

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 $p = F(n)$ taken by a fixed (irreducible and primitive) polynomial $F \in \mathbf{Z}[X]$ 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 ≥ 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 $g \geq 0$ (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 $\deg(D) \geq 2g + 1$, which we assume from now on: there exists in that case a Riemann-Roch variety \mathcal{H}_D over k such that, for any field extension K/k , the points in $\mathcal{H}_D(K)$ “are” the rational functions $f : C \rightarrow \mathbf{P}^1$, 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}_D is isomorphic to a dense open subset of affine space \mathbf{A}^d where $d = \deg(D) + 1 - g \geq g + 2$ (see, e.g., [15, Lemma 5.0.6], where \mathcal{H}_D is the closure of the space $\text{Fct}(C, \deg(D), D, \emptyset)$, which contains functions with $\deg(D)$ 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 $f: U \rightarrow \mathbf{A}^1$ on U , we denote by $\Gamma_f \subset U \times \mathbf{A}^1$ the graph of f . Now, let $S \subset U \times \mathbf{A}^1$ be a fixed algebraic curve defined over k . We form the subscheme

$$\mathcal{Z}_D \subset \mathcal{H}_D \times U \times \mathbf{A}^1$$

defined by

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

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

$$\pi_D: \mathcal{Z}_{D,S} \rightarrow \mathcal{H}_{D,S}$$

is finite étale (we will check this in detail in Lemma 15 below). We call this map the *Bunyakowsky covering* associated to (C, D, S) .

Definition (Bunyakowsky group). The *Bunyakowsky group* of \mathcal{Z}_D over k is the geometric Galois group of the Galois closure of the covering $\mathcal{Z}_{D,S} \rightarrow \mathcal{H}_{D,S}$, 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 $\pi_{D,*}\bar{\mathbf{Q}}_\ell$, on any dense open subset of \mathcal{H}_D where it is lisse.

The next section explains the choice of terminology. We will be interested in the following problem:

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 $\mathcal{Z}_{D,S} \rightarrow \mathcal{H}_{D,S}$?

In this paper, we answer the first question in fair generality. The result is most complete if k has characteristic zero, and requires some additional assumptions in positive characteristic.

To state the results most precisely, we begin with a simple proposition. **We assume from now on that $S \subset U \times \mathbf{A}^1$ is smooth and geometrically irreducible, and not contained in a “vertical” line $\{x\} \times \mathbf{A}^1$.**

Proposition 1. *With notation and assumptions as above, there exists an effective divisor E on \tilde{S} and an dense open subset \mathcal{H}_D^1 of \mathcal{H}_D such that for $f \in \mathcal{H}_D^1$, the polar divisor of the meromorphic function on \tilde{S} extending the function $(x, y) \mapsto y - f(x)$ is equal to D . Moreover, the degree of D is equal to the degree of π_D .*

We will denote by E the divisor given by this proposition and by n its degree. In characteristic 0, we will prove:

Theorem 2. *With notation and assumptions as above, assume further that k is a field of characteristic 0. If $\deg(D) \geq 2g + 3$, then the Bunyakowsky group is maximal, i.e., it is isomorphic to \mathfrak{S}_n .*

In positive characteristic, we will require some conditions on the geometric data involved. To state them, we use the following definition:

Definition 3. We say that S is *almost finite outside* D ¹ if, for any pole z of the meromorphic function extending $Y: S \rightarrow \mathbf{A}^1$ such that $\tilde{x}(z) \notin D$, the differential dY has a pole at x , where $\tilde{x}: \tilde{S} \rightarrow \mathbf{C}$ is the extension of the first projection.

Remark 4. This property is always true (whatever the choice of D) if k has characteristic zero, but may fail in positive characteristic. As the name suggests, it is also true if $S \rightarrow U$ is finite (for instance, in the case of a plane curve $F(x, y) = 0$ and D supported at ∞ , it is true if $F \in k[X, Y]$ is monic as a polynomial in Y).

Theorem 5. *With notation and assumptions as above, assume moreover that k is not of characteristic 2.*

Assume also that:

- (a) *The projection $x: S \rightarrow U$ is separable.*
- (b) *S is almost finite outside D .*

Then, if $\deg(D) \geq 2g + 3$, the Bunyakowsky group is maximal, i.e., it is isomorphic to \mathfrak{S}_n , provided 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{S} is ≥ 1 and $p \nmid n$.*

Remark 6. Note that this theorem does contain Theorem 2 as special case, since the geometric conditions (a) and (b) concerning the curves are always valid then, and so is the first of the three possibilities offered in (2) concerning the divisor.

If k has characteristic $p > 0$, then condition (a) is fairly natural. As we already hinted, Condition (b) is most easily verified if the first projection $x: S \rightarrow U$ is a *finite* morphism, since in that case the second projection has no pole outside of \tilde{x}^*D , so $S \rightarrow U$ is trivially almost finite.

Among the three possible assumptions in (2), note that the first condition concerning E is satisfied if p is “large enough” compared with the degree of D and the genus of \tilde{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 (with \tilde{S} of genus ≥ 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 $S \rightarrow U$ 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 $C = \mathbf{P}^1$ and D is supported at infinity, this theorem reduces (in most cases) to a theorem of Entin [9]. After a digression in Section 3 on some group-theoretic questions suggested by the arithmetic interpretation, we consider separately in Section 4 the special case where $S = U \times \{0\}$. The result is then due to Katz [15] and it 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 finally explained in Section 5. The main idea is an adaptation of *another* argument of Katz in [15], using Lefschetz pencils on curves, and techniques of Katz and Rains [17].

¹Find better name.

Remark 7. 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 [15] and [17]. We illustrate this with one example related to twists of elliptic curves over function fields. Consider a field k and let $C = \mathbf{P}^1$ and $D = d(\infty)$. Let W be the hypersurface

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

Form then the algebraic variety

$$V_D = \{(x, y, f, t) \in \mathbf{A}^2 \times \mathcal{H}_D \times U \mid (x, y, t, f(t)) \in W\}$$

with its natural projection $\pi: V_D \rightarrow \mathcal{H}_D$. Then the fiber over $f \in \mathcal{H}_D(k)$ 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 $R^1\pi_!\mathbf{Q}_\ell$ is then the study of the variation of the L-functions of these elliptic curves.

Note however that the techniques developed 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 [9]. We thank R. Pink and W. Sawin for explaining and correcting various points of algebraic geometry and Z. Rudnick for his remarks and criticisms. Also thanks to L. Bary-Soroker for pointing out the paper [3] of Bender and Pollack. This work was partially supported by a DFG-SNF lead agency program grant (grant 200021L.153647).

2. ARITHMETIC INTERPRETATION

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

We take $C = \mathbf{P}^1$ over k and $D = d(\infty)$ with $d \geq 1$. Then $U = \mathbf{A}^1$ and \mathcal{H}_D “is” the space of polynomials of degree d (compare with [15, Remark 5.0.7]). It is isomorphic to $\mathbf{G}_m \times \mathbf{A}^d$ by mapping a polynomial to the sequence of its coefficients.

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

$$S : F(x, y) = 0$$

where $F \in k[X, Y]$ 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}_D over f in that case is the set

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

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

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

where we view F as a polynomial in $A[Y]$, and use the substitution $F(f) \in A[Y] = k[X, Y]$. So the question is that of determining the Galois group $G_{d,F}$ of a “generic” polynomial of the form $F(f)$ for $f \in k[X]$ 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 $\nu \geq 1$ in \bar{k} . If the Galois group $G = G_{d,F}$ 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 $C \subset G_{d,F}$, we have

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

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

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

as $\nu \rightarrow +\infty$, where the constant $\mu_{d,F} > 0$ is the proportion of elements of $G_{d,F}$ whose 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 [6], but similar ideas already occur in work of Birch and Swinnerton-Dyer [5] in 1959).

In the particular case that the group $G_{d,F}$ is the full symmetric group \mathfrak{S}_n (as in Theorem 5), we have $\mu_{d,F} = 1/n$, the proportion of n -cycles in \mathfrak{S}_n . (See Section 3 below for some group-theoretic discussion of this property.)

This special case of the Bunyakowsky problem has been solved in many cases by Entin [9, 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 $A[Y]$; 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 [11], Pollack [20], Bary-Soroker [1], among others.

The precise result we obtain from (parts of) Theorem 5 is:

Corollary 8. *Let k be a finite field of odd characteristic p . Let $F \in k[X, Y]$ be a polynomial such that the affine curve S defined by the equation $F(x, y) = 0$ in $\mathbf{A}^1 \times \mathbf{A}^1$ is smooth, geometrically irreducible, and is not contained in a vertical line. Let \tilde{S} be the smooth projective model of S and denote its genus by $g \geq 0$. Assume that the projection $(x, y) \rightarrow x$ is separable and that $(x, y) \rightarrow y$ is almost finite outside $x^*(\infty)$.*

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

For $\nu \geq 1$, we have

$$\frac{1}{|k|^{(d+1)\nu}} |\{f \in k_\nu[X] \mid F(f) \text{ is irreducible in } k_\nu[X]\}| = \frac{1}{n} + O(E_1 |k|^{-\nu/2}),$$

where the implied constant is absolute and

$$E_1 = 3 \cdot 2^{5+2n} \cdot (3 + (2 + 2n) \deg(F)(2n - 1))^{d+2n+3} \cdot n^{-1}.$$

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 [3].) It is then possible to deduce, e.g., the existence of *some* irreducible specialization $F(f)$ 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 $O(|k|^{-\nu/2})$, where the implied constant depends on F , this follows from Theorem 5 (applied to $C = \mathbf{P}^1$ and $D = d(\infty)$) and the Chebotarev Density Theorem as in [19, 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 $F(f)$ is squarefree of degree n . Then the covering π_D is étale (Lemma 15 below). Its Galois closure is the covering $V_D \rightarrow U$ such that

$$(2) \quad V_D = \{(f, (x_1, y_1), \dots, (x_n, y_n)) \in U \times S^n \mid f(x_i) = y_i \text{ for } 1 \leq i \leq n\}.$$

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

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

Then, by the relation between irreducibility and Galois action recalled above, we obtain from [19, Proof of Th. 1] the relation

$$(3) \quad \frac{1}{|U(k_{\nu})|} |\{f \in U(k_{\nu}) \mid F(f) \text{ is irreducible in } k_{\nu}[\mathbf{X}]\}| = \frac{1}{n} + O(E_1 |k|^{-\nu/2}),$$

where the implied constant is absolute, and

$$E_1 = \sum_{\varrho} |\alpha(\varrho)| \sum_i \dim H_c^i(U \times \bar{k}, \varrho).$$

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

We have then

$$E_1 \leq (\max_{\varrho} |\alpha(\varrho)|) \sum_{\varrho} \sum_i \dim H_c^i(U \times \bar{k}, \varrho).$$

From the explicit computation of the Fourier coefficients $\alpha(\varrho)$ (see, e.g, [2, Prop. 10]), we get

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

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

$$H_c^i(V_D \otimes \bar{k}, \bar{\mathbf{Q}}_\ell) = \bigoplus_{\varrho} H_c^i(U \times \bar{k}, \varrho)$$

and

$$E_1 \leq \frac{1}{n} \sum_i \dim H_c^i(V_D \otimes \bar{k}, \bar{\mathbf{Q}}_\ell).$$

We proceed to estimate the sum of Betti numbers of V_D using the results of Katz [16]. For this purpose, we must represent V_D as a subvariety of \mathbf{A}^N defined by $\leq r$ equations of degree $\leq \delta$ 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 $F(f)$ is squarefree of degree n . We represent U as a closed subscheme of $\mathbf{A}^{(d+1)+2}$ with extra variables to ensure that $\deg(F(f)) = n$ and that $\text{res}(F(f), F(f)') \neq 0$; in terms of the coefficients of f , the resultant $\text{res}(F(f), F(f)')$ has degree $\leq \deg_Y(F)(2n-1)$. So we can take parameters

$$(N_1, r_1, \delta_1) = (d+3, 2, \deg_Y(F)(2n-1))$$

to embed U in \mathbf{A}^{N_1} using at most r_1 equations of degree $\leq \delta_1$.

Recalling (2), we deduce that we can take parameters

$$(N, r, \delta) = (N_1 + 2n, r_1 + 2n, \max(\delta_1, \deg(F), d))$$

(since $f(x_i) = y_i$ is a single equation of degree d , and $(x_i, y_i) \in S$ is a single equation of degree $\deg(F)$). By [16, Cor. of Th. 1], it follows that

$$\sum_i \dim H_c^i(V_D \otimes \bar{k}, \bar{\mathbf{Q}}_\ell) \leq 3 \cdot 2^{5+2n} \cdot (3 + (r_1 + 2n)\delta)^{N_1+2n+1}.$$

where $\delta = \max(d, \deg(F), (2n-1)\deg_Y(F)) \leq (2n-1)\deg(F)$. Comparing with (3), we obtain

$$\frac{1}{|U(k_\nu)|} |\{f \in U(k_\nu) \mid F(f) \text{ is irreducible in } k_\nu[X]\}| = \frac{1}{n} + O(E_1 |k|^{-\nu/2}),$$

where E_1 is the constant is the statement of the corollary, and the implied constant is absolute.

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

$$|U(k_\nu)| = |k|^{\nu(d+1)} + O(E_2 |k|^{\nu(d+1/2)})$$

where the implied constant is absolute and

$$E_2 = \sum_i \dim H_c^i(U \times \bar{k}, \bar{\mathbf{Q}}_\ell) \leq E_1.$$

Hence the bound for U implies the result as stated. \square

Remark 9. (1) For simplicity, we have not included the alternative of Theorem 5 where the divisor E is coprime to p .

(2) The degree n of the polynomial $F(f)$ 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 $aY^{\deg_Y(F)}$, we will have $n = d \deg_Y(F) + \deg_X(a)$.²

(3) One might also get bounds using the results of [18], 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 10. Assume k has characteristic ≥ 5 . Consider $F(X, Y) = Y^2 - X^3 - aX - b$, 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 $F(f)$ is 3 if $\deg(f) = 1$, and $2 \deg(f)$ if $\deg(f) \geq 3$. Theorem 5 applies for $\deg(f) \geq 5$. However, experiments for $k = \mathbf{Q}$ (combined with Hilbert’s irreducibility theorem) suggest that the result holds in that case for $\deg(f) \geq 1$, at least for most cubics.

Remark 11. The proof of Theorem 5 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 $F(f)$ 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 transposition 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 20).

3. A GROUP-THEORETIC DIGRESSION

The general limit (1) shows that Corollary 8 would also follow in the same form whenever the Bunyakowsky group G has the property that the proportion of n -cycles in G (when viewed as a subgroup of \mathfrak{S}_n) is $1/n$. Moreover, the existence of irreducible specializations $F(f)$ only requires that G contains at least one n -cycle. One may ask how widespread these conditions are for transitive permutation groups.

It is useful first to note that a subgroup of \mathfrak{S}_n has density $1/n$ of n -cycles if and only if it contains a unique G -conjugacy class of n -cycles. This is because, all n -cycles being conjugate in \mathfrak{S}_n with cyclic centralizer of order n (generated by the n -cycle itself), the centralizer in G of any n -cycle is also cyclic of order n . Therefore the density of n -cycles is $1/n$ times the number of conjugacy classes thereof. Using this, we will say, for short, that a permutation group of degree n is *unicyclic* if it has proportion $1/n$ of n -cycles.

Computations (with MAGMA’s database of transitive groups of degree ≤ 31) show that in many cases, the symmetric group \mathfrak{S}_n is far from the only transitive permutation group of degree n containing n -cycles, and also far from the only unicyclic group, although the latter are much rarer. In the range $4 \leq n \leq 31$, there are at least two unicyclic groups for all n and often more. For instance, for degree 20, there are (up to isomorphism) 1117 transitive permutation groups, among which 332 contain at least one n -cycle, and 35 are unicyclic.

²Note in particular, if $\deg_Y(F)$ and $\deg_X(a)$ are coprime, this will be prime infinitely often as d varies.

On the other hand, if we restrict to *primitive* permutation groups of degree n , then there is an explicit list of all possible unicyclic groups. Precisely, it follows from the classification of all primitive permutation groups of degree n containing an n -cycle, due to Feit [10, Th. 4.1] and Jones [13], that there are only two possibilities:

- If n is prime, there is a unique unicyclic primitive permutation group G of degree n , distinct from \mathfrak{S}_n , namely the semi-direct product $G = \mathbf{F}_n \rtimes \mathbf{F}_n^\times$ (the n -cycles in G are the $n - 1$ non-zero elements of the subgroup \mathbf{F}_n , so their proportion is indeed $1/n$). In fact, since n is prime, this is even the only transitive unicyclic permutation group of degree n that is not \mathfrak{S}_n .
- If n is not prime, then \mathfrak{S}_n is the unique unicyclic primitive permutation group of degree n .

(The list of Feit and Jones contains more groups containing n -cycles, but they are not unicyclic; it should be noted that their classification result depends on the classification of finite simple groups).

To conclude, we remark that (although we will not give details) it is possible to use Entin's method [9] to show *a priori* that the Bunyakowsky group is primitive in great generality (because it suffices to show that it is 2-transitive, and this can be done using the Chebotarev density theorem by computing the number of orbits on $\{1, \dots, n\}^2$, as Entin does). This means that proving (1) with limit $1/n$ is (in principle) "almost" equivalent to proving that the Bunyakowsky group is equal to \mathfrak{S}_n !

4. 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 $S = U \times \{0\} \subset U \times \mathbf{A}^1$. The fiber of the projection π_D over $f \in \mathcal{H}_D$ is then the scheme of zeros of the function f ; the space $\mathcal{H}_{D,S}$ is then the scheme $\text{Fct}(C, \deg(D), D, \emptyset)$ of Katz [15, Lemma 5.0.6]. We will denote it $\mathcal{H}_{D,0}$ for clarity, and similarly for the covering $\mathcal{Z}_{D,0} \rightarrow \mathcal{H}_{D,0}$.

The following result of Katz computes the Bunyakowsky group in that case, in a stronger form than actually implied by the statement of Theorem 5 in that case.

Theorem 12 (Katz). *Let k be a field. Let C/k be a smooth projective algebraic curve of genus $g \geq 0$, let D be an effective k -rational divisor on C of degree $\geq 2g + 1$, and let U be the open complement of the support of D . Let $S = U \times \{0\}$. The Bunyakowsky group G is then isomorphic to \mathfrak{S}_n , where $n = \deg(D)$.*

Proof. We give two proofs, one by Katz from [15] and one based on results of Katz and Rains in [17], in this second case under the slightly more restrictive condition that $\deg(D) \geq 2g + 3$. Observe first that the monodromy group G is naturally isomorphic to a subgroup of \mathfrak{S}_n , since by construction of the scheme $\mathcal{H}_{D,0}$, the fiber $\pi_D^{-1}(f)$ over $f \in \mathcal{H}_{D,0}$ is a finite set with $n = \deg(D)$ distinct elements, and G is naturally isomorphic to a permutation group of the generic fiber.

(1) The statement is simply a special case of [15, 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 $\mathcal{H}_{D,0}$ such that the pullback of $\pi_{D,*}\bar{\mathbf{Q}}_\ell$ along this family already has maximal geometric

monodromy group \mathfrak{S}_n , since the monodromy representation of the subfamily factors through that of the whole family.

Assume that $\deg(D) \geq 2g + 3$. By [17, Th. 6.2.11, Cor. 6.2.15] (a result due to Katz and Rains), there exists $f_0 \in \mathcal{H}_{D,0}$ 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 $f_0: U \rightarrow \mathbf{A}^1$.

We will show that this geometric monodromy group is the same as the geometric monodromy for the covering $\mathcal{Z}_{D,0} \rightarrow \mathcal{H}_{D,0}$ 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 $f_0 - t \in \mathcal{H}_{D,0}$. It is open in \mathbf{A}^1 (because $\mathcal{H}_{D,0}$ is open in the space \mathcal{H}_D of functions with divisor D) and non-empty (since $0 \in V$) hence dense. Consider the morphism

$$q : \begin{cases} V \longrightarrow \mathcal{H}_{D,0} \\ t \mapsto f_0 - t \end{cases},$$

and the pullback $q^*\mathcal{Z}_{D,0} \rightarrow V$ of $\mathcal{Z}_{D,0} \rightarrow \mathcal{H}_{D,0}$ along q . We have

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

The morphism

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

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 $q^*\mathcal{Z}_{D,0}$ of the projection π_D corresponds to the morphism $f_0: f_0^{-1}(V) \rightarrow V$. Hence we have an isomorphism

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

on V , and hence the result of Katz and Rains implies that the geometric monodromy group of $q^*\mathcal{Z}_{D,0} \rightarrow V$ is \mathfrak{S}_n . \square

Remark 13. (1) In characteristic $\neq 2$ and if $\deg(D) < p$, the most delicate part of the result of Katz and Rains can be avoided, even for $\deg(D) \geq 2g + 1$: one can then pick a function $f_0 \in \mathcal{H}_{D,0}$ such that f_0 defines a Lefschetz pencil outside D by [15, Th. 2.2.6], and then it is a relatively simple fact (see [14, proof of Lemma 7.10.2.3] or [17, Th. 6.2.4 (2)]) that the monodromy group of $f_{0,*}\bar{\mathbf{Q}}_\ell$ is \mathfrak{S}_n (the assumption $\deg(D) < p$ and the fact that f_0 defines a Lefschetz pencil outside D in the sense of [14, Def. 2.0.13] are equivalent with saying that f_0 is a supermorse function on $U = C - D$, in the sense of [14, 7.10.2.2]).

In particular, this argument gives an alternate approach in characteristic 0 to the proof in [15, Cor. 9.2.3].

(2) As Katz comments in [15, 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 14. *Let C/\mathbf{Q} be a smooth projective algebraic curve of genus $g \geq 0$, let D be an effective \mathbf{Q} -rational divisor on C of degree $\geq 2g + 1$. Fix a \mathbf{Q} -basis of the vector space $\Gamma(C, \mathcal{L}(D))$ of functions with polar divisor $\leq D$ on C , and define $\mathcal{H}_D(\mathbf{Z})$ as the intersection*

of $\mathcal{H}_D(\mathbf{Q})$ and of the lattice in $\Gamma(C, \mathcal{L}(D))$ spanned by this basis. Let H be a height function on $\mathcal{H}_D(\mathbf{Z})$, e.g., define $H(f)$ as the largest absolute value of a coefficient in a \mathbf{Z} -linear combination of the given basis that represents $f \in \mathcal{H}_D(\mathbf{Z})$.

For $N \geq 1$, let $B(N) = |\{f \in \mathcal{H}_D(\mathbf{Z}) \mid H(f) \leq N\}|$. Then for $N \geq 1$, we have

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

Proof. This follows by combining the previous proposition and Hilbert's Irreducibility Theorem (see Serre's treatment in [21, §3.4]), followed by an estimate of Cohen [7] for the number of integral points of bounded size in a "thin" set (see the proof of [21, Th. 3.4.4] for the details). \square

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

It would be quite interesting to see if, for some of the degrees not covered by this theorem, one obtains some "interesting" Galois groups.

5. COMPUTING THE GEOMETRIC BUNYAKOWSKY GROUP

We will prove Theorem 5 by generalizing the second argument used in the proof of Theorem 12. We may assume that k is algebraically closed, since the statement of Theorem 5 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 $\deg(D) \geq 2g + 1$, and the curve $S \subset U \times \mathbf{A}^1$. We assume that S is smooth and geometrically irreducible, and we denote by \tilde{S} its projective smooth model.

We denote by π_D the covering $\mathcal{Z}_D \rightarrow \mathcal{H}_D$ defined in the introduction. We first confirm that this is a finite étale covering over a dense open subset of \mathcal{H}_D .

Lemma 15. *The morphism π_D is a finite étale covering over the dense open set $\mathcal{H}_{D,S}$ of \mathcal{H}_D formed of those $f \in \mathcal{H}_D$ where the intersection $\Gamma_f \cap S$ is transverse.*

Proof. We will first check that $\mathcal{H}_{D,S}$ is an open dense subset in \mathcal{H}_D , which is a variant of [15, Lemma 5.0.6]. To prove this, we begin by noting that this set is open in \mathcal{H}_D by viewing it as union of subsets of \mathcal{H}_D where the zero divisor of $Y - f$ is linearly equivalent to some divisor on \tilde{S} and has support in $U \times \mathbf{A}^1$ with no multiplicity (compare with loc. cit.).

It is then enough to prove that there exists some $f_0 \in \mathcal{H}_D$ 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 $dy \neq 0$, and otherwise, there exists f_0 with $df_0 \neq 0$, as shown in [15, proof of Lemma 5.0.6].

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

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

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

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 ([15, 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 z of g , the differential dg has a pole at z . If k has characteristic 0, then g defines a strong Lefschetz pencil if and only if it defines a Lefschetz pencil.

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

We denote by E_Y the part of the polar divisor of Y outside \tilde{x}^*D .

Proposition 16. *Assume that S is not contained in a vertical line $\{x\} \times \mathbf{A}^1$. There exists an effective divisor E_0 on \tilde{S} supported on \tilde{x}^*D such that $E = E_Y + E_0$ has the following property: there exists an open dense subset \mathcal{H}_D^1 of \mathcal{H}_D such that, for all $f \in \mathcal{H}_D^1$, the polar divisor of the morphism $\tilde{S} \rightarrow \mathbf{P}^1$ extending $Y - f$ on \tilde{S} is equal to E and its zeros are in S .*

Proof. For any point p in $\tilde{S} - S$, the set of $f \in \mathcal{H}_D$ such that the morphism extending $Y - f$ is non-zero at p is open in \mathcal{H}_D . It is non-empty (because if some f belongs to it, then cf doesn't, for all $c \neq 1$). So there is an open dense subset \mathcal{H}_D^0 of \mathcal{H}_D such that the zeros of the morphism extending $Y - f$ are in S .

Let $f \in \mathcal{H}_D$ and let g be the morphism extending $Y - f$. If $z \in \tilde{S}$ is a pole of g , then either it is a pole of Y , or $\tilde{x}(z)$ is a pole of f (i.e., $z \in \tilde{x}^*D$).

If z is a pole of Y and $z \notin \tilde{x}^*D$, then z appears as a pole for any $f \in \mathcal{H}_D$, and its multiplicity is independent of f .

On the other hand, let z be a point in the support of \tilde{x}^*D . Let $\nu_1 \geq 0$ be the order of the pole of Y at z and let $\nu_2 \geq 1$ be the ramification index of π_1 at z . Then by definition of \mathcal{H}_D , the order of the pole of \tilde{f} at z is $m\nu_2$, where m is the multiplicity of $\tilde{x}(z)$ in D . If $m\nu_2 \neq \nu_1$, then the order of the pole of g at z is always $\max(m\nu_2, \nu_1)$. If $m\nu_2 = \nu_1$, there is an open dense subset $U_z \subset \mathcal{H}_D$ such that the order of the pole of g at z is $m\nu_2$. 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

$$E_0 = \sum_{z \in \text{Supp}(\tilde{x}^*D)} \max(\nu_1(z), m(z)\nu_2(z)) \cdot [(x, y)]$$

and take \mathcal{H}_D^1 to be the intersection of the open dense sets \mathcal{H}_D^0 and U_z for z in the support of \tilde{x}^*D . \square

We denote by E the divisor given by this proposition and by \mathcal{H}_D^1 the corresponding open dense subset.

Example 17. Consider $\mathbf{C} = \mathbf{P}^1$, $U = \mathbf{A}^1$, $D = d(\infty)$ and S the hyperbola $\{(x, y) \mid xy = 1\} \subset U \times \mathbf{A}^1$. Then \tilde{S} is also \mathbf{P}^1 . The morphism Y can be identified with the morphism $[x : y] \mapsto y/x$ on \mathbf{P}^1 , and \tilde{x} is identified with the morphism $[x : y] \mapsto x/y$. The space \mathcal{H}_D is the space of polynomials of degree d . We have $E_Y = (0)$ and the polar divisor of $Y - f = 1/x - f$ is $(0) + d(\infty)$ for all f .

Lemma 18. *Assume that there exists $f_0 \in \mathcal{H}_D^1(k)$ such that the function $g = y - \tilde{f}_0$ on \tilde{S} defines a strong Lefschetz pencil outside E , and furthermore that either $\deg(E)$ is prime, or E is coprime to p , or $p \nmid \deg(E)$ and the genus of \tilde{S} is ≥ 1 . Then the Bunyakowsky group for D and S is maximal, i.e., it is \mathfrak{S}_n where $n = \deg(E)$.*

Proof. The variation with $t \in \mathbf{A}^1$ of the solutions $(x, y) \in U \times \mathbf{A}^1$ of $g(x, y) = y - f_0(x) = t$ correspond exactly (as in the proof of Proposition 12) to the variation of the solutions $(x, y) \in S$ of $y = f_0(x) - t$, i.e, to the intersections $S \cap \Gamma_{f_0-t}$.

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

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

with projection $(t, f, x, y) \mapsto t$. But $(t, f, x, y) \mapsto (x, y)$ is an isomorphism $q^*\mathcal{Z}_D \rightarrow g^{-1}(V) \subset \tilde{S}$, 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 [17, Th. 6.2.15] proved in Theorem 21 below, we deduce that the Bunyakowsky group is maximal under the conditions we state. \square

The following proposition, combined with Lemma 18 therefore implies Theorem 5. The conditions to ensure the existence of a strong Lefschetz pencil hint admittedly at tinkering and lack elegance, and a more definitive statement should be true.

Proposition 19. *Let k be an algebraically closed field of odd characteristic. Assume that $\deg(D) \geq 2g + 2$, that S is not contained in a vertical line $x = x_0$ in $U \times \mathbf{A}^1$, and that dY has a pole at any $z \in E_Y$.*

In the space \mathcal{H}_D^1 there exists a function f_0 such that $Y - f_0$ is a strong Lefschetz pencil on \tilde{S} outside the divisor E .

Proof. This is an application of the very general results of SGA 7 [8], with some tweaks similar to those in [15].

We already observed that the function Y belongs to $\Gamma(\tilde{S}, \mathcal{L}(E))$; moreover, we have $\tilde{f} \in \Gamma(\tilde{S}, \mathcal{L}(E))$ for all $f \in \Gamma(C, \mathcal{L}(D))$. Let L be the subspace generated by Y and by these sections \tilde{f} in $\Gamma(\tilde{S}, \mathcal{L}(E))$. This defines in the usual way (see [12, II, prop. 7.3] for instance) a closed embedding $i: \tilde{S} \rightarrow \mathbf{P}(L)$. We first claim that this embedding is a *Lefschetz embedding* in the sense of [8, Exp. XVII, 2.3].

For the proof, we first note that (as in [15, 2.0.2, 2.2.5]) the hyperplane sections associated to this embedding correspond to the subschemes on \tilde{S} of zeros of the non-zero elements $g \in L$.

By [8, Exp. XVII, cor. 3.5.0 and prop. 3.3], it is enough to find a point $(x_0, y_0) \in \tilde{S}$ 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 $U \times \mathbf{A}^1$ (viewed as an open set in \tilde{S}) where the tangent space 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{S} at (x_0, y_0) – such points exist since \tilde{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

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

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

$$f = y_0 + c_1\varpi + c'_2\varpi^2 + \dots$$

where $c'_2 \neq c_2$ (in the completed local ring of C at x_0). We can find a function $f \in L$ with this property if $\deg(D) \geq 2g + 2$ since the Riemann-Roch theorem (on C) allows us to specify arbitrarily the terms up to ϖ^2 of functions in $\Gamma(C, \mathcal{L}(D))$ (compare [15, proof of Lemma 2.2.2]).

By the definition of Lefschetz embeddings [8, Exp. XVII, 2.3], it follows that there exists an open dense subset \mathcal{U} of the projective space of lines in L such that any line $\ell \in \mathcal{U}$ is a Lefschetz pencil on \tilde{S} with respect to the closed embedding i ([8, Exp. XVII, 2.2]).

Arguing exactly as in [15, Prop. 2.0.11, (3)], in the space of lines through a given hyperplane H in $\mathbf{P}(L)$ for which the hyperplane section $i(\tilde{S}) \cap H$ is finite, there is an open dense subset \mathcal{U}' such that all lines $\ell \in \mathcal{U}'$ are Lefschetz pencils outside H . Any such line is defined by a single function $g \in L$, so $g = cY - \tilde{f}$ for some $c \in k$ and $\tilde{f} \in \Gamma(C, \mathcal{L}(D))$; it cannot be the case that $c = 0$ for all g corresponding to lines in \mathcal{U}' , since the subset where $c = 0$ is a proper closed subscheme of $\mathbf{P}(L)$. Taking then the intersection of \mathcal{H}_D with those g in \mathcal{U}' corresponding to $c \neq 0$, we obtain a dense open subset of \mathcal{H}_D such that $Y - \tilde{f}$ is a Lefschetz pencil outside E for all \tilde{f} belonging to this open set.

Now we must finally check that there is also a dense open set of \mathcal{H}_D with elements defining a strong Lefschetz pencil. By [17, Lemma 6.2.7], there exists a dense open set \mathcal{U}'' of \mathcal{H}_D such that if $f \in \mathcal{U}''$, then for any pole P of f of order $a \geq 1$, 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}_D^1 (and possibly satisfies some further open conditions) then $g = Y - \tilde{f}$ defines a strong Lefschetz pencil outside E , which will conclude the proof.

Let $z \in \tilde{S}$ be a pole of g . If z belongs to E_Y , then dY has a pole at z by assumption, and df is regular, so that dg has a pole. Otherwise, $x = \tilde{x}(z)$ belongs to the support of D , so that f has a pole at x . Since $f \in \mathcal{U}''$, the differential df has a pole at x . Since the projection $\tilde{S} \rightarrow U$ is separable, 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 dY at z 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. \square

Remark 20. (1) Note that from the point of view of number fields, the proof of Theorem 5 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 $g: \tilde{S} \rightarrow \mathbf{P}^1$, 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”. This is quite striking from a number field perspective.

(3) This proof is quite comparable also to the argument of Bender and Wittenberg [4].

6. 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 5.

Theorem 21. *Let k be an algebraically closed field of characteristic p . Let \tilde{S} be a smooth projective connected curve of genus $g \geq 1$ and $f: \tilde{S} \rightarrow \mathbf{P}^1$ such that f has polar divisor some effective divisor D with $\deg(D) \geq 2g + 3$ 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 $f_*\bar{Q}_\ell$ is \mathfrak{S}_n for $\ell \neq p$.*

Proof. This follows closely the proof of Katz and Rains [17, Th. 6.2.11]. Let G denote the geometric monodromy group of $f_*\bar{Q}_\ell$. 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 $G = \mathfrak{S}_n$ by [17, 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 $G = \mathfrak{S}_n$ is that a primitive subgroup of \mathfrak{S}_n containing a transposition is equal to \mathfrak{S}_n (see [17, Lemma 6.3.2]).

Step 1. We first show that G contains a transposition. As in [17, 6.3.7, 6.3.8], it is enough to prove that $f_*\bar{Q}_\ell$ 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 $f_*\bar{Q}_\ell$ 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 $f_*\bar{Q}_\ell$ 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 [17, (6.3.8.1)] the relations

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

since $g \geq 1$. 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 $\deg((df)_0) \geq 1$, 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 [17, 6.3.10–6.3.11], this is equivalent to proving that there is no factorization $f = h \circ \phi$ with

$$\tilde{S} \xrightarrow{\phi} C_1 \xrightarrow{h} \mathbf{P}^1,$$

where C_1 is a smooth projective curve of genus $g_1 \geq 0$, and ϕ (resp. h) is a morphism of degree $\deg(\phi) \geq 2$ (resp. $\deg(h) \geq 2$). 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 [17, 6.3.12]).

Now let $D_1 = \sum_i e_i Q_i$ be the polar divisor of h , with distinct Q_i 's and $e_i \geq 1$. 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 $D_2 = \sum_i f_i Q_i$ with $f_i \geq 1$. 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 [17, 6.3.14]: since h is étale over \mathbf{A}^1 , the divisor of dh is $-D_2$. Hence

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

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

$$\sum_i f_i = 2.$$

Since $f_i \geq 1$, this means that either $D_2 = Q_1 + Q_2$ with $Q_1 \neq Q_2$ or $D_2 = 2Q_1$.

In the first case, dh has poles of order 1 at Q_1 and Q_2 , which is only possible if h has poles of order divisible by p at these points, so we have $p \mid e_1$ 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. \square

REFERENCES

- [1] L. Bary-Soroker: *Irreducible values of polynomials*, Adv. Math., 229 (2012), 854–874.
- [2] J. Bellaïche: *Théorème de Chebotarev et complexité de Littlewood*, Annales Sci. ENS 49 (2016), 579–632.
- [3] A.O. Bender and P. Pollack: *On quantitative analogues of the Goldbach and twin prime conjectures over $\mathbf{F}_q[t]$* , [arXiv:0912.1702](https://arxiv.org/abs/0912.1702).
- [4] A.O. Bender and O. Wittenberg: *A potential analogue of Schinzel’s hypothesis for polynomials with coefficients in $\mathbf{F}_q[t]$* , International Math. Res. Notices 2005, no. 36, 2237–2248.
- [5] B. Birch and H. Swinnerton-Dyer: *Note on a problem of Chowla*, Acta Arithmetica 5 (1959), 417–423.
- [6] S.D. Cohen: *The distribution of polynomials over finite fields*, Acta Arith. 17 (1970), 255–271.
- [7] S.D. Cohen: *The distribution of Galois groups and Hilbert’s irreducibility theorem*, Proc. London Math. Soc. (3) 43 (1981), 227–250.
- [8] P. Deligne and N. Katz (editors): *Groupes de monodromie en géométrie algébrique*, SGA 7 II, Lecture Notes Math. 340, Springer, 1973.
- [9] A. Entin: *On the Bateman-Horn conjecture for polynomials over large finite fields*, Compositio Math. 152 (2016), 2525–2544.
- [10] W. Feit: *Some consequences of the classification of finite simple groups*, in “The Santa Cruz conference on finite groups”, Proc. Sympos. Pure Math. 37, AMS (1980), 175–181.
- [11] C. Hall: *L-functions of twisted Legendre curves*, Journal of Number Theory 119 (2006), 128–147.
- [12] R. Hartshorne: *Algebraic geometry*, Grad. Texts Math. 52, Springer 1977.
- [13] G. A. Jones: *Cyclic regular subgroups of primitive permutation groups*, J. Group Theory 5 (2002), 403–407.
- [14] N. Katz: *Exponential sums and differential equations*, Annals of Math. Studies, 124, Princeton Univ. Press, 1990.
- [15] N. Katz: *Twisted L-functions and monodromy*, Annals of Math. Studies 150 (2002).
- [16] N. Katz: *Sums of Betti numbers in arbitrary characteristic*, Finite Fields Appl. 7 (2001), no. 1, 29–44.
- [17] N. Katz: *Moments, monodromy and perversity*, Annals of Math. Studies, 159, Princeton Univ. Press, 2005.
- [18] E. Kowalski: *The large sieve, monodromy, and zeta functions of algebraic curves*, J. reine angew. Math. 601 (2006), 29–69.
- [19] E. Kowalski: *On the rank of quadratic twists of elliptic curves over function fields*, International J. Number Th. 2 (2006), 267–288.
- [20] P. Pollack: *Simultaneous prime specializations of polynomials over finite fields*, Proc. Lond. Math. Soc. (3) 97 (2008), 545–567.
- [21] 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