854–874.

[4] S.D. Cohen: *The distribution of polynomials over finite fields*, Acta Arith. 17 (1970), 255–271.

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

[6] P. Deligne and N. Katz (editors): *Groupes de monodromie en géométrie algébrique*, SGA 7 II, Lecture Notes Math. 340, Springer, 1973.

[7] A. Entin: *On the Bateman-Horn conjecture for polynomials over large finite fields*, Compositio Math., to appear dx.doi.org/10.1112/S0010437X16007570preprint.

[8] C. Hall: L-*functions of twisted Legendre curves*, Journal of Number Theory 119 (2006), 128–147.

[9] R. Hartshorne: *Algebraic geometry*, Grad. Texts Math. 52, Springer 1977.

[10] N. Katz: *Exponential sums and differential equations*, Annals of Math. Studies, 124, Princeton Univ. Press, 1990.

[11] N. Katz: *Twisted* L-*functions and monodromy*, Annals of Math. Studies 150 (2002).

[12] N. Katz: *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. 7 (2001), no. 1, 29–44.

[13] N. Katz: *Moments, monodromy and perversity*, Annals of Math. Studies, 159, Princeton Univ. Press, 2005.

[14] E. Kowalski: *The large sieve, monodromy, and zeta functions of algebraic curves*, J. reine angew. Math. 601 (2006), 29–69.

[15] E. Kowalski: *On the rank of quadratic twists of elliptic curves over function fields*, International J. Number Th. 2 (2006), 267–288.

[16] P. Pollack: *Simultaneous prime specializations of polynomials over finite fields*, Proc. Lond. Math. Soc. (3) 97 (2008), 545–567.

[17] J-P. Serre: *Topics in Galois theory*, Research Notes in Math. 1, 2nd edition, A.K. Peters, 2008.

ETH Zürich – D-MATH, Rämistrasse 101, CH-8092 Zürich, Switzerland

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