PRIME SPECIALIZATION IN HIGHER GENUS I

BRIAN CONRAD AND KEITH CONRAD

Abstract. A classical conjecture predicts how often a polynomial in $\mathbf{Z}[T]$ takes prime values. The natural analogous conjecture for prime values of a polynomial $f(T) \in \kappa[u][T]$, where κ is a finite field, is false. The conjecture over $\kappa[u]$ was modified in earlier work by introducing a correction factor that encodes unexpected periodicity of the Möbius function at the values of f on $\kappa[u]$ when $f \in \kappa[u][T^p]$, where p is the characteristic of κ.

In this paper, for $p \neq 2$ we extend the Möbius periodicity results for $\kappa[u]$ – the affine κ-line – to the case when f has coefficients in the coordinate ring A of any higher-genus smooth affine κ-curve with one geometric point at infinity. The basic strategy is to pull up results from the genus-0 case by means of well-chosen projections to the affine line. Our techniques can also be used to prove nontrivial properties of a correction factor in the conjecture on primality statistics for values of $f \in A[T^p]$ on A, even as f and κ vary.

1. Introduction

This paper establishes a higher-genus generalization of theorems proved for the affine line in [2]. To motivate what we will do here, which otherwise may seem idiosyncratic, we begin by reviewing the main conclusions in [2] and two interesting applications.

There is a classical conjecture predicting how often an irreducible polynomial in $\mathbf{Z}[T]$ takes prime values. (One has to assume there are no local obstructions, unlike $T^2 - T + 2$, which is irreducible but only has even values on $\mathbf{Z}$, thus having a local obstruction at 2.) The well-known analogies between $\mathbf{Z}$ and $\kappa[u]$ for a finite field κ lead to a natural conjecture for how often an irreducible polynomial in $\kappa[u][T]$ takes prime values on $\kappa[u]$. For example, if we work with $T^3 + u$ over $\mathbf{F}_3[u]$, we ask how often $g^3 + u$ is irreducible as g runs over $\mathbf{F}_3[u]$. We will sample over all g of a common degree n and see what happens as the degree gets large. Analogies with the classical setting over $\mathbf{Z}$ suggest that

$$\#\{g \in \mathbf{F}_3[u] : \deg g = n, g^3 + u \text{ is prime in } \mathbf{F}_3[u]\} \sim \frac{2 \cdot 3^{n-1}}{n} \tag{1.1}$$

as $n \to \infty$. In particular, the number of prime specializations in degree n is predicted to grow exponentially with n. However, this is false in a rather surprising way. When $n \equiv 0 \bmod 4$ and $n > 0$, it can be proved that $g^3 + u$ has an even number of irreducible factors when g has degree n and thus $g^3 + u$ is not irreducible (so the count on the left side of (1.1) is 0). When $n \equiv 2 \bmod 4$, the count on the left side of (1.1) appears *numerically* to be approximately twice as large as the right side. On the other hand, when n is odd (1.1) looks correct numerically. (See [1, Table 2] for data when $9 \leq n \leq 16$.) Thus it seems that we can correct (1.1) by including a periodic sequence of correction factors $1, 2, 1, 0$ on the right side according as $n \equiv 1, 2, 3, 0 \bmod 4$.

2000 *Mathematics Subject Classification.* 11N32.

Key words and phrases. Möbius bias.

B.C. was partially supported by the Alfred P. Sloan Foundation and NSF grant DMS-0093542 during work on this paper. The authors thank J. de Jong and R. Lazarsfeld for helpful discussions.

There are more $f(T) \in \kappa[u][T]$ such that the number of $g \in \kappa[u]$ with $\deg g = n$ and $f(g)$ prime in $\kappa[u]$ does not appear to fit an asymptotic estimate resembling (1.1) that is suggested by analogies with $\mathbf{Z}$. All such known $f(T)$ lie in $\kappa[u][T^p]$, where p is the characteristic of κ. (Incidentally, this avoids the case $\deg_T f = 1$ for which the expected frequency of prime values of $f(g)$ is the proved $\kappa[u]$-analogue of Dirichlet's theorem.) Numerically, it appears that the asymptotic prediction can always be fixed by introducing a correction factor which is a function of n mod 4, as we saw above for $T^3 + u$ over $\mathbf{F}_3[u]$.

Of course, basing a correction factor on numerical evidence is hardly satisfying. The main discovery in [2], which is joint work with R. Gross, is that there is a systematic and heuristically reasonable way to predict these new correction factors in advance, in terms of the following feature of the Möbius function on $\kappa[u]$. (The Möbius function on $\kappa[u]$ is defined by $\mu(h) = (-1)^r$ when h is squarefree in $\kappa[u]$ with r monic irreducible factors and $\mu(h) = 0$ otherwise.)

Theorem 1.1 ([2, Thm. 4.8])**.** *Let κ be a finite field of odd characteristic p, and fix $f(T) \in \kappa[u][T^p]$ that has positive T-degree and is squarefree in $\kappa[u][T]$. The function $g \mapsto \mu(f(g))$ for $g \in \kappa[u]$ is "quasi-periodic" in the sense that there is a nonzero polynomial $M_{f,\kappa} \in \kappa[u]$ such that, for any $g_1 = c_1 u^{n_1} + \cdots$ and $g_2 = c_2 u^{n_2} + \cdots$ in $\kappa[u]$ with sufficiently large degrees n_1 and n_2,*

$$g_1 \equiv g_2 \bmod M_{f,\kappa}, \quad \chi(c_1) = \chi(c_2), \quad n_1 \equiv n_2 \bmod 4 \Longrightarrow \mu(f(g_1)) = \mu(f(g_2)),$$

where χ is the quadratic character on $\kappa^\times$.

This theorem, which has no known parallel for the Möbius function on values of a polynomial in $\mathbf{Z}[T]$, has its most interesting applications for irreducible $f(T)$. However, for the proof of the theorem it is convenient to work in the generality of squarefree $f(T)$. In characteristic 2, similar periodicity results are described in [2] in terms of more intricate methods resting on 2-adic liftings.

A consequence of Theorem 1.1 is that the ratio

$$\frac{\sum_{\deg g = n, (f(g), M_{f,\kappa}) = 1} \mu(f(g))}{\sum_{\deg g = n, (f(g), M_{f,\kappa}) = 1} |\mu(f(g))|} \in \mathbf{Q} \cap [-1, 1], \tag{1.2}$$

which appears at first to be a complicated function of n, is in fact periodic in $n \gg 0$ with period dividing 4. We found that for irreducible $f(T)$ that is inseparable over $\kappa(u)$, using 1 minus the periodic values as a correction factor numerically appears to fix deviations between primality counts on $f(g)$ for $\deg g = n$ and asymptotic predictions for these counts (as $n \to \infty$) such as on the right side of (1.1). For example, when $f(T) = T^3 + u$ and $\kappa = \mathbf{F}_3$, the ratio (1.2) has periodic values $0, -1, 0, 1$ for $n \geq 1$, so 1 minus this sequence is $1, 2, 1, 0$ for $n \geq 1$, which matches the numerical data mentioned above. See [1] and [2, §6] for a further discussion of the correction factor (1.2), including its properties as f and κ vary.

There are two additional reasons that Möbius periodicity in our Theorem 1.1 is an interesting phenomenon:

(1) The effect of nonzero Möbius averages in characteristic p is reminiscent of the parity problem in sieve methods. It implies that, unlike the classical case over $\mathbf{Z}$, the parity problem in the function field case is not simply a problem of technique in prime-counting questions but is a real phenomenon in prime-counting itself, as we saw with $g^3 + u$ over $\mathbf{F}_3[u]$ when $\deg g \equiv 0 \bmod 4$.

(2) In [4], which is joint work with H. Helfgott, we used Möbius periodicity to find a non-isotrivial elliptic curve E over $\kappa(u)(T)$, for any finite κ of odd characteristic, such that $\mathrm{rank}(E(\kappa(u)(T))) < \mathrm{rank}(E_t(\kappa(u)))$ for all $t \in \kappa(u)$ if we grant the parity conjecture for ranks of elliptic curves over $\kappa(u)$. This is interesting because, by other work of Helfgott, any elliptic curve over $\mathbf{Q}(T)$ with rank less than the rank of all but finitely many of its smooth specializations over $\mathbf{Q}$ must be isotrivial if certain widely believed conjectures in analytic number theory are true; such isotrivial examples over $\mathbf{Q}(T)$ have been highlighted elsewhere, *e.g.*, in [8].

Since the unexpected behavior of $\mu(f(g))$ in characteristic p is related to two basic themes in number theory (counting prime values of polynomials and Mordell–Weil ranks for an elliptic curve), it is natural to go beyond the case of $\kappa[u]$ and study the Möbius function on values of a polynomial over the coordinate ring of a higher-genus smooth affine curve instead of $\kappa[u]$. The starting point for this paper was the following question: does the periodicity in Theorem 1.1 carry over when $\kappa[u]$ is replaced with a higher-genus coordinate ring? Since the proofs in [2] for the case of $\kappa[u]$ made essential use of properties of $\kappa[u]$ that do not hold in higher genus (such as the absence of Weierstrass gaps at ∞), answering this question is not merely an exercise in adapting the earlier proofs to a more general setting. Our affirmative answer to this motivating question is given in Theorem 1.3, below which we describe some of its applications.

Let us now formulate our setup more precisely. When counting prime values of a polynomial on the ring of integers of a number field, the simplest case to consider is when there is just one archimedean place ($\mathbf{Q}$ or an imaginary quadratic field). Counting prime values in such cases has been checked numerically and gives a good fit with standard predictions, even when the class number exceeds 1. In the higher-genus function field case we shall likewise restrict our attention to cases with one (geometric) point at infinity. To this end, let k be a perfect field with characteristic $p > 0$, let A be the coordinate ring of a smooth geometrically connected affine curve C over k such that C has exactly one geometric point ξ at infinity (so ξ is k-rational), and let $K = k(C)$ be the fraction field of A. For example, C could be the affine part of an elliptic curve over k given by a Weierstrass equation. For $a \in A - \{0\}$, define the *degree* of a to be

$$\deg(a) := -\operatorname{ord}_\xi(a) \geq 0; \tag{1.3}$$

this is the analogue of the degree on $k[u]$.

For finite k and $f \in A[T^p]$, we want to prove an analogue of Theorem 1.1. Define $\mu : A \to \{0, 1, -1\}$ by $\mu(\alpha) = 0$ if the ideal αA is divisible by the square of a prime ideal (this holds if $\alpha = 0$) and $\mu(\alpha) = (-1)^{\#\operatorname{Spec}(A/\alpha A)}$ otherwise. For later purposes, it is also convenient to make another definition:

Definition 1.2. For nonzero $f = \sum_i \alpha_i T^i \in A[T]$, its *total degree* is

$$\deg_{u,T} f = \max_i(-\operatorname{ord}_\xi(\alpha_i) + i).$$

If $A = k[u]$ then this definition recovers the usual notion of total degree for a 2-variable polynomial. (This is the reason for the notation, with u considered to be a parameter along C.) For emphasis (and to avoid confusion), we shall sometimes write $\deg_T f$ rather than $\deg f$ to denote the usual T-degree of a nonzero $f \in A[T]$.

The main goal of the present paper is to develop the higher-genus theory of Möbius periodicity in odd characteristic. Since the theory in genus 0 in [2] only required f to be squarefree rather than irreducible, we will work with $f(T) \in A[T^p]$ that is squarefree in

$K[T]$ (not necessarily irreducible). We will require $p \neq 2$ and leave the much more difficult case of characteristic 2 to [3].

To formulate our main result about Möbius periodicity, we introduce some notation. We let A, K, and C be as above, let $f \in A[T^p]$ be squarefree in $K[T]$ with positive degree, and let $Z = \mathrm{Spec}(A[T]/(f))$ be the associated zero scheme in $C \times \mathbf{A}^1_k$. We assume that the projection $Z \to C$ has finite fibers, which is a geometric analogue of the classical condition that a polynomial in $\mathbf{Z}[T]$ has no prime dividing all of its coefficients. Under these assumptions the projection $Z \to \mathbf{A}^1_k$ turns out to be generically étale, and we let $B \subseteq Z$ be its finite branch scheme. Finally, we let $I = I_f \subseteq A$ be the nonzero radical ideal whose zero locus is the image of B in C.

Theorem 1.3. *With notation and hypotheses as above, if k is finite then the function $a \mapsto \mu(f(a))$ is "quasi-periodic" modulo I in the sense that if $a, a' \in A$ are nonzero and $\deg(a), \deg(a') \gg 0$ then*

$$a \equiv a' \bmod I,\ \frac{a}{a'} \in (K_\xi^\times)^2,\ \deg(a) \equiv \deg(a') \bmod 4 \Rightarrow \mu(f(a)) = \mu(f(a')). \tag{1.4}$$

Here K_ξ is the completion of K at ξ and the "sufficient largeness" of $\deg(a)$ and $\deg(a')$ only depends on the genus of K/k and the total degree $\deg_{u,T} f$ (but not on k).

If -1 is a square in $k^\times$ or if $\deg_T f$ is even then the condition $\deg(a) \equiv \deg(a') \bmod 4$ in (1.4) may be relaxed to congruence modulo 2 without affecting the largeness condition on $\deg(a)$ and $\deg(a')$.

The special case of Theorem 1.3 in genus 0 (that is, $A = k[u]$) is a more precise version of Theorem 1.1 in the sense that it gives geometric meaning to $M_{f,k}$ in Theorem 1.1 with $\kappa = k$ (and it refines the periodicity criterion if -1 is a square in $k^\times$ or $\deg_T f$ is even). It is this more precise version that is proved in [2, Thm. 4.8] and used in the proof of Theorem 1.3. In [3] we give two applications of Theorem 1.3 (and its proof): (i) the definition of a correction factor in a higher-genus primality-counting conjecture for values of f on A (a *prime value* of f on A is a value that generates a prime ideal), and (ii) asymptotic and nontriviality properties of this correction factor as f and the finite constant field vary. It is these applications that are the reason for interest in Theorem 1.3. Our treatment of characteristic 2 in [3] builds on the techniques used here in odd characteristic and also requires some input from rigid and formal geometry.

Remark 1.4. Although Theorem 1.3 imposes a primitivity requirement on $f \in A[T]$ (via the assumption that $Z \to C$ has finite fibers), no primitivity condition is used in the genus-0 case given in [2, Thm. 4.8]. In fact, the inductive method of proof used in [2] is ill-suited to a primitivity hypothesis. We impose a primitivity restriction for our work in higher genus due to crucial intermediate results such as Theorem 2.5, Lemma 5.1, and Theorem 5.2 below. Our intended arithmetic applications satisfy the primitivity hypothesis anyway, and it is straightforward to check that to prove [2, Thm. 4.8] it is sufficient to treat just the primitive case.

Now we turn to an overview of the basic strategy underlying our proof of Theorem 1.3 over a finite field $k = \kappa$. We have to construct some finite projections $\pi : C \to \mathbf{A}^1_\kappa$ such that (among other things) the associated "norm polynomials" $\mathrm{N}_\pi(f) \in \kappa[u][T^p]$ are squarefree in $\kappa(u)[T]$ and primitive with respect to $\kappa[u]$. Periodicity results in higher genus shall thereby be inferred by applying our genus-zero results in [2] to $\mathrm{N}_\pi(f)$ and to several other auxiliary

norm polynomials over $\kappa[u]$. Due to the way we use [2] here, the methods in the present paper are not sufficient to reprove the main results in [2].

An important difference between the case of genus zero and the case of higher genus is illustrated by our work with discriminants. In [2], for $p \neq 2$ we used an idea of Swan to express $\mu(h)$ (for nonzero $h \in \kappa[u]$) in terms of the discriminant of h: $\mu(h) = (-1)^{\deg h}\chi(\mathrm{disc}_\kappa\, h)$, where χ is the quadratic character on $\kappa^\times$ (see Theorem 3.1 below as well). Resultants have more convenient algebraic properties than discriminants, so it is useful to express $\mathrm{disc}_\kappa\, h$ in terms of the resultant $R_{\kappa[u]}(h, h')$ of h and h', where $\mathrm{disc}_\kappa\, h$ denotes the discriminant of the κ-algebra $\kappa[u]/(h)$ with respect to the ordered basis $\{1, u, \ldots, u^{\deg h - 1}\}$. (This agrees with the usual definition of the discriminant of a polynomial when the leading coefficient is 1, but not necessarily otherwise.) Taking care to account for the possibility $\deg h' < \deg h - 1$ in positive characteristic,

$$\mathrm{disc}_\kappa\, h = \frac{(-1)^{d(d-1)/2}}{(\mathrm{lead}\, h)^{d+\deg h'}} R_{\kappa[u]}(h, h') \tag{1.5}$$

when h and h' are both nonzero in $\kappa[u]$, where $d = \deg h$.

Since $R_{\kappa[u]}(h, h')/(\mathrm{lead}\, h)^{\deg h'}$ is the norm $\mathrm{N}_{(\kappa[u]/(h))/\kappa}(h')$ when $h' \neq 0$, (1.5) may be restated as the identity (valid even if $h' = 0$)

$$\mathrm{disc}_\kappa(\kappa[u]/(h)) = \frac{(-1)^{d(d-1)/2}}{(\mathrm{lead}\, h)^d} \mathrm{N}_{(\kappa[u]/(h))/\kappa}(h'). \tag{1.6}$$

The higher-genus analogue of (1.6) computes $\mathrm{disc}_\kappa(A/(\alpha))$ for $\alpha \in A - \{0\}$ via a formula in Theorem 4.1. This analogous formula works over an arbitrary field in the role of κ (as does (1.6)), but it is not as explicit as (1.6): it depends on the choice of a κ-basis $\underline{\varepsilon} = \{\varepsilon_i\}$ of A with $-\mathrm{ord}_\xi(\varepsilon_i)$ strictly increasing in i (see §3) and the choice of a nonzero vector field D on C in place of the constant vector field ∂_u in (1.6). The factor $(-1)^{d(d-1)/2}$ in (1.6) is replaced with a constant $b_{D,d,\underline{\varepsilon}} \in \kappa^\times$, where $d = -\mathrm{ord}_\xi(\alpha)$. This constant is not affected by replacing κ with any extension field, and it seems hopeless in general to determine how $b_{D,d,\underline{\varepsilon}}$ depends on d. Since the mod-4 (as opposed to mod-2) periodicity properties in d for the Möbius function in the case of genus 0 (proved in [2]) are largely due to the fact that $(-1)^{d(d-1)/2}$ in (1.6) depends on $d \bmod 4$, our lack of understanding of $b_{D,d,\underline{\varepsilon}}$ in the general case presents an obstacle that we did not encounter in the earlier work in genus 0. It is essentially for this reason that we are forced to use indirect "reduction to genus 0" arguments in our study of Möbius periodicity in higher-genus cases.

The key to our Möbius periodicity results is a new identity for discriminants (whose proof does not use reduction to genus 0):

Theorem 1.5. *Keep hypotheses and notation as in Theorem* 1.3*, except that we allow k to be any perfect field with any positive characteristic p. For any $d \geq 0$, let V_d^0 be the variety of regular functions on C with a pole of order exactly d at ξ. Also, let $B \subseteq C$ be the image of the non-étale locus of the generically étale projection $Z \to C$ from the zero scheme Z of f in $C \times \mathbf{A}^1_k$.*

If d is sufficiently large (only depending on the total degree $\deg_{u,T} f$ and genus g of K/k), then for any k-algebra k' and any $a \in V_d^0(k')$ we have

$$\begin{aligned} \mathrm{disc}_{k'}((k' \otimes_k A)/(f(a))) &= w_d(a) \prod_{x=(u_x,t_x)\in B} \mathrm{N}_{k'\otimes_k k(x)/k'}(a(u_x) - t_x)^{\ell(\mathscr{O}_{B,x})} \\ &= w_d(a)\mathrm{N}_{B_{k'}/k'}(a - T) \end{aligned} \tag{1.7}$$

for a suitable unit w_d on V_d^0, where the exponent $\ell(\mathscr{O}_{B,x})$ is the length at x for B.

Remark 1.6. In [3, §2] we propose a correction factor in the standard conjecture for primality statistics of values of f on A. The local geometric interpretation of the exponents $\ell(\mathscr{O}_{B,x})$ in Theorem 1.5 is the key to proving asymptotic and nontriviality properties of this correction factor as f varies in suitable families. This suggests that the standard conjecture for primality statistics of values of f on A is false for "many" $f \in A[T^p]$.

Some important technical issues have been deliberately omitted in the statement of Theorem 1.5, such as how to define the discriminant in (1.7) as an element of k' so that, as in the classical $k[u]$-case, there is no unit-square ambiguity. This matter is addressed by Lemma 3.3 and the subsequent discussion there by using a k-basis $\underline{\varepsilon} = \{\varepsilon_1, \varepsilon_2, \dots\}$ of A with $-\mathrm{ord}_\xi(\varepsilon_i)$ strictly increasing in i; the unit w_d in (1.7) depends on $\underline{\varepsilon}$. The significance of Theorem 1.5 is that the norm factors have nothing to do with d and are determined by a modulo the ideal I as in Theorem 1.3. For finite k and odd p, discriminants are connected to Möbius values through their quadratic characters (see Theorem 3.1). By Theorem 1.5, upon specifying the congruence class of a modulo I the remaining variation in the quadratic character of the discriminant of $A/(f(a))$ as d and $a \in V_d^0(k)$ vary is encoded in the quadratic character of $w_d(a) \in k^\times$. Since V_d^0 is the complement of a hyperplane in an affine space when $d \geq 2g$ (with g the genus of K/k), the structure of the unit w_d for $d \geq 2g$ is simple: $w_d = b_d \ell_d^{e_d}$ for some $b_d \in k^\times$ and $e_d \in \mathbf{Z}$ with ℓ_d the unique linear form defining the hyperplane and satisfying $\ell_d(\varepsilon_{d+1-g}) = 1$. To prove Theorem 1.3, by Theorem 1.5 and (3.1) we only need to study the "discrete invariants" $b_d \bmod (k^\times)^2$ and $e_d \bmod 2$ thereby attached to w_d as d varies with $d \bmod 4$ fixed. This is done by algebraic methods in [2] in the case of genus 0, where explicit formulas are given for b_d and e_d as functions of $d \gg 0$ when using the standard monomial basis $\underline{\varepsilon} = \{1, u, u^2, \dots\}$ of $k[u]$. It is hopeless to find explicit formulas in general. Also, although $e_d \bmod 2$ is independent of $\underline{\varepsilon}$, the residue class $b_d \bmod (k^\times)^2$ enjoys no such independence in general unless $e_d \bmod 2$ vanishes. Thus, to study $b_d \bmod (k^\times)^2$ and $e_d \bmod 2$ we relate them to analogous discrete invariants attached to norm polynomials $\mathrm{N}_\pi(f) \in k[u][T^p]$ for many suitable finite flat maps $\pi : C \to \mathbf{A}^1$.

We now give a brief outline of the paper. In §2 we study the ideal I in Theorem 1.3. In §3, we use the results in §2 to define the unit w_d in Theorem 1.5 and to formulate a variant on Theorem 1.5 (see Theorem 3.6) that describes how the unit w_d varies with d when $p \neq 2$. In §4 we use deformation theory and the product formula for $\mathbf{G}_m$-valued local symbols to prove Theorem 1.5 (it follows from (4.10) and Theorem 4.5). Some "good" projections $\pi : C \to \mathbf{A}^1$ are constructed in §5, and these are used along with Theorem 1.5 to prove Theorem 3.6 in §6; this proof rests on analogous results proved in the case of genus 0 (by entirely different methods) in [2]. At the end of §6 we bring together these results and methods to prove Theorem 1.3.

Notation and Terminology. For two nonzero polynomials $f(T)$ and $g(T)$ in $\mathcal{A}[T]$, where $\mathcal{A}$ is a commutative ring, their resultant is denoted $R_{\mathcal{A}}(f, g) \in \mathcal{A}$. Usually $\mathcal{A} = A$ (the higher-genus ring under study). We write the degree of $f(T)$ as either $\deg f$ or $\deg_T f$. The context should remove any confusion due to the other meaning of deg as in (1.3). We refer to Definition 1.2 for our "total degree" notation $\deg_{u,T}$. The radical of an ideal J is denoted $\mathrm{Rad}(J)$. We write k for a general (perfect) field and κ for a finite field. If V is a finite-dimensional vector space over a field k then $\mathbf{P}(V) := \mathrm{Proj}(\mathrm{Sym}(V^\vee))$ is the projective space over k that classifies families of hyperplanes in V.

2. Branch points and squarefreeness

It will be technically useful both here and in geometric arguments in later sections to work with a ground field that is perfect and not necessarily finite, so we let k denote a perfect field of positive characteristic p (even allowing $p = 2$). We let C be a smooth and geometrically connected affine curve over k. Its coordinate ring is denoted A, so $C \simeq \mathrm{Spec}\, A$ and the function field $K = k(C)$ is the fraction field of A. In contrast with §1, we do not require C to have only one geometric point at infinity.

We now carry out a preliminary study of properties of the ideal I that was introduced in Theorem 1.3. The importance of this ideal is that it controls squarefreeness properties: for $f \in A[T]$ as in Theorem 1.3 and $a \in A$, the property of the ideal $(f(a))$ in A being squarefree only depends on $a \bmod I$. (This is made precise in Theorem 2.5.) As a consequence, the condition $\mu(f(a)) \neq 0$ is governed by the congruence class of $a \bmod I$. This is crucial in our later study of periodicity properties for $\mu(f(a))$ as a varies in A.

Definition 2.1. A nonzero $f \in A[T]$ is *primitive* over C (or with respect to A) if, for all closed points $c \in C$, the specialization $f_c \in k(c)[T]$ of $f \in A[T]$ is nonzero.

Pick a nonzero $f \in A[T]$ with $\deg_T f > 0$. Let

$$Z = Z_f = \mathrm{Spec}(A[T]/(f)) \hookrightarrow C \times \mathbf{A}^1_k \tag{2.1}$$

be the zero-scheme of f. The polynomial f is squarefree in $K[T]$ and primitive with respect to A if and only if Z_f is reduced and the projection $\mathrm{pr}_1 : Z_f \to C$ is quasi-finite. *Throughout this section we assume that the polynomial f in $A[T]$ is squarefree in $K[T]$ and primitive with respect to A, and that* $\deg_T f > 0$.

Since k is perfect, the (possibly reducible) curve $Z = Z_f$ is generically smooth over k. By consideration of each of the irreducible components of the reduced Z, we see that Z is flat over C.

We now assume $f \in A[T^p]$. This is equivalent to the geometric condition that the flat first projection $\mathrm{pr}_1 : Z \to C$ is non-étale at all generic points of Z (*i.e.*, pr_1 is nowhere étale). If $\{\phi_i\}$ is the set of monic irreducible factors of f in $K[T]$ then the ϕ_i's correspond bijectively to the irreducible components of Z, and $\phi_i \in K[T^p]$ for all i. Since $\deg_T \phi_i \geq p > 1$ for all i, $f(a) \in A$ is nonzero for all $a \in A$. Also, no ϕ_i lies in $k[T]$ because otherwise we would have $\phi_i \in k[T^p]$ and so by perfectness of k this ϕ_i would be a pth power, contrary to f being squarefree in $K[T]$. Thus, the projection $\mathrm{pr}_2 : Z \to \mathbf{A}^1_k$ is quasi-finite and flat.

Lemma 2.2. *For f and $Z = Z_f$ as above, the second projection $\mathrm{pr}_2 : Z \to \mathbf{A}^1_k$ is generically étale.*

Proof. We can assume k is algebraically closed, and it suffices to prove that for every $z \in Z(k)$ the finite flat induced map $\mathscr{O}^{\wedge}_{\mathbf{A}^1_k, \mathrm{pr}_2(z)} \to \mathscr{O}^{\wedge}_{Z,z}$ on complete local rings has étale generic fiber. By linear translation in T we can assume $\mathrm{pr}_2(z) = 0$. Letting u be a local parameter on C at $\mathrm{pr}_1(z)$, the map induced by pr_2 on complete local rings is a finite flat map $k[\![T]\!] \to k[\![u,T]\!]/(\varphi)$ where $\varphi \in k[\![u,T^p]\!]$. Moreover, the nonzero φ is squarefree in $k[\![u,T]\!]$ because $k[\![u,T]\!]/(\varphi) = \mathscr{O}^{\wedge}_{Z,z}$ is reduced (as Z is reduced and excellent). Using Weierstrass Preparation, we may suppose (by passage to a unit multiple) that φ is a monic Weierstrass polynomial in $k[\![T]\!][u]$ that is squarefree in $k[\![u,T]\!]$ and lies in $k[\![u,T^p]\!]$. Thus, the monic irreducible factorization of φ in $k(\!(T)\!)[u]$ consists of Weierstrass polynomials in $k[\![T^p]\!][u]$, so if the generic fiber $k(\!(T)\!)[u]/(\varphi)$ of the finite flat $k[\![T]\!]$-algebra $k[\![u,T]\!]/(\varphi) = k[\![T]\!][u]/(\varphi)$ has non-étale generic fiber then in $k[\![u,T]\!]$ the element φ is divisible by an element of

$k[\![T^p]\!][u] \cap k((T))[u^p] = k[\![u^p, T^p]\!]$ that is a non-unit in $k[\![u,T]\!]$. Such elements are pth powers of non-units in $k[\![u,T]\!]$, contradicting the condition that (φ) is a nonzero radical ideal in this ring. ■

By Lemma 2.2, $\Omega^1_{Z/\mathbf{A}^1_k}$ has finite support in Z. A natural scheme structure on this support is provided by the annihilator ideal of $\Omega^1_{Z/\mathbf{A}^1_k}$, and we call this k-finite scheme the *branch scheme* B for pr_2. We shall study the properties of the following ideal:

Definition 2.3. The ideal $I = I_f$ is the nonzero radical ideal in A whose zero locus in $C = \operatorname{Spec} A$ is the image of B under the projection $\mathrm{pr}_1 : Z = Z_f \to C$.

Example 2.4. If $A = k[u]$, then in the notation of [2, Def. 3.4], $I = (M_f^{\mathrm{geom}})$. Also, since k is perfect, the formation of I_f is compatible with any extension of the ground field.

We are interested in studying the prime factorization of the (nonzero) principal ideal $(f(a))$ in A as a varies. An element $\alpha \in A$ is called *squarefree* if $\alpha \neq 0$ and the ideal (α) is squarefree.

Theorem 2.5. *Let $f \in A[T^p]$ be squarefree in $K[T]$ and primitive with respect to A, and assume $\deg_T f > 0$. For any $a \in A$, $f(a)$ is not squarefree if and only if $a(c) = t$ in $k(x)$ for some $x = (c,t) \in B \subseteq Z \subseteq C \times \mathbf{A}^1_k$. In particular, the property that $f(a) \in A$ is squarefree only depends on the image of a in A/I.*

Proof. The nonzero ideal $(f(a))$ is squarefree if and only if the finite k-algebra $A/(f(a))$ is reduced. Since k is perfect, this property is equivalent to $A/(f(a))$ being étale over k, so we conclude that $f(a)$ is squarefree in A if and only if it is squarefree in $k' \otimes_k A$, where k'/k is any extension field. Thus, we may assume k is algebraically closed.

We wish to study the property that $\mathrm{ord}_c(f(a)) \geq 2$ for some closed point $c \in C$. Let D be a k-derivation of A that is nonzero in the cotangent space at c, so for any $a \in A$ we have $\mathrm{ord}_c(f(a)) \geq 2$ if and only if $f(a)$ and $D(f(a))$ vanish at c. Since a intervenes in $f(a)$ only through a^p (as $f \in A[T^p]$), we get the crucial identity

$$D(f(a)) = (Df)(a), \tag{2.2}$$

where $h \mapsto Dh$ is the $k[T]$-linear derivation of $A[T]$ that acts as D on A. Thus, $\mathrm{ord}_c(f(a)) \geq 2$ if and only if

$$f_c(a(c)) = (Df)_c(a(c)) = 0. \tag{2.3}$$

In particular, it is necessary that $z := (c, a(c)) \in C \times \mathbf{A}^1_k$ lies on Z.

Assuming $z \in Z$, we claim that (2.3) says exactly that $\mathrm{pr}_2 : Z \to \mathbf{A}^1_k$ is not étale at z (*i.e.*, $(c, a(c)) \in B$). Fix a local parameter u at c. On complete local rings, pr_2 induces a map

$$k[\![T - a(c)]\!] = \widehat{\mathscr{O}}_{\mathbf{A}^1_{k,a(c)}} \to \widehat{\mathscr{O}}_{Z,z} = \widehat{\mathscr{O}}_{C,c}[\![T - a(c)]\!]/(f) = k[\![u, T - a(c)]\!]/(f)$$

with D restricting to a unit multiple of ∂_u on $\widehat{\mathscr{O}}_{C,c} = k[\![u]\!]$. Hence, the vanishing conditions on f and Df at z say that $f(u, a(c))$ has vanishing linear and constant terms. The map $\mathrm{pr}_2 : Z \to \mathbf{A}^1_k$ has fiber scheme over $a(c)$ with artin local coordinate ring $k[\![u]\!]/(f(u, a(c)))$ at z, so $f(u, a(c)) = u^2(\cdots)$ if and only if $\mathrm{pr}_2^{-1}(a(c))$ is non-reduced at $z = (c, a(c))$, and since pr_2 is quasi-finite and flat such non-reducedness says that pr_2 is not étale at z. ■

A variant on the proofs of Lemma 2.2 and Theorem 2.5 yields the following result that will be used below and in our study of characteristic 2 in [3]; we omit the proof.

Theorem 2.6. *Suppose $h \in A[T]$ is primitive and has the property that $h(T^p)$ is squarefree of positive degree in $K[T]$. The zero-scheme $Z_h \subseteq C \times \mathbf{A}^1_k$ of h is a reduced curve with quasi-finite flat projections to C and $\mathbf{A}^1_k$, and $Z_h \to \mathbf{A}^1_k$ is generically étale. If $B \subseteq Z_h$ is the k-finite branch scheme of this latter projection, then for any $a \in A$ the nonzero $h(a^p) \in A$ is not squarefree if and only if $a(c)^p = t$ in $k(x)$ for some $x = (c,t) \in B$.*

3. Discriminants of finite algebras

Fix f as in Theorem 2.5 and assume $k = \kappa$ is a finite field with characteristic $p > 2$. By Theorem 2.5, to prove Theorem 1.3 over κ we may restrict attention to those $a \in A$ that lie in a congruence class of A/I on whose members the values of f are squarefree in A (so the finite κ-algebra $A/(f(a))$ is étale). For such a, we want a formula for $\mu(f(a)) = \pm 1$ other than the definition of $\mu(f(a))$. A preliminary such formula is provided by the generalized Swan identity from [2, Thm. 2.3] that we now recall:

Theorem 3.1. *Let R be a finite étale algebra over a finite field κ of odd characteristic. Set $\mu(R) = (-1)^{\#\operatorname{Spec}(R)} = \pm 1$. Let χ be the quadratic character on $\kappa^\times$ and let $\operatorname{disc}_\kappa R \in \kappa^\times/(\kappa^\times)^2$ be the discriminant of R. Then*

$$\mu(R) = (-1)^{\dim_\kappa R}\chi(\operatorname{disc}_\kappa R).$$

Applying Theorem 3.1 to $R = A/(f(a))$ for elements a as above (*i.e.*, a lies in a congruence class of A/I on which the values of f are squarefree), we have

$$\mu(f(a)) = (-1)^{\dim_\kappa(A/(f(a)))}\chi(\operatorname{disc}_\kappa(A/(f(a)))) \neq 0. \tag{3.1}$$

Our first task is to rewrite this formula in a manner that is well-suited to variation in a. In particular, although the discriminant of $A/(f(a))$ is just a coset in $\kappa^\times/(\kappa^\times)^2$, we need to promote it to an algebraic function of a.

It is now convenient to assume that k is merely a perfect field with arbitrary positive characteristic p. Let $\overline{C}$ be the unique k-smooth proper curve containing C as a dense open subset, and let g be the genus of $\overline{C}$. We now assume that $\overline{C} - C$ consists of a *single* k-rational point ξ. Letting $\operatorname{lead}(f) \in A - \{0\}$ denote the leading coefficient of f, the product formula on $\overline{C}$ gives the vector-space dimension formula

$$\begin{aligned}\dim(A/(f(a))) = -\operatorname{ord}_\xi(f(a)) &= \dim(A/(a)) \cdot \deg(f) + \dim(A/(\operatorname{lead}(f))) \\ &= (-\operatorname{ord}_\xi(a)) \cdot \deg(f) + \dim(A/(\operatorname{lead}(f))).\end{aligned} \tag{3.2}$$

provided that a has a pole of sufficiently high order at ξ (depending on $\deg_T f$ and the ξ-orders of the coefficients of $f \in A[T]$, so only depending on $\deg_{u,T} f$). Explicitly, if $f = \sum_{j=0}^m \alpha_j T^j$ with $m = \deg_T f$ and $\alpha_j \in A$ then (3.2) holds if $-\operatorname{ord}_\xi(a) > \nu(f)$, with

$$\nu(f) := \max_{0 \leq i \leq m-1} \frac{\operatorname{ord}_\xi(\alpha_m) - \operatorname{ord}_\xi(\alpha_i)}{m - i}; \tag{3.3}$$

note that for some $i < m$ we have $\alpha_i \neq 0$ because $f \in A[T^p]$ with f squarefree in $K[T]$ and $\deg_T f > 0$. Clearly $\nu(f)$ is unaffected by extension of the constant field k.

Consider nonzero elements a and a' in A such that $\operatorname{ord}_\xi(a) \equiv \operatorname{ord}_\xi(a') \bmod 2$ and both a and a' lie in a common congruence class of A/I whose representatives yield squarefree specialization for f. Clearly (3.1) and (3.2) reduce Theorem 1.3 to the problem of determining whether or not the ratio of the nonzero discriminants of the finite étale algebras $A/(f(a))$ and $A/(f(a'))$ is a square in the constant field when $p > 2$, k is finite, and both $-\operatorname{ord}_\xi(a)$ and $-\operatorname{ord}_\xi(a')$ are greater than $\nu(f)$. We now begin a study of such discriminants over any

perfect ground field k with any positive characteristic, with f satisfying the hypotheses in Theorem 2.5; we will not use oddness of the characteristic until the middle of §6 (where we prove Theorem 3.6), and some of what is done before this point will be used in the characteristic-2 setting in [3].

For $d \in \mathbf{Z}$, define $V_d = L(d \cdot \xi)$ to be the vector space of regular functions on C with at worst a pole of order d at ξ. We shall write

$$\underline{V}_d := \mathrm{Spec}(\mathrm{Sym}(V_d^\vee))$$

to denote the affine space over $\mathrm{Spec}\, k$ defined by V_d (so $\underline{V}_d(k') = k' \otimes_k V_d$ for any k-algebra k'). If $d \geq 2g-1$ then $\underline{V}_d$ has dimension $d+1-g$, and if $d \geq 2g$ then the inclusion $\underline{V}_{d-1} \hookrightarrow \underline{V}_d$ is a hyperplane (by Riemann–Roch). For $d \geq 0$, we define

$$\underline{V}_d^0 = \underline{V}_d - \underline{V}_{d-1} \subseteq \underline{V}_d$$

to be the open complement of $\underline{V}_{d-1}$ in $\underline{V}_d$ (so for $d \geq 2g$ and any extension field k' of k the set $\underline{V}_d^0(k')$ is the complement of the hyperplane $k' \otimes_k V_{d-1}$ in the k'-vector space $k' \otimes_k V_d$).

Provided that $d > \nu(f)$ (see (3.3)), it follows from (3.2) that for $a \in A$ with a pole of order d at ξ,

$$-\mathrm{ord}_\xi(f(a)) = \rho(d) := d \cdot \deg_T f + \dim_k(A/(\mathrm{lead}(f))). \tag{3.4}$$

Hence, for $d > \nu(f)$ the evaluation of $f \in A[T]$ at varying $a \in A$ defines a map of sets

$$V_d - V_{d-1} \to V_{\rho(d)} - V_{\rho(d)-1}. \tag{3.5}$$

To make the algebraic nature of this map precise, it will be convenient to relativize it as follows. For any k-scheme S, we write $\overline{C}_S, \xi_S$, and C_S to denote the base-changes of $\overline{C}, \xi$, and C to S, so C_S is the open complement of $\xi_S(S)$ in $\overline{C}_S$. For any $d \geq 0$, k-flatness of S yields the equality

$$\underline{V}_d(S) = \mathrm{H}^0(\overline{C}_S, \mathscr{O}_{\overline{C}_S}(d \cdot \xi_S)),$$

and the set $\underline{V}_d^0(S)$ is the subset of sections $\sigma \in \underline{V}_d(S)$ such that $\{1, \sigma\}$ generates $\mathscr{O}_{\overline{C}_S}(d \cdot \xi_S)$. By the universal property of $\mathbf{P}^1$, we can equivalently say that $\underline{V}_d^0(S)$ is (functorially in S) identified with the set of finite flat S-morphisms $\pi : \overline{C}_S \to \mathbf{P}^1_S$ of constant degree d such that $\pi^{-1}(\infty) = d \cdot \xi_S$ as relative effective Cartier divisors on $\overline{C}_S$.

Evaluation of $f \in A[T]$ defines a map from $\mathscr{O}_{C_S}$ back to itself as a sheaf of sets, and the relativization of (3.4) asserts that this evaluation carries $\underline{V}_d(S)$ into $\underline{V}_{\rho(d)}(S)$ for $d > \nu(f)$ and carries $\underline{V}_d^0(S)$ into $\underline{V}_{\rho(d)}^0(S)$ for such d; this relativization is easily verified on geometric points, and the general case follows since $\underline{V}_\delta^0$ is an open subscheme of $\underline{V}_\delta$ for all δ. For $d > \nu(f)$, we thereby get a k-morphism

$$f : \underline{V}_d^0 \to \underline{V}_{\rho(d)}^0 \tag{3.6}$$

inducing (3.5) on k-points.

Our goal is to study

$$a \mapsto \mathrm{disc}_k(A/(f(a)))$$

as an algebraic function $\underline{V}_d^0 \to \mathbf{A}^1_k$ for $d > \nu(f)$, so the first problem we need to address is how to systematically compute such discriminants *without* unit-square ambiguity.

Choose a basis $\{\varepsilon_1, \ldots, \varepsilon_g\}$ of V_{2g-1} whose elements have increasing pole-order at ξ, and for $d \geq 2g$ choose a representative $\varepsilon_{d-g+1} \in V_d$ for a basis of the 1-dimensional quotient space V_d/V_{d-1}.

Let $0 = w_1 < \cdots < w_g \leq 2g-1$ be the Weierstrass gap sequence at ξ; that is, for $d \leq 2g-1$ we have $V_{d-1} \neq V_d$ if and only if $d \in \{w_1, \ldots, w_g\}$. Hence, $-\mathrm{ord}_\xi(\varepsilon_r) = w_r$ for $r \leq g$, so $-\mathrm{ord}_\xi(\varepsilon_i)$ is strictly increasing in i and $-\mathrm{ord}_\xi(\varepsilon_i) = i+g-1$ for $i > g$. Since $A = \cup V_d$, we get a basis $\{\varepsilon_1, \varepsilon_2, \ldots\}$ of A as a k-vector space. For $d \geq 2g$, an element $\alpha \in A - \{0\}$ with $-\mathrm{ord}_\xi(\alpha) = d$ (*i.e.*, $\alpha \in V_d^0$) is uniquely written as $\alpha = \sum_{j \leq d+1-g} c_j(\alpha)\varepsilon_j$ with $c_{d+1-g}(\alpha) \neq 0$. An important point is that for *all* α with pole order at ξ equal to a fixed $d \geq 2g$ we can use the *same* d-element subset of $\{\varepsilon_1, \ldots, \varepsilon_{d+g}\}$ to represent a basis of the finite k-algebra $A/(\alpha)$. This is an analogue of the division algorithm in $k[u]$ (using $\varepsilon_i = u^{i-1}$), and it is influenced by the nature of Weierstrass gaps at ξ:

Lemma 3.2. *Fix $d \geq 2g$. For all $\alpha \in A$ with $-\mathrm{ord}_\xi(\alpha) = d$, a set of representatives of a k-basis of $A/(\alpha)$ is given by*

$$\{\varepsilon_1, \ldots, \varepsilon_{d+g}\} - \{\varepsilon_{d+w_r+1-g}\}_{1 \leq r \leq g}. \tag{3.7}$$

Proof. By the product formula, $\dim_k A/(\alpha) = -\mathrm{ord}_\xi(\alpha) = d$. Since the set (3.7) has size d, it suffices to check it has linearly independent image in $A/(\alpha)$. Suppose there is a linear combination $\sum_{m \leq d+g} c_m \varepsilon_m \in V_{d+2g-1}$ that lies in (α), where $c_m = 0$ whenever $m = d+w_r+1-g$ for some $1 \leq r \leq g$. We want $c_m = 0$ for all m. The ideal (α) has k-basis given by the $\alpha\varepsilon_i$'s. Since $-\mathrm{ord}_\xi(\alpha\varepsilon_i) = d - \mathrm{ord}_\xi(\varepsilon_i)$ is strictly increasing in i, for a k-linear combination $\sum b_j \alpha\varepsilon_{i_j}$ with pairwise distinct i_j's and all b_j in $k^\times$ we have $\sum b_j \alpha\varepsilon_{i_j} \in V_\delta$ if and only if all $\alpha\varepsilon_{i_j}$'s lie in V_δ. We are interested in the case $\delta = d+2g-1$, and clearly the only $\alpha\varepsilon_i$'s lying in V_{d+2g-1} are the $\alpha\varepsilon_r$'s with $-\mathrm{ord}_\xi(\varepsilon_r) \leq 2g-1$, which is to say that such an $\alpha\varepsilon_i$ is one of the elements $\alpha\varepsilon_1, \ldots, \alpha\varepsilon_g$. For $1 \leq r \leq g$, clearly $\alpha\varepsilon_r \in V_{d+w_r}^0$.

Thus, we get a linear equation

$$\sum_{m=1}^{d+g} c_m \varepsilon_m - \sum_{r=1}^{g} c_r' \alpha\varepsilon_r = 0 \tag{3.8}$$

with $c_1', \ldots, c_g' \in k$. Since $c_m = 0$ whenever $m = d + w_s + 1 - g$ for some $1 \leq s \leq g$, in which case $m \geq g+1$ and hence $-\mathrm{ord}_\xi(\varepsilon_m) = m+g-1 = d+w_s$ runs over the set of pole-orders of the $\alpha\varepsilon_r$'s at ξ for $1 \leq r \leq g$, any two terms in (3.8) with a nonzero coefficient have distinct pole orders at ξ. Thus, the vanishing of (3.8) forces all coefficients in (3.8) to vanish. ■

Here is the analogue of Lemma 3.2 over k-schemes.

Lemma 3.3. *For $d \geq 2g$, any k-scheme S, and any $a \in \underline{V}_d^0(S)$, the zero-scheme Z_a of a on C_S has structure map $\mathrm{pr} : Z_a \to S$ that is finite and locally free of rank d, and $\mathrm{pr}_*\mathscr{O}_{Z_a}$ is a finite free $\mathscr{O}_S$-module with basis represented by* (3.7)*.*

Proof. Since Z_a is the zero-scheme of a fiberwise nonvanishing section a of a line bundle $\mathscr{O}_{\overline{C}_S}(d \cdot \xi_S)$ on a proper smooth S-curve $\overline{C}_S$ whose geometric fibers are connected, the proper map $Z_a \to S$ must be quasi-finite and hence finite. Thus, the formation of $\mathrm{pr}_*\mathscr{O}_{Z_a}$ commutes with base change on S. Lemma 3.2 implies that the fiber of Z_a over each $s \in S$ has rank d and that (3.7) projects to a set of global sections of $\mathscr{O}_{Z_a} = \mathscr{O}_{C_S}/(a)$ that, as a set of sections of the $\mathscr{O}_S$-module $\mathrm{pr}_*\mathscr{O}_{Z_a}$, induces a $k(s)$-basis on the s-fiber for all $s \in S$. Hence, it remains to show that the finite and finitely presented S-scheme Z_a is flat (then $\mathrm{pr}_*\mathscr{O}_{Z_a}$ will be a locally free $\mathscr{O}_S$-module, necessarily of rank d with (3.7) necessarily providing a global basis). This S-flatness problem is intrinsic to the section $a|_{C_S}$ of $\mathscr{O}_{C_S}$ since Z_a is disjoint from $\xi_S(S)$ (because $a \in \underline{V}_d^0(S)$ is a generating section of $\mathscr{O}(d \cdot \xi_S)$ near $\xi_S(S)$). We

may reduce to the case of noetherian S. By the local flatness criterion, the S-flatness of $\mathscr{O}_{Z_a} = \mathscr{O}_{C_S}/(a)$ follows from the S-flatness of C_S and the fact that the induced section a_s of each fiber-sheaf $\mathscr{O}_{C_s}$ is a regular section (*i.e.*, nowhere a zero divisor). ■

For $d \geq 2g$ and a k-scheme S, pick a section $a \in \underline{V}_d^0(S)$. By Lemma 3.3, the S-finite zero-scheme Z_a in C_S has structure sheaf $\mathscr{O}_{Z_a} = \mathscr{O}_{C_S}/(a)$ that we view as a finite free $\mathscr{O}_S$-module of rank d (we suppress the pushforward notation relative to the finite structure map $Z_a \to S$). We wish to compute $\mathrm{disc}_S(\mathscr{O}_{Z_a})$ as a global section of $\mathscr{O}_S$ by using a basis that is independent of a. More specifically, we define this discriminant to be a determinant relative to the ordered $\mathscr{O}_S$-basis (3.7) of $\mathscr{O}_{Z_a}$ provided by Lemma 3.3. Let us write $\mathrm{disc}_{S,\underline{\varepsilon}}(\mathscr{O}_{Z_a})$ for this well-defined section of $\mathscr{O}_S$.

Since we are using a choice of basis that is independent of a and is compatible with base change on S, the construction

$$a \mapsto \mathrm{disc}_{S,\underline{\varepsilon}}(\mathscr{O}_{Z_a}) \tag{3.9}$$

from $\underline{V}_d^0(S)$ to $\Gamma(S, \mathscr{O}_S)$ defines a k-scheme morphism

$$\mathrm{disc}_{\underline{\varepsilon},d} : \underline{V}_d^0 \to \mathbf{A}_k^1 \tag{3.10}$$

for $d \geq 2g$. We will be interested in the composite

$$\mathrm{disc}_{\underline{\varepsilon},\rho(d)} \circ f : \underline{V}_d^0 \to \mathbf{A}_k^1 \tag{3.11}$$

which makes sense for $d > \max(\nu(f), 2g)$ by (3.6).

For $d \geq 2g$, the specification of the basis $\varepsilon_1, \ldots, \varepsilon_{d+1-g}$ for V_d gives an identification

$$\underline{V}_d \simeq \mathrm{Spec}\, k[c_1, \ldots, c_{d+1-g}]$$

where $\{c_j\}_{j \leq d+1-g}$ is the dual basis to $\{\varepsilon_j\}_{j \leq d+1-g}$, so we have a coordinatization

$$\underline{V}_d^0 \simeq \mathrm{Spec}\, k[c_1, \ldots, c_{d+1-g}][1/c_{d+1-g}]$$

for the complement of the hyperplane $\underline{V}_{d-1} = \{c_{d+1-g} = 0\}$. In terms of such coordinates, we can concretely summarize the construction (3.10) as follows: for each extension field k'/k and $a \in A' = k' \otimes_k A$ with pole-order $d \geq 2g$ at ξ, we have computed $\mathrm{disc}_{k'}(A'/(a)) \in k'$ as an *algebraic* function of the $\underline{\varepsilon}$-coordinates of $a = \sum_{j \leq d+1-g} c_j(a)\varepsilon_j$ with $c_{d+1-g}(a)$ invertible. If we change our initial basis $\underline{\varepsilon} = \{\varepsilon_i\}$ to another basis $\underline{\varepsilon}' = \{\varepsilon_i'\}$ then for $d \geq 2g$ and $a \in \underline{V}_d^0(S)$ the invertible change-of-basis matrix between the two resulting $\mathscr{O}_S$-module bases of $\mathscr{O}_{Z_a}$ has entries in $\Gamma(S, \mathscr{O}_S)$ that depend functorially on a. We conclude that the algebraic function $\mathrm{disc}_{\underline{\varepsilon}',d}$ on $\underline{V}_d^0$ is a unit-square multiple of the algebraic function $\mathrm{disc}_{\underline{\varepsilon},d}$.

The following definition uses the finite branch scheme provided by Theorem 2.5.

Definition 3.4. For each point $x = (u_x, t_x) \in C \times \mathbf{A}_k^1$ in the k-finite branch scheme B of $\mathrm{pr}_2 : Z \to \mathbf{A}_k^1$ and for each $d \geq 0$, let $P_{x,d} : \underline{V}_d \to \mathbf{A}_k^1$ be the algebraic function defined functorially on k'-points by

$$a \mapsto P_{x,d}(a) = \mathrm{N}_{k' \otimes_k k(x)/k'}(a(u_x) - 1 \otimes t_x) \in k' \tag{3.12}$$

for k-algebras k' and $a \in \underline{V}_d(k') = k' \otimes_k V_d \subseteq k' \otimes_k A$, with $a(u_x)$ denoting the image of a under the natural map $k' \otimes_k A \twoheadrightarrow k' \otimes_k k(u_x) \subseteq k' \otimes_k k(x)$.

We view $P_{x,d}$ as an element of the coordinate ring of $\underline{V}_d$, a polynomial ring over k. If k'/k is an extension over which x splits into physical points $\{x_i'\}$ then $k' \otimes_k k(x) \simeq \prod_i k'(x_i')$ since $k(x)/k$ is separable (as k is perfect), and so we have a compatible factorization $P_{x,d} = \prod_i P_{x_i',d}$ as algebraic functions on $\underline{V}_{d/k'}$. This simple behavior of $P_{x,d}$'s with respect to

extension of k will be implicitly used without comment when we enlarge the ground field in later arguments. The coordinate ring of $\underline{V}_d$ is a unique factorization domain. How does $P_{x,d}$ factor in this ring?

Lemma 3.5. *For positive $d \geq 2g$, $P_{x,d}$ is irreducible in the coordinate ring of $\underline{V}_d$ and, for $x \neq x'$, the elements $P_{x,d}$ and $P_{x',d}$ in this coordinate ring are not unit multiples of each other. Geometrically, the zero schemes $\{P_{x,d} = 0\}$ for $x \in B$ are pairwise-distinct irreducible and reduced hypersurfaces in $\underline{V}_d$.*

Proof. The finite separable extension $k(x)/k$ is a quotient of $k(u_x) \otimes_k k(t_x)$, and hence is generated over k by $k(u_x)$ and $k(t_x)$. Consider the polynomial function of degree 1

$$\ell_x : a = \sum_{j \leq d+1-g} c_j \varepsilon_j \mapsto \sum c_j \varepsilon_j(u_x) - t_x = a(u_x) - t_x \in k(x)$$

on $k(x) \otimes_k V_d$, where t_x is the image of T in the residue field at $x \in C \times \mathbf{A}^1_k$. The norm map of symmetric algebras $\mathrm{Sym}(k(x) \otimes_k V_d^\vee) \to \mathrm{Sym}(V_d^\vee)$ carries ℓ_x to $P_{x,d}$. It is obvious that ℓ_x is nonconstant for positive $d \geq 2g$, since by Riemann–Roch we can find elements $a_1, a_2 \in k(x) \otimes_k V_d$ with $a_1(u_x) = 0$ and $a_2(u_x) \neq 0$ for such d. Hence, $P_{x,d}$ is nonconstant for such d.

To prove the irreducibility of $P_{x,d}$ over k it is equivalent to prove that for a Galois extension k'/k into which $k(x)/k$ embeds, distinct k-embeddings $\sigma, \sigma' : k(x) \rightrightarrows k'$ carry ℓ_x to polynomials on $k(x) \otimes_k V_d$ of degree 1 that are not scalar multiples of each other. Pick k' and choose k-embeddings $\sigma, \sigma' : k(x) \rightrightarrows k'$. Suppose there exists $\theta \in {k'}^\times$ such that $\sigma(\ell_x) = \theta \cdot \sigma'(\ell_x)$, so $\sigma(t_x) = \theta \cdot \sigma'(t_x)$ and $\sigma(\varepsilon_j(u_x)) = \theta \cdot \sigma'(\varepsilon_j(u_x))$ for $1 \leq j \leq d+1-g$. We need to prove that $\sigma = \sigma'$. Taking $j = 1$ gives $\varepsilon_j(u_x) \in k^\times$, so $\theta = 1$. Since $d > 0$ and $d \geq 2g$, V_d generates A as a k-algebra. Thus, $\{\varepsilon_1(u_x), \ldots, \varepsilon_{d+1-g}(u_x)\}$ generates the k-algebra quotient $k(u_x)$ of A. Hence, we get that $\sigma|_{k(u_x)} = \sigma'|_{k(u_x)}$, so σ and σ' coincide because $k(x)$ is generated over k by $k(u_x)$ and $k(t_x)$. This proves the irreducibility of $P_{x,d}$ over k.

To see that the $P_{x,d}$'s are not unit multiples of each other as we vary x (with fixed positive $d \geq 2g$), unique factorization allows us to pass to the case of algebraically closed k, where we just have to show that the polynomials ℓ_x and $\ell_{x'}$ of degree 1 are not scalar multiples of each other for $x \neq x'$. Equivalently, we want ℓ_x and $\ell_{x'}$ to have distinct zero loci in V_d. Since $d > 0$ and $d \geq 2g$, by Riemann–Roch we can find $a \in V_d$ with $a(u_x) = t_x$ and $a(u_{x'}) \neq t_{x'}$. Hence, $\ell_x(a) = 0$ and $\ell_{x'}(a) \neq 0$. ∎

Since the nonzero radical ideal $I \subseteq A$ as in Definition 2.3 cuts out the reduced locus in C whose support is the union of the u_x's, we see via (3.12) that $P_{x,d}(a)$ only depends on a modulo I. Write $P^0_{x,d}$ to denote $P_{x,d}|_{\underline{V}^0_d}$. For fixed positive $d \geq 2g$ and varying $x \in B$, Lemma 3.5 ensures that the $P_{x,d}$'s have distinct (nonempty) irreducible zero-loci on $\underline{V}_d$. By Riemann–Roch, none of these zero-loci are contained in the hyperplane $\underline{V}_{d-1}$, so the $P^0_{x,d}$'s are nonassociate irreducibles in the coordinate ring of the hyperplane complement $\underline{V}^0_d = \underline{V}_d - \underline{V}_{d-1}$. For our purposes, the importance of the irreducible zero-loci $\{P^0_{x,d} = 0\}$ in $\underline{V}^0_d$ is that, for $d > \max(\nu(f), 2g)$, Theorem 2.5 identifies the union of these irreducible hypersurfaces with the locus of points $a \in \underline{V}^0_d(k')$ (for varying field extensions k'/k) such that $(k' \otimes_k A)/(f(a))$ is non-étale over k'.

The unit group of the coordinate ring $\mathscr{O}(\underline{V}_d^0) \simeq k[c_1, \ldots, c_{d+1-g}][1/c_{d+1-g}]$ of $\underline{V}_d^0$ fits into a canonical short exact sequence

$$1 \longrightarrow k^\times \longrightarrow \mathscr{O}(\underline{V}_d^0)^\times \xrightarrow{\mathrm{ord}_{\underline{V}_{d-1}}} \mathbf{Z} \longrightarrow 0 \tag{3.13}$$

(using the normalized order-function at the generic point η_{d-1} of $\underline{V}_{d-1}$ in $\underline{V}_d$).

Using the UFD property of $\mathscr{O}(\underline{V}_d^0)$ and the structure of $\mathscr{O}(\underline{V}_d^0)^\times$ as in (3.13) for such d, there exist unique $b_{d,\underline{\varepsilon}} \in k^\times$, $e_{d,\underline{\varepsilon}} \in \mathbf{Z}$, and positive integers $e_{x,d,\underline{\varepsilon}}$ such that

$$\mathrm{disc}_{\underline{\varepsilon},\rho(d)} \circ f = b_{d,\underline{\varepsilon}} c_{d+1-g}^{e_{d,\underline{\varepsilon}}} \prod_{x \in B} (P_{x,d}^0)^{e_{x,d,\underline{\varepsilon}}} \tag{3.14}$$

in the coordinate ring of $\underline{V}_d^0$. Here we have fixed $\underline{\varepsilon} = \{\varepsilon_i\}$ to define the discriminant function on the left side of (3.14), and c_{d+1-g} is the dual functional to ε_{d+1-g} with respect to the resulting basis $\{\varepsilon_1, \ldots, \varepsilon_{d+1-g}\}$ of V_d. We emphasize that (3.14) is an equality of algebraic functions on $\underline{V}_d^0$ and *not* on $\underline{V}_d$ because the function $\mathrm{disc}_{\underline{\varepsilon},\delta}$ is only defined on the open locus $\underline{V}_\delta^0$ in $\underline{V}_\delta$ for varying δ. By (3.1), the proof of Theorem 1.3 will require a good understanding of the abstract exponents in (3.14) as d and $\underline{\varepsilon}$ vary.

Since $\mathscr{O}(\underline{V}_d^0)$ is a UFD, the exponents $e_{x,d,\underline{\varepsilon}}$ in (3.14) are independent of the coordinatization $\underline{\varepsilon}$ because they are the exponents for an irreducible factorization of a nonzero element of $\mathscr{O}(\underline{V}_d^0)$ that is intrinsic up to unit-square factor in $\mathscr{O}(\underline{V}_d^0)$ and the $P_{x,d}$'s are independent of coordinates. Thus, we shall now write $e_{x,d}$ rather than $e_{x,d,\underline{\varepsilon}}$.

Changing the basis $\underline{\varepsilon}$ changes the left side of (3.14) by a unit square on $\underline{V}_d^0$, so $e_{d,\underline{\varepsilon}}$ mod 2 is independent of $\underline{\varepsilon}$. However, $e_{d,\underline{\varepsilon}} \in \mathbf{Z}$ is not independent of $\underline{\varepsilon}$, due to the description (3.13) of $\mathscr{O}(\underline{V}_d^0)^\times$ as the product of $k^\times$ and the infinite cyclic group of powers of a defining equation for the hyperplane V_{d-1} in V_d. Unfortunately, $b_{d,\underline{\varepsilon}}$ mod $(k^\times)^2$ does depend on $\underline{\varepsilon}$ in general, so we must keep track of $\underline{\varepsilon}$ when using (3.14), but if $e_{d,\underline{\varepsilon}}$ mod 2 vanishes (a condition that is independent of $\underline{\varepsilon}$) then $b_{d,\underline{\varepsilon}}$ mod $(k^\times)^2$ is independent of $\underline{\varepsilon}$.

For ease of notation we shall now write b_d and e_d instead of $b_{d,\underline{\varepsilon}}$ and $e_{d,\underline{\varepsilon}}$; however, we must not forget the dependence on $\underline{\varepsilon}$. Note that the parity of the differences $e_d - e_{d'}$ is independent of $\underline{\varepsilon}$ since the parities of e_d and $e_{d'}$ are independent of $\underline{\varepsilon}$ (even though $e_d, e_{d'} \in \mathbf{Z}$ depend on $\underline{\varepsilon}$). The parity of such differences will be our main focus of study in the proof of Theorem 1.3.

It is difficult to analyze e_d mod 2 directly in the higher-genus case, and the structure of the constant b_d seems to be beyond the reach of geometric methods (*e.g.*, for genus zero we can say little about $b_{d,\underline{\varepsilon}}$ except when $\underline{\varepsilon} = \{u^{i-1}\}_{i \geq 1}$ is the monomial basis with respect to some global coordinate u on the affine line). We saw in [2] that for finite k the source of mod-4 periodicity properties for average values of $a \mapsto \mu(f(a))$ in the genus-zero case is entirely due to the dependence of b_d mod $(k^\times)^2$ on d mod 4 and the dependence of e_d mod 2 on d mod 2 for large d, and our understanding of such dependence is restricted to the case $\underline{\varepsilon} = \{u^{i-1}\}$ for which there are formulas for $e_{d,\underline{\varepsilon}} \in \mathbf{Z}$ and $b_{d,\underline{\varepsilon}} \in k^\times$ (see [2, Thm. 4.1]). Thus, the proof of Theorem 1.3 will require more work beyond the identification of the exponents $e_{x,d}$ in (3.14) as branch-scheme multiplicities in Theorem 1.5.

By (3.14), to prove Theorem 1.3 we are motivated to show that for *finite* k of odd characteristic and d and d' in the same congruence class mod 2 the difference $e_d - e_{d'}$ is even provided that d and d' are large enough (where "large" depends only on the total degree $\deg_{u,T} f$ of f and the genus g of K/k). It is also necessary to understand the dependence

of $b_d \bmod (k^\times)^2$ on $d \bmod 4$ for such large d. Both of these problems have a satisfactory solution in odd characteristic without finiteness restrictions on the base field:

Theorem 3.6. *Under the hypotheses as in Theorem* 1.5*, assume also that* $p > 2$*. With notation as above, the difference* $e_d - e_{d'}$ *is even when* $d \equiv d' \bmod 2$ *and* $d, d' \gg 0$*, and if the common parity of such* e_d *and* $e_{d'}$ *is even then the ratio* $b_d/b_{d'}$ *is a square in* $k^\times$ *when* $d \equiv d' \bmod 4$ *and* $d, d' \gg 0$*. If* $-1 \in k^\times$ *is a square or* $\deg_T f$ *is even, then* $b_d/b_{d'}$ *is a square in* $k^\times$ *if* e_d *and* $e_{d'}$ *are even with* $d \equiv d' \bmod 2$ *and* $d, d' \gg 0$*. These largeness conditions on* d *and* d' *depend only on the total degree* $\deg_{u,T} f$ *and the genus* g*.*

Remark 3.7. The proof of Theorem 1.3 only requires Theorem 3.6 in the case of finite fields, and we do not know any application of Theorem 3.6 in the generality of infinite perfect fields. Hence, we will only prove Theorem 3.6 for finite base fields and we leave it as an exercise for the interested reader to work out the reduction of the general case to the case of finite fields by using EGA-style direct limit methods. The two interesting points in the reduction step are: (i) the setup over k is *not* finitely presented over $\mathbf{F}_p$, due to the choice of the infinitely many ε_i's, and (ii) to prove that the ratio $b_d/b_{d'}$ is a square when e_d and $e_{d'}$ are even, one needs to show that if a unit u on a normal scheme X of finite type over $\mathbf{F}_p$ is an nth power in the residue field at each closed point of X then u is an nth power on X when $p \nmid n$.

To handle (ii) one uses the Lang–Weil estimate. For (i) the key observation is that for each irreducible factor $P^0_{x,d+1}$ of $\mathrm{disc}_{\underline{\varepsilon},\rho(d+1)} \circ f$ on $\underline{V}^0_{d+1}$, the irreducible zero-locus of $P^0_{x,d+1}$ on $\underline{V}^0_{d+1}$ has Zariski closure in $\underline{V}_{d+1}$ that is the zero locus of $P_{x,d+1}$, and for $d \geq 2g$ this closure meets the hyperplane $\underline{V}_d$ in the zero locus of $P_{x,d+1}|_{\underline{V}_d} = P_{x,d}$. In this way, $P^0_{x,d+1}$ determines $P^0_{x,d}$ for $d > \max(\nu(f), 2g)$, and this mechanism for relating irreducible factorizations in coordinate rings of *disjoint* varieties $\underline{V}^0_d$ for different d's is independent of $\underline{\varepsilon}$.

The assertion in Theorem 3.6 is independent of the choice of $\underline{\varepsilon}$ because $e_d \bmod 2$ is independent of $\underline{\varepsilon}$, as is $b_d \bmod (k^\times)^2$ when e_d is even. This is important because the strategy for proving Theorem 3.6 is to make choices of $\underline{\varepsilon}$ adapted to some well-chosen projections $\pi : \overline{C} \to \mathbf{P}^1_k$ that will enable us to pull up results from the genus-0 case that we settled in [2, Thm. 4.1]. The proof of Theorem 3.6 (for finite k) is given in §6, building on preliminary work in §5 where we construct the necessary projections. In contrast with our proofs of Theorems 1.3 and 3.6 in §6, our proof of Theorem 1.5 in the next section does not use reduction to the case of genus 0.

4. Factoring discriminants and norms

The main results we establish in this section are a factorization for a kind of generalized discriminant (Theorem 4.4) and a refinement that determines the exponents in this factorization (Theorem 4.5). The second of these two results yields Theorem 1.5 as a special case (as we explain below (4.10)). We emphasize at the outset that it is essential that we prove Theorems 4.4 and 4.5 without restriction on the characteristic because these results shall be applied over 2-adic fields in [3].

The starting point for our proof of Theorem 1.5 is a generalization of the classical identity

$$\mathrm{disc}(k[u]/(h)) = \frac{(-1)^{d(d-1)/2}}{\mathrm{lead}(h)^d} \cdot \prod_\rho h'(\rho) = \frac{(-1)^{d(d-1)/2}}{\mathrm{lead}(h)^d} \cdot \mathrm{N}_{(k[u]/(h))/k}(h') \tag{4.1}$$

for a nonzero polynomial $h \in k[u]$ of degree $d \geq 1$ over any field k, with the discriminant computed relative to the ordered k-basis $\{1, u, \ldots, u^{d-1}\}$ of $k[u]/(h)$ and ρ running through the set of roots of h in a splitting field.

To set up the geometric generalization of (4.1) for higher genus, given in Theorem 4.1, we now let k be an arbitrary field (possibly of characteristic 0, such as a 2-adic field) and as usual we fix a smooth proper geometrically connected curve $\overline{C}$ of genus g over k and we let $\xi \in \overline{C}(k)$ be a rational point. We let A denote the coordinate ring of the affine complement $C = \overline{C} - \{\xi\}$, and as in §3 we define $\underline{V}_d$ and $\underline{V}_d^0 = \underline{V}_d - \underline{V}_{d-1}$ in terms of C and ξ. Fix a nonzero vector field on C, and identify it with a nonzero k-linear derivation $D : A \to A$. Let $Z(D) \subseteq C$ be the k-finite zero-scheme of this vector field.

For $d \geq 2g$, we functorially define algebraic functions

$$\mathrm{N}_{Z(D)/k,d} : \underline{V}_d \to \mathbf{A}^1_k, \;\; \mathrm{N}_{D,d} : \underline{V}_d^0 \to \mathbf{A}^1_k$$

on points valued in k-algebras k' as follows:

$$\mathrm{N}_{Z(D)/k,d}(a) = \mathrm{N}_{Z(D)_{k'}/k'}(a) \in k', \;\; \mathrm{N}_{D,d}(a^0) = \mathrm{N}_{((k' \otimes_k A)/(a^0))/k'}(Da^0) \in k' \tag{4.2}$$

for $a \in \underline{V}_d(k') = k' \otimes_k V_d$ and $a^0 \in \underline{V}_d^0(k')$; recall from Lemma 3.3 that $(k' \otimes_k A)/(a^0)$ is a finite free k'-module of rank d, since $d \geq 2g$. When $Z(D)$ is empty, $\mathrm{N}_{Z(D)/k,d}$ denotes the constant function 1.

By Riemann–Roch, $\mathrm{N}_{Z(D)/k,d}$ is nonconstant for $d \geq 2g$ if $Z(D)$ is nonempty. Using Bertini's theorem over an algebraic closure $\overline{k}$ of k, when $d \geq 2g+1$ (so the linear system $|d \cdot \xi|$ is very ample) there exists $a^0 \in \underline{V}_d^0(\overline{k})$ with an étale divisor of zeros that is disjoint from $Z(D)_{\overline{k}}$, so Da^0 is nonvanishing everywhere along the étale zero-locus of a^0 and hence $\mathrm{N}_{D,d}(a^0) \neq 0$. Thus $\mathrm{N}_{D,d} \neq 0$ for $d \geq 2g+1$.

Upon choosing a k-basis $\underline{\varepsilon}$ of A adapted to the V_d's as in §3, we define the algebraic function $\mathrm{disc}_{\underline{\varepsilon},d}$ on $\underline{V}_d^0$ as in (3.9). The generalization of (4.1) is:

Theorem 4.1. *Fix a choice of $\underline{\varepsilon}$ and let $e_{D,d} = 2g - 2 - \mathrm{ord}_\xi(D) - d \in \mathbf{Z}$. For $d \geq 2g+2$, there exists $b_{D,d,\underline{\varepsilon}} \in k^\times$ such that*

$$\mathrm{N}_{Z(D)/k,d} \cdot \mathrm{disc}_{\underline{\varepsilon},d} = b_{D,d,\underline{\varepsilon}} c_{d+1-g}^{e_{D,d}} \cdot \mathrm{N}_{D,d} \tag{4.3}$$

as algebraic functions on $\underline{V}_d^0$.

In the special case $C = \mathbf{A}^1_k = \mathrm{Spec}\, k[u]$, $\varepsilon_i = u^{i-1}$, and $D = \partial_u$, we have $Z(D) = \emptyset$ and $e_{D,d} = -d$, so (4.3) recovers (4.1) for $d \geq 2$ by taking $b_{D,d,\underline{\varepsilon}} = (-1)^{d(d-1)/2}$. It follows that in this specific genus-zero case $b_{D,d,\underline{\varepsilon}}$ only depends on d through the congruence class d mod 4, but for higher genus we do not expect there to exist an $\underline{\varepsilon}$ and D such that dependence of $b_{D,d,\underline{\varepsilon}}$ mod $(k^\times)^2$ on d is as simple as it is in genus 0 with $\underline{\varepsilon} = \{u^{i-1}\}$ and $D = \partial_u$. For ease of notation, we shall write $b_{D,d}$ rather than $b_{D,d,\underline{\varepsilon}}$, but we must not forget the dependence on $\underline{\varepsilon}$.

Proof. An equivalent formulation of (4.3) is the statement that the nonzero rational function

$$\frac{\mathrm{N}_{Z(D)/k,d} \cdot \mathrm{disc}_{\underline{\varepsilon},d}}{c_{d+1-g}^{e_{D,d}} \cdot \mathrm{N}_{D,d}} \in k(\underline{V}_d^0)^\times$$

is in $k^\times$. Since k is algebraically closed in the function field of $\underline{V}_d^0$, it suffices to prove the theorem after base-change to an algebraic closure of k. Thus, we now suppose that k is algebraically closed.

The k-rational zeros of the left side of (4.3) consist of those $a \in A$ with $\mathrm{ord}_\xi(a) = -d$ such that $A/(a)$ is non-reduced or a vanishes at a zero of D. This is exactly the condition that Da and a have a common zero on C, which says precisely that the image of Da in the finite k-algebra $A/(a)$ has vanishing norm. Hence, the zero loci of the nonzero functions $\mathrm{N}_{Z(D)/k} \cdot \mathrm{disc}_{\underline{\varepsilon},d}$ and $\mathrm{N}_{D,d}$ on $\underline{V}_d^0$ are the same. Granting for a moment that these functions have the same multiplicities at the generic points of their common zero locus, the structure (3.13) of units on the regular variety $\underline{V}_d^0$ then yields (4.3) up to the determination of the exponent $e_{D,d} \in \mathbf{Z}$. In order to compute $e_{D,d}$, we evaluate both sides of (4.3) at λa with $\lambda \in k^\times$ and $a \in V_d^0$. The left side acquires the multiplier $\lambda^{\deg Z(D)}$ and the right side acquires the multiplier $\lambda^{e_{D,d}+\dim_k A/(a)}$. Thus, $e_{D,d} = \deg Z(D) - \dim_k A/(a) = 2g-2-\mathrm{ord}_\xi(D)-d$, as desired.

It remains to compare generic multiplicities. For each $z \in Z(D)$ (if $Z(D)$ is nonempty), the vanishing locus $\{a \in V_d \,|\, a(z) = 0\}$ is a hyperplane in V_d that meets V_d^0. A generic $a \in V_d^0$ vanishing on $Z(D)$ vanishes at only one point $z \in Z(D)$ since $d \geq 2g+1$. In particular, the zero-scheme of $\mathrm{N}_{Z(D)/k,d}$ on $\underline{V}_d^0$ has its irreducible components in bijection with the points z of $Z(D)$; physically, these irreducible components are the loci $\{a \in \underline{V}_d^0 \,|\, a(z) = 0\}$ for $z \in Z(D)$.

Lemma 4.2. *For $z \in Z(D)$, the multiplicity of $\{a \in \underline{V}_d^0 \,|\, a(z) = 0\}$ as an irreducible component of the zero-scheme of $\mathrm{N}_{Z(D)/k,d}$ in $\underline{V}_d^0$ is $\mathrm{ord}_z(D)$.*

Proof. Pick $a \in V_d^0$ vanishing at some $z_0 \in Z(D)$ and not vanishing at any other z's in $Z(D)$ (we do not need to assume $\mathrm{ord}_{z_0}(a) = 1$, though this could be assumed by choosing a generically). We will prove the lemma by computing the ideal generated by $\mathrm{N}_{Z(D)/k,d}$ in the regular complete local ring at a on $\underline{V}_d^0$.

Consider a finite local k-algebra R and $\widetilde{a} \in \underline{V}_d^0(R)$ lifting a. We need to make explicit the condition that $\mathrm{N}_{Z(D)/k,d}(\widetilde{a}) \in R$ vanishes. This is the norm of the element $\widetilde{a}$ in the finite flat R-algebra $R \otimes_k \mathscr{O}(Z(D))$. This R-algebra has $R \otimes_k \mathscr{O}(Z(D))_z$ as its local factor at each $z \in Z(D)$, and the component $\widetilde{a}_z$ of $\widetilde{a}$ in the z-factor is a unit when $z \neq z_0$ since the reduction $a(z)$ of $\widetilde{a}_z$ is a unit. Hence the vanishing of $\mathrm{N}_{Z(D)/k}(\widetilde{a}) \in R$ is equivalent to the vanishing of the norm of $\widetilde{a}_{z_0} \in R \otimes_k \mathscr{O}(Z(D))_{z_0}$ relative to R. Choose a k-algebra isomorphism $\mathscr{O}(Z(D))_{z_0} \simeq k[t]/(t^e)$ where $e = \mathrm{ord}_{z_0}(D)$, so $\widetilde{a}_{z_0} = b_0 + b_1 t + \ldots b_{e-1}t^{e-1}$ with $b_0 = \widetilde{a}(z_0) \in \mathfrak{m}_R$. The matrix for multiplication by $\widetilde{a}_{z_0}$ relative to the R-basis $\{1, t, \ldots, t^{e-1}\}$ is lower-triangular with all diagonal entries equal to b_0, so the determinant of this matrix is $b_0^e = \widetilde{a}(z_0)^e$.

It follows that $\mathrm{N}_{Z(D)/k,d}$ is a unit multiple of the $\mathrm{ord}_{z_0}(D)$th power of "evaluation at z_0" (viewed as an element in $V_d^\vee$) in the regular complete local ring at a on $\underline{V}_d^0$. This evaluation has kernel equal to a height-1 (principal) prime ideal since evaluation at $z_0 \in C$ is a linear function on $\underline{V}_d$. This completes the proof that the irreducible component $\{a \in \underline{V}_d^0 \,|\, a(z) = 0\}$ in the zero scheme of $\mathrm{N}_{Z(D)/k,d}$ on $\underline{V}_d^0$ has multiplicity $\mathrm{ord}_{z_0}(D)$. ∎

To prove (4.3) via a comparison of generic multiplicities, we next check that the two factors on the left side of (4.3) have zero loci with no irreducible component in common. Since $d \geq 2g+1$ the Riemann–Roch and Bertini theorems ensure that for each $z \in Z(D)$ there exists $a \in A$ with $\mathrm{ord}_\xi(a) = -d$, $a(z) = 0$, and a k-étale divisor of zeros $\mathrm{div}_0(a)$, so $\mathrm{disc}_{\underline{\varepsilon},d}(A/(a)) \neq 0$. Hence, irreducible components of $\{\mathrm{N}_{Z(D)/k} = 0\}$ on $\underline{V}_d^0$ are not irreducible components of $\{\mathrm{disc}_{\underline{\varepsilon},d} = 0\}$ on $\underline{V}_d^0$. Thus, Lemma 4.2 now motivates us to show that for each $z_0 \in Z(D)$ we have:

Lemma 4.3. *There is a dense open U in the irreducible smooth zero-locus*

$$\{a \in \underline{V}_d^0 \,|\, a(z_0) = 0\}$$

such that for any closed point $a \in U$, the image of $\mathrm{N}_{D,d}$ in $\mathscr{O}_{\underline{V}_d^0,a}$ is a unit multiple of the function $\widetilde{a} \mapsto \widetilde{a}(z_0)^{\mathrm{ord}_{z_0}(D)}$ on $\underline{V}_d^0$.

Proof. A generically-chosen closed point $a \in V_d^0$ vanishing at z_0 does not vanish elsewhere on $Z(D)$ and has an étale divisor of zeros. Fix such an a. We shall now show that $\mathrm{N}_{D,d}$ viewed as an element of the regular local ring at a vanishes in the same artinian quotients as does the element $\widetilde{a} \mapsto \widetilde{a}(z_0)^{\mathrm{ord}_{z_0}(D)}$ in the symmetric algebra of the dual space $V_d^\vee$.

More specifically, for any finite local k-algebra R and any $\widetilde{a} \in \underline{V}_d^0(R)$ lifting a, we will show that $\mathrm{N}_{D,d}(\widetilde{a}) \in R$ vanishes if and only if $\widetilde{a}(z_0)^{\mathrm{ord}_{z_0}(D)} \in R$ vanishes. By definition, $\mathrm{N}_{D,d}(\widetilde{a}) \in R$ is the R-norm of the element $D\widetilde{a}$ in the finite flat R-algebra $(R \otimes_k A)/(\widetilde{a})$. This algebra is uniquely a product of local rings lifting the decomposition of $A/(a)$ into a product of local rings. Since a has an étale divisor of zeros, $A/(a)$ is a product of copies of k with one such factor corresponding to the zero z_0 of a. Since D is nonvanishing at the other zeros of a and hence is dual to a local generator of $\Omega^1_{C/k}$ near such points, Da is nonvanishing at these other (simple) zeros of a. Thus, $D\widetilde{a}$ is a unit in the local factor rings of $(R \otimes_k A)/(\widetilde{a})$ away from the z_0-factor. It follows that $\mathrm{N}_{D,d}(\widetilde{a}) \in R$ is a unit multiple of $(D\widetilde{a})(z_0) \in R$. Since D vanishes at z_0 to order $e := \mathrm{ord}_{z_0}(D)$, we can write $D = u^e\partial$ near z_0, where ∂ is dual to a local generator of $\Omega^1_{C/k}$ near z_0 and $u \in A_{z_0}$ is a uniformizer. Thus, upon uniquely extending D and ∂ to R-derivations of $R \otimes_k A_{z_0}$ we have $D\widetilde{a} = (1 \otimes u)^e \cdot (\partial\widetilde{a})$ in $R \otimes_k A_{z_0}$. The simplicity of z_0 as a zero of a ensures that ∂a is nonvanishing at z_0, so $(\partial\widetilde{a})(z_0)$ is a unit in R.

By the definition of $\mathrm{N}_{D,d}$, it follows that $\mathrm{N}_{D,d}(\widetilde{a}) \in R$ must therefore be a unit multiple of the eth power of the image of u in the factor ring $((R \otimes_k A)/(\widetilde{a}))_{z_0} \simeq R$. Hence, we must check that this image is a unit multiple of $\widetilde{a}(z_0)$. Using the isomorphism $\widehat{A}_{z_0} \simeq k[\![u]\!]$ we want to show that in the quotient $R[\![u]\!]/(\widetilde{a}_{z_0}) \simeq R$, with $R[\![u]\!]$ identified as the complete local ring on $C \otimes_k R$ along the section z_0, the residue class of u is a unit multiple of $\widetilde{a}(z_0)$. Since a has a simple zero at z_0, the u-adic expansion of $\widetilde{a}_{z_0}$ in $R[\![u]\!]$ has constant term $\widetilde{a}(z_0) \in \mathfrak{m}_R$ and has linear-coefficient equal to a unit. Thus, $\widetilde{a}(z_0) \equiv u \cdot (\text{unit}) \bmod \widetilde{a}_{z_0}$, as desired. ∎

By Lemmas 4.2 and 4.3, to complete the proof of (4.3) we have to work generically on an irreducible component Y of $\{\mathrm{disc}_{\underline{\varepsilon},d} = 0\}$: we must prove that at the generic point η of Y, the order of $\mathrm{N}_{D,d}$ in the discrete valuation ring $\mathscr{O}_{\underline{V}_d^0,\eta}$ is the same as the order of $\mathrm{disc}_{\underline{\varepsilon},d}$. In fact, we will make comparisons in $\mathscr{O}_{\underline{V}_d^0,a}$, a UFD, for a well-chosen closed point $a \in Y$. The first step is to construct a suitable a.

The natural scaling-action by $\mathbf{G}_m$ on $\underline{V}_d^0$ preserves the zero-scheme $\{\mathrm{disc}_{\underline{\varepsilon},d} = 0\}$, and the $\mathbf{G}_m$-action preserves the irreducible components of this zero-scheme because $\mathbf{G}_m$ is geometrically irreducible. Since $d \geq 2g+1$, we have a canonical closed immersion

$$\overline{C} \hookrightarrow \mathbf{P} := \mathbf{P}(\mathrm{H}^0(\overline{C}, d \cdot \xi)),$$

and since $d \geq 2g+2$ the projective tangent line $\mathbf{T}_x(\overline{C})$ to $\overline{C}$ in $\mathbf{P}$ at any $x \in C(k)$ meets $\overline{C}$ to order exactly 2 at x and to order 1 at all other intersection points. Pick a closed point a_1 in the smooth locus of Y_{red} such that a_1 does not lie on any irreducible component of $\{\mathrm{disc}_{\underline{\varepsilon},d} = 0\}$ except for Y. The point a_1 corresponds to a hyperplane H_1 in $\mathbf{P}$ whose degree-d intersection with $\overline{C}$ is supported in C and is non-reduced at a unique point $x \in C(k)$.

The argument immediately preceding Lemma 4.3 shows that for a generic choice of a_1 we have $x \notin Z(D)$, and in fact $H_1 \cap \overline{C} \subseteq C - Z(D)$. Fix such an a_1, so $\mathrm{ord}_x(a_1) \geq 2$.

Pick a hyperplane H_2 in $\mathbf{P}$ so that $H_2 \cap \overline{C}$ is supported in $C - Z(D)$ and is étale except for a double point at x (such H_2 can be found since $d \geq 2g+2$). Thus, H_2 arises from some $a_2 \in V_d^0$ (unique up to the $\mathbf{G}_m$-action) and a_2 also lies in the zero locus of $\mathrm{disc}_{\underline{\varepsilon},d}$. In particular, H_1 and H_2 must both contain the projective tangent line $\mathbf{T}_x(\overline{C})$. Consider the pencil of hyperplanes $\{\lambda H_1 + \mu H_2\}$ joining H_1 and H_2. All hyperplanes H in this pencil contain $\mathbf{T}_x(\overline{C})$, so $H \cap \overline{C}$ contains x to order at least 2. A generic such H does not contain ξ since $\xi \notin H_2$, so the scheme-theoretic intersection $H \cap \overline{C}$ is the divisor of zeros $\mathrm{div}_0(a_H)$ for an $a_H \in V_d^0$ that is unique up to unit-scaling. Note that a_H is in the zero scheme of $\mathrm{disc}_{\underline{\varepsilon},d}$ on $\underline{V}_d^0$ since $\mathrm{ord}_x(a_H) \geq 2$.

For generic H in the pencil, the only irreducible component of $\{\mathrm{disc}_{\underline{\varepsilon},d} = 0\}$ containing a_H is Y because the point $a_1 \in Y$ is not in other irreducible components and Y is $\mathbf{G}_m$-stable, and moreover $\mathrm{div}_0(a_H) = H \cap \overline{C}$ is disjoint from $Z(D)$ since $H_1 \cap \overline{C} \subseteq C - Z(D)$. Also, for generic H the intersection $H \cap \overline{C}$ is non-étale only at x, with order of contact exactly 2: this is immediate by generization from the fact that H_2 enjoys this property. Hence, by picking generic H in the pencil we find a closed point $a \in Y$ such that (i) a lies on no other irreducible components of the zero-scheme of $\mathrm{disc}_{\underline{\varepsilon},d}$, and (ii) $\mathrm{div}_0(a)$ is disjoint from $Z(D)$ and is étale away from a single double zero at some point $x \in C(k)$. We will now prove that $\mathrm{disc}_{\underline{\varepsilon},d}$ and $\mathrm{N}_{D,d}$ are unit multiples of each other in the regular complete local ring $\widehat{\mathscr{O}}_{\underline{V}_d^0,a}$ for any such a, and hence they are also unit multiples of each other in $\mathscr{O}_{\underline{V}_d^0,a}$; localizing at the generic point η of Y will then yield $\mathrm{ord}_\eta(\mathrm{disc}_{\underline{\varepsilon},d}) = \mathrm{ord}_\eta(\mathrm{N}_{D,d})$, completing the proof of Theorem 4.1.

Pick a finite local k-algebra R and $\widetilde{a} \in \underline{V}_d^0(R)$ lifting our above choice of $a \in \underline{V}_d^0(k)$ corresponding to a generic H in the pencil. It suffices to show that the vanishing of $\mathrm{disc}_{\underline{\varepsilon},d}(\widetilde{a}) \in R$ is equivalent to the vanishing of $\mathrm{N}_{D,d}(\widetilde{a}) \in R$. That is, we want the degree-d finite flat R-algebra $(R \otimes_k A)/(\widetilde{a})$ to have vanishing discriminant in R if and only if the image of $D\widetilde{a}$ in $(R \otimes_k A)/(\widetilde{a})$ has vanishing norm in R. Since the k-finite $\mathrm{Spec}(A/(a))$ in C is étale at all points away from x and has a zero at x of order exactly 2, the R-algebra $(R \otimes_k A)/(\widetilde{a})$ decomposes into a product of copies of R and a single rank-2 local factor ring

$$((R \otimes_k A)/(\widetilde{a}))_x = (R \otimes_k A)_x/(\widetilde{a})$$

that deforms the local ring $(A/a)_x$ at x on the zero-scheme of a on $C = \mathrm{Spec}\, A$. Moreover, $D\widetilde{a}$ has unit image in the rank-1 local factors of $(R \otimes_k A)/(\widetilde{a})$ because (i) these factors correspond to the (simple) zeros of a away from x, and (ii) Da is necessarily nonzero at simple zeros of a since the vector field D on C is nonvanishing at all points of the k-scheme $\mathrm{Spec}(A/(a)) \subseteq C$. Thus, $\mathrm{disc}_{\underline{\varepsilon},d}(\widetilde{a}) \in R$ is a unit multiple of the discriminant of the rank-2 finite flat R-algebra $(R \otimes_k A)_x/(\widetilde{a})$. A similar argument using the definition of $\mathrm{N}_{D,d}$ in (4.2) (with $k' = R$) shows that the norm $\mathrm{N}_{D,d}(\widetilde{a}) \in R$ is a unit multiple of the norm of the image of $D\widetilde{a}$ in the rank-2 algebra $(R \otimes_k A)_x/(\widetilde{a})$.

In the completion $(R \otimes_k A)_x^\wedge \simeq R \otimes_k A_x^\wedge \simeq R[\![u]\!]$, the image of $\widetilde{a}$ has reduction $a \in k[\![u]\!]$ with order 2. Thus, by Weierstrass Preparation, we can find an R-algebra isomorphism $R \otimes_k A_x^\wedge \simeq R[\![U]\!]$ carrying $\widetilde{a}$ to $U^2 + rU + s$ with $r, s \in \mathfrak{m}_R$. Since $x \notin Z(D)$, the continuous R-derivation of $R \otimes_k A_x^\wedge$ induced by D must be dual to a generator of $\widehat{\Omega}^1_{(R \otimes_k A_x^\wedge)/R}$, or in other words must be a unit multiple of $\mathrm{d}/\mathrm{d}U$, since D is dual to a local generator of $\Omega^1_{C/k,x}$. Thus, $\mathrm{N}_{D,d}(\widetilde{a})$ is a unit multiple of the norm of the U-derivative $2U + r$ in

$(R \otimes_k A)_x/(\widetilde{a}) \simeq (R \otimes_k A)^\wedge_x/(\widetilde{a}) \simeq R[U]/(U^2 + rU + s)$. This norm is $-r^2 + 4s$. Meanwhile, the discriminant of this rank-2 algebra computed with respect to the basis $\{1, U\}$ is $r^2 - 4s$. Thus, this norm and discriminant are indeed unit multiples of each other, and so one vanishes in R if and only if the other does. ■

To apply Theorem 4.1 we shall now assume that k is *perfect* (still possibly of characteristic 0). Pick $h \in A[T]$ with $\deg h > 0$. Assume that its zero scheme $Z_h \subseteq C \times \mathbf{A}^1_k$ is reduced with quasi-finite (necessarily flat) projections to both C and $\mathbf{A}^1_k$, and assume that the projection $Z_h \to \mathbf{A}^1_k$ is étale generically on Z_h. In characteristic 0, these conditions say that h is both primitive with respect to A (see Definition 2.1) and squarefree in $K[T]$ with no irreducible factor in $k[T]$. In particular, h has a nonzero lower-degree coefficient, so it makes sense to define $\nu(h)$ as in (3.3). Recall also from Lemma 2.2 and Theorem 2.6 that in characteristic $p > 0$ our assumptions on h hold if h is primitive and either $h(T^p)$ is squarefree in $K[T]$ or $h \in K[T^p]$ with h squarefree in $K[T]$.

Let $B \subseteq Z_h$ be the k-finite branch scheme for the map $Z_h \to \mathbf{A}^1_k$, so for each $x = (u_x, t_x) \in B$ we get an algebraic function $P_{x,d}$ on $\underline{V}_d$ defined as in (3.12). If $d > \nu(h)$ then as in (3.6) the polynomial h defines an algebraic map $\underline{V}^0_d \to \underline{V}^0_{\rho(d)}$ with $\rho(d) = d \cdot \deg h - \mathrm{ord}_\xi(\mathrm{lead}(h))$. For any nonzero k-linear derivation $D : A \to A$ and $d > \nu(h)$ we define the k-morphism $\mathscr{R}_d(h, Dh) : \underline{V}^0_d \to \mathbf{A}^1_k$ by

$$\mathscr{R}_d(h, Dh) : a \mapsto \mathrm{N}_{((k' \otimes_k A)/(h(a)))/k'}((Dh)(a)) \in k' \tag{4.4}$$

for $a \in \underline{V}^0_d(k')$ with any k-algebra k'; here $(k' \otimes_k A)/(h(a))$ is a finite free k'-module of rank $\rho(d)$, and $Dh \in A[T]$ is defined by extending D to a $k[T]$-linear derivation on $A[T]$. In the genus-0 case $A = k[u]$ with D having no zeros on the affine line, $\mathscr{R}_d(h, Dh)(a)$ is essentially the resultant of $h(a)$ and $(Dh)(a)$ (up to multiplication by a unit $b_{D,d} \cdot \mathrm{lead}(h(a))^{e_{D,d}}$ on $\underline{V}^0_d$ for some $b_{D,d} \in k^\times$ and $e_{D,d} \in \mathbf{Z}$ that are independent of a).

Theorem 4.4. *Let $h \in A[T]$ and the k-derivation $D : A \to A$ be as above. Assume that $Z(D)$ is disjoint from the image in C of the branch scheme B. For $d > \max(\nu(h), 2g)$ there exist positive integers $e_{x,d}$ (independent of D) for all $x \in B$ and a unit $w_{D,d}$ on $\underline{V}^0_d$ such that on $\underline{V}^0_d$*

$$\mathscr{R}_d(h, Dh) = w_{D,d} \cdot (\mathrm{N}_{Z(D)/k,\rho(d)} \circ h) \cdot \prod_{x \in B} (P^0_{x,d})^{e_{x,d}}, \tag{4.5}$$

and in the coordinate ring of $\underline{V}^0_d$ the factors $\mathrm{N}_{Z(D)/k,\rho(d)} \circ h$ and $\{P^0_{x,d}\}_{x \in B}$ are pairwise relatively prime.

If $D' : A \to A$ is a second nonzero k-derivation with $Z(D')$ disjoint from the image of B in C then $w_{D',d}/w_{D,d}$ has order $\deg h \cdot \mathrm{ord}_\xi(D'/D)$ along the hyperplane $\underline{V}_{d-1}$ in $\underline{V}_d$.

Proof. Due to the simple behavior of $P_{x,d}$ under change in the perfect ground field (as we recorded above Lemma 3.5), we may assume k is algebraically closed. If B is nonempty, then for each $x = (u_x, t_x) \in B \subseteq C \times \mathbf{A}^1_k$ and $d > \max(\nu(h), 2g)$ the irreducible zero locus of $P_{x,d}$ on $\underline{V}^0_d$ is not contained in the zero locus of $\mathrm{N}_{Z(D)/k,\rho(d)} \circ h$. Indeed, since $u_x \notin Z(D)$ and $d \geq 2g$ with $d > 0$, there exists $a \in V^0_d$ such that $a(u_x)$ equals t_x and $a(c)$ avoids the set of at most $\deg h$ roots of the nonzero specialization $h_c \in k[T]$ for each of the finitely many $c \in Z(D)$ (so $\mathrm{N}_{Z(D)/k,\rho(d)}(h(a)) \neq 0$ and $P_{x,d}(a) = 0$). Since reduced irreducible schemes of finite type over k (such as $\{P_{x,d} = 0\}$) are generically regular and $\underline{V}^0_d$ is regular, to prove (4.5) we have to show:

- for $a \in V_d^0$, $\mathscr{R}_d(h, Dh)(a) = 0$ if and only if some $P_{x,d}(a)$ vanishes or $h(a)$ vanishes at some zero of D on C (so $Dh \neq 0$),
- for a generic choice of closed point a of $\{\mathrm{N}_{Z(D)/k,\rho(d)} \circ h = 0\}$ (if this locus is not empty), the functions $\mathrm{N}_{Z(D)/k,\rho(d)} \circ h$ and $\mathscr{R}_d(h, Dh)$ on $\underline{V}_d^0$ are unit multiples of each other in the regular complete local ring on $\underline{V}_d^0$ at a,
- for a generic choice of closed point a in the irreducible and reduced $\{P_{x,d} = 0\}$, the image of $\mathscr{R}_d(h, Dh)$ in the regular complete local ring at a on $\underline{V}_d^0$ is independent of D up to unit multiple (this ensures that the multiplicity $e_{x,D,d}$ of the irreducible $P_{x,d}$ as a factor of $\mathscr{R}_d(h, Dh)$ in the coordinate ring of $\underline{V}_d^0$ is independent of D, and so may be denoted $e_{x,d}$).

We shall verify each of these in turn.

Step 1. To compare zero loci, note that $\mathscr{R}_d(h, Dh)(a) = 0$ if and only if some $c \in C(k)$ at which $h(a)$ vanishes is also a zero of $(Dh)(a)$, or equivalently $a(c)$ is a simultaneous zero of the specializations h_c and $(Dh)_c$ in $k[T]$. This says that the point $(c, a(c)) \in C \times \mathbf{A}_k^1$ is in the common zero locus of h and Dh. For a point $(c, a(c))$ in Z_h, certainly $(c, a(c))$ is in Z_{Dh} if $c \in Z(D)$. If $c \notin Z(D)$, so D is dual to a generator of $\Omega^1_{C/k}$ near c, the calculation in completions in the proof of Theorem 2.5 shows that the vanishing of Dh at $(c, a(c))$ is equivalent to the quasi-finite flat projection $Z_h \to \mathbf{A}_k^1$ having non-reduced (*i.e.*, non-étale) fiber at $(c, a(c))$. This says $(c, a(c)) \in B$; *i.e.*, $P_{x,d}(a) = 0$ for some $x \in B$.

Step 2. Consider the elements $\mathrm{N}_{Z(D)/k,\rho(d)} \circ h$ and $\mathscr{R}_d(h, Dh)$ in the complete local ring of $\underline{V}_d^0$ at a closed point a of $\{\mathrm{N}_{Z(D)/k,\rho(d)} \circ h = 0\}$, assuming this zero locus is not empty. For generic such a, $(u_x, a(u_x)) \notin Z_h$ for all $x = (u_x, t_x) \in B$ and the function $h(a) \in A = k[C]$ vanishes at exactly one point $z_0 \in Z(D)$ (*i.e.*, $(z, a(z))$ lies in Z_h for exactly one $z \in Z(D)$) because $d \geq 2g + 1$. We claim that in the complete local ring on $\underline{V}_d^0$ at such a generic a, the element $\mathrm{N}_{Z(D)/k,\rho(d)} \circ h$ is a unit multiple of the function $\widetilde{a} \mapsto h_{z_0}(\widetilde{a}(z_0))^{\mathrm{ord}_{z_0}(D)}$ from the symmetric algebra of $V_d^\vee$. To prove this, first use the map of local rings $h_a^* : \mathscr{O}_{\underline{V}^0_{\rho(d)}, h(a)} \to \mathscr{O}_{\underline{V}^0_d, a}$ obtained by pullback along $h : \underline{V}_d^0 \to \underline{V}^0_{\rho(d)}$ to form the germ

$$(\mathrm{N}_{Z(D)/k,\rho(d)} \circ h)_a = h_a^*((\mathrm{N}_{Z(D)/k,\rho(d)})_{h(a)}).$$

The right side is equal to $h_a^*(\mathrm{ev}_{z_0}^{\mathrm{ord}_{z_0}(D)}) \cdot (\text{unit})$ due to the proof of Lemma 4.2, where $\mathrm{ev}_{z_0} \in \mathscr{O}_{\underline{V}_d^0, a}$ denotes the "evaluate at z_0" functional in $V_d^\vee$. Hence, we obtain

$$(\mathrm{N}_{Z(D)/k,\rho(d)} \circ h)_a = (\widetilde{a} \mapsto h(\widetilde{a})(z_0)^{\mathrm{ord}_{z_0}(D)}) \cdot (\text{unit}). \tag{4.6}$$

Fix a generic a as above. Because $(u_x, a(u_x)) \notin Z_h$ for all $x \in B$, each point $(c, a(c))$ lying in Z_h with $D_c \neq 0$ (*i.e.*, with $c \neq z_0$) must have the property that projection from Z_h to $\mathbf{A}_k^1$ is étale at $(c, a(c))$ and hence $(Dh)(c, a(c)) \neq 0$. That is, $(Dh)(a) \in A$ is nonvanishing at all zeros of $h(a)$ on C away from z_0. Since $z_0 \in Z(D)$ is not equal to any of the u_x's, so $(z_0, a(z_0)) \notin B$, the projection $Z_h \to \mathbf{A}_k^1$ is étale at $(z_0, a(z_0))$. Equivalently, $(z_0, a(z_0))$ is an étale point in the $a(z_0)$-fiber of the map $Z_h \to \mathbf{A}_k^1$. That is, if we write $h = \sum \alpha_j (T - a(z_0))^j$ in $A[T]$, then α_0 has a simple zero at $a(z_0)$. Thus, $h(a) \equiv \alpha_0 + \alpha_1 \cdot (a - a(z_0)) \bmod \mathfrak{m}_{z_0}^2$, so $\mathrm{ord}_{z_0}(h(a)) = 1$ if and only if $\alpha_0 + \alpha_1(a - a(z_0))$ has a simple zero at z_0. Since α_0 has a simple zero at z_0, it is clearly an additional generic condition on our $a \in V_d^0$ that $\mathrm{ord}_{z_0}(h(a)) = 1$. In other words, for a generic closed point a on $\{\mathrm{N}_{Z(D)/k,\rho(d)} \circ h = 0\}$ the value $h(a) \in A$ is a local parameter at z_0. Choose such an a.

For any finite local k-algebra R and $\widetilde{a} \in \underline{V}_d^0(R)$ lifting a,

$$\mathscr{R}_d(h, Dh)(\widetilde{a}) = \mathrm{N}_{((R\otimes_k A)/(h(\widetilde{a})))/R}((Dh)(\widetilde{a})) = (\mathrm{unit}) \cdot \mathrm{N}_{((R\otimes_k A^\wedge_{z_0})/(h(\widetilde{a}_{z_0})))/R}((Dh)_{z_0}(\widetilde{a}))$$

in R. Let $u \in A$ be a uniformizer at z_0. The natural map $R \to (R \otimes_k A^\wedge_{z_0})/(h(\widetilde{a}_{z_0}))$ is an isomorphism and, by writing $D = u^e\partial$ near z_0 with $e := \mathrm{ord}_{z_0}(D)$ and ∂ dual to a local generator of $\Omega^1_{C/k}$ near z_0, we can use the same argument as in the proof of Lemma 4.3 to conclude that $\mathscr{R}_d(h, Dh)(\widetilde{a})$ is a unit multiple of $h_{z_0}(\widetilde{a}(z_0))^{\mathrm{ord}_{z_0}(D)}$ in R. Thus, by passing to the inverse limit over artinian quotients R of $\mathscr{O}^\wedge_{\underline{V}_d^0,a}$ and using (4.6), $\mathscr{R}_d(h, Dh)$ and $\mathrm{N}_{Z(D)/k,\rho(d)} \circ h$ are unit multiples in $\mathscr{O}_{\underline{V}_d^0,a}$ and thus have the same multiplicity at the generic points of the zero locus of $\mathrm{N}_{Z(D)/k,\rho(d)} \circ h$ on $\underline{V}_d^0$ (assuming this zero locus is not empty).

Step 3. Before passing to consideration of multiplicities of $P^0_{x,d}$'s as factors of $\mathscr{R}_d(h, Dh)$ in $\mathscr{O}^\wedge_{\underline{V}_d^0,a}$ for generic choices of a closed point a in $\{P_{x,d} = 0\}$, we note that since $d \geq 2g$ and $d > 0$ there is no possibility of repetition among irreducible factors when we consider how different factors on the right side of (4.5) may contribute to the zero-scheme of $\mathscr{R}_d(h, Dh)$. Indeed, for rational points $a \in V_d^0$ with $P_{x,d}(a) = 0$ for some $x \in B$ and a near the generic point of the irreducible hypersurface $\{P_{x,d} = 0\}$, the zero locus of $h(a)$ on C is disjoint from $Z(D)$ (see the argument at the beginning of the present proof) and moreover $P_{x',d}(a) \neq 0$ for $x' \neq x$. We choose $x \in B$ and such an a that is sufficiently generic on the irreducible and reduced zero scheme $\{P^0_{x,d} = 0\}$; in particular, a lies in the regular locus of $\{P^0_{x,d} = 0\}$. Thus, up to unit multiple in the complete local ring of $\underline{V}_d^0$ at a, the element $\mathscr{R}_d(h, Dh)$ is a power of $P^0_{x,d}$ and we must prove that the positive exponent for this power is independent of D when a is generic.

Consider two fixed derivations D and D' compatible with the hypotheses of the theorem, so by picking our above a generically we may assume that both D and D' have nonzero specialization at the zeros of a. Hence, as sections of the sheaf of derivations of $\mathscr{O}_C$, both D and D' are unit multiples of each other near the zeros of a. It follows that in the regular local ring $\mathscr{O}^\wedge_{\underline{V}_d^0,a}$, the elements $\mathscr{R}_d(h, Dh)$ and $\mathscr{R}_d(h, D'h)$ are unit multiples of each other (*i.e.*, they vanish at the same set of local artinian points). This proves that the multiplicity of $P^0_{x,d}$ as a factor of $\mathscr{R}_d(h, Dh)$ is independent of the choice of D. This completes Step 3, and so proves (4.5).

To compute the order of $w_{D',d}/w_{D,d}$ along the hyperplane $\underline{V}_{d-1} \hookrightarrow \underline{V}_d$ for D' as in the final assertion of Theorem 4.4, we consider ratio of (4.5) for D' and (4.5) for D, evaluated at a generic $a \in V_d^0$. For $\phi = D'/D \in k(\overline{C})^\times$, genericity of a ensures that the divisor of $h(a)$ is disjoint from the divisor of ϕ away from ξ, so we readily compute that $w_{D',d}(a)/w_{D,d}(a)$ is equal to $\phi(\mathrm{div}_C h(a))/h(a)(\mathrm{div}_C\phi)$. The theory of local symbols for rational maps from smooth algebraic curves to $\mathbf{G}_m$ [12, III, §1.4] identifies this ratio with the product of local symbols $(\phi, h(a))_x$ for $x \in C(k)$, so the product formula for such local symbols gives

$$\phi(\mathrm{div}_C h(a))/h(a)(\mathrm{div}_C\phi) = (\phi, h(a))_\xi^{-1} = (-1)^{\mathrm{ord}_\xi(h(a))\,\mathrm{ord}_\xi(\phi)} \cdot \frac{h(a)^{\mathrm{ord}_\xi(\phi)}}{\phi^{\mathrm{ord}_\xi(h(a))}}(\xi) \tag{4.7}$$

for generic $a \in V_d^0$. Since $\mathrm{ord}_\xi(h(a)) = -\rho(d)$ as in (3.4) with f replaced by $h \in A[T]$, we obtain

$$\frac{w_{D',d}(a)}{w_{D,d}(a)} = (-1)^{\rho(d)\,\mathrm{ord}_\xi(D'/D)} \cdot \frac{h(a)^{\mathrm{ord}_\xi(D'/D)}}{\phi^{-\rho(d)}}(\xi). \tag{4.8}$$

As a function of the coordinates $c_1, \ldots, c_{d+1-g}$ of $a \in V_d$ relative to a basis $\varepsilon_1, \ldots, \varepsilon_{d+1-g}$ as in §3, (4.8) shows that for $d > \max(\nu(h), 2g)$ the order of $w_{D',d}/w_{D,d}$ along the hyperplane $\underline{V}_{d-1}$ defined by the equation $c_{d+1-g} = 0$ is $\mathrm{ord}_\xi(D'/D)\deg h$. ■

Combining Theorem 4.1 and Theorem 4.4, when k is perfect and $Z(D)$ is disjoint from the u_x's we arrive at an identity

$$\mathscr{R}_d(h, Dh) \cdot (\mathrm{disc}_{\underline{\varepsilon},\rho(d)} \circ h) = \widetilde{w}_{D,d,\underline{\varepsilon}} \cdot (\mathrm{N}_{D,\rho(d)} \circ h) \cdot \prod_{x \in B} (P^0_{x,d})^{e_{x,d}} \tag{4.9}$$

on $\underline{V}^0_d$ when $d > \max(\nu(h), 2g+2)$ (so $\rho(d) \geq 2g+1$), where $\widetilde{w}_{D,d,\underline{\varepsilon}}$ is a unit on $\underline{V}^0_d$ and the explicit formula for both $e_{D,d}$ in (4.3) and $\mathrm{ord}_{\underline{V}_{d-1}}(w_{D',d}/w_{D,d})$ in Theorem 4.4 imply that $\mathrm{ord}_{\underline{V}_{d-1}}(\widetilde{w}_{D,d,\underline{\varepsilon}})$ is independent of D. A stronger property is true: $\widetilde{w}_{D,d,\underline{\varepsilon}}$ is *independent* of D. This property holds provided that $(\mathrm{N}_{D,\rho(d)} \circ h)/\mathscr{R}_d(h, Dh)$ is independent of the choice of D, and such independence of D follows by inspection of values at generic geometric closed points (since any two choices of D have ratio given by an element of $k(\overline{C})^\times$). We shall now write w_d instead of $\widetilde{w}_{D,d,\underline{\varepsilon}}$, suppressing explicit mention of the dependence of w_d on $\underline{\varepsilon}$.

Using the structure (3.13) of units on $\underline{V}^0_d$, we can rewrite (4.9) as an equality of rational functions on $\underline{V}^0_d$:

$$\mathrm{disc}_{\underline{\varepsilon},\rho(d)} \circ h = b_d c_{d+1-g}^{e_d} \prod_x (P^0_{x,d})^{e_{x,d}} \cdot \frac{\mathrm{N}_{D,\rho(d)} \circ h}{\mathscr{R}_d(h, Dh)}, \tag{4.10}$$

with *any* nonzero k-linear derivation $D : A \to A$, where both $b_d \in k^\times$ and $e_d \in \mathbf{Z}$ depend on $\underline{\varepsilon}$ but are independent of D, and $e_d \bmod 2$ is independent of $\underline{\varepsilon}$ (as is $b_d \bmod (k^\times)^2$ if e_d is even). Note that (4.10) recovers (3.14) when k has positive characteristic p and h is a polynomial in T^p, since the ratio on the right side of (4.10) then equals 1 because $(Dh)(a) = D(h(a))$ for all Yoneda-points $a \in \underline{V}^0_d$ in such cases. Thus, Theorem 1.5 is a special case of:

Theorem 4.5. *In the setting of Theorem* 4.4*, for all sufficiently large d (only depending on the genus g and the total degree $\deg_{u,T} h$), the exponent $e_{x,d}$ in* (4.5) *is the length $\ell(\mathscr{O}_{B,x})$ at x for the k-finite branch scheme B of the projection from $Z = Z_h \subseteq C \times \mathbf{A}^1_k$ to the T-line.*

We shall deduce Theorem 4.5 from a more general setup that does not involve derivations. First, observe that the hypotheses on h and D in Theorem 4.4 ensure that (i) the exponent $e_{x,d}$ in (4.5) is the multiplicity of the irreducible $P^0_{x,d}$ as a factor of $\mathscr{R}_d(h, Dh)$ in the UFD coordinate ring of $\underline{V}^0_d$, and (ii) the curves $\{h = 0\}$ and $\{Dh = 0\}$ in $C \times \mathbf{A}^1_k$ have finite intersection that contains B as an open and closed subscheme. (Strictly speaking, the "curve" $\{Dh = 0\}$ may be empty, though this can only happen if B is empty.)

Let $h_1, h_2 \in A[T]$ be nonzero elements whose (possibly empty) zero loci Z_{h_j} in $C \times \mathbf{A}^1_k$ have finite intersection. For each $x = (u_x, t_x) \in Z_{h_1} \cap Z_{h_2}$ and $d > 0$ we define $P_{x,d} : \underline{V}^0_d \to \mathbf{A}^1_k$ by $a \mapsto \mathrm{N}_{k(x)/k}(a(u_x) - t_x)$, as usual. We define $\nu(h_1)$ as in (3.3), with the convention $\nu(h_1) = 0$ if h_1 is a monomial, and as in (3.6) for $d > \nu(h_1)$ we use substitution into h_1 to define an algebraic map $\underline{V}^0_d \to \underline{V}^0_{\rho_1(d)}$ with $\rho_1(d) = d \cdot \deg h_1 - \mathrm{ord}_\xi(\mathrm{lead}(h_1))$. For such d we may therefore define the k-morphism $\mathscr{R}_d(h_1, h_2) : \underline{V}^0_d \to \mathbf{A}^1_k$ by

$$\mathscr{R}_d(h_1, h_2) : a \mapsto \mathrm{N}_{((k' \otimes_k A)/h_1(a))/k'}(h_2(a)) \in k'$$

for $a \in \underline{V}^0_d(k')$ with any k-algebra k'; this is a generalization of (4.4), and in the case $A = k[u]$ with monic h_1 and h_2 it agrees (up to universal sign conventions) with the function that

sends a to the resultant of the ordered pair $(h_1(a), h_2(a))$ (hence the notation). The same method as at the beginning of the proof of Theorem 4.4 shows that for $d > \max(\nu(h_1), 2g)$ we have

$$\mathscr{R}_d(h_1, h_2) = w_d \cdot \prod_{x \in Z_{h_1} \cap Z_{h_2}} (P^0_{x,d})^{e_{x,d}} \tag{4.11}$$

for some $e_{x,d} > 0$ and some unit w_d on $\underline{V}^0_d$. The exponent $e_{x,d}$ is the multiplicity of the irreducible $P^0_{x,d}$ as a factor of $\mathscr{R}_d(h_1, h_2)$, and so Theorem 4.5 is a special case of:

Theorem 4.6. *For $h_1, h_2 \in A[T]$ as above, if $d > 2g + 2\deg_{u,T} h_1 \cdot \deg_{u,T} h_2$ then the exponent $e_{x,d}$ in (4.11) is equal to the intersection number $e_x = i_x(Z_{h_1}, Z_{h_2})$ at x.*

Our proof is modelled on the simpler case $A = k[u]$ that is treated in [2, Thm. 4.5].

Proof. Since k is perfect, we may and do take k to be algebraically closed.

Step 1. Let us first treat the cases when $\deg_T h_1 = 0$ or $\deg_T h_2 = 0$. First assume $\deg_T h_2 = 0$, so $h_2 = a_0 \in A - \{0\}$. The case $h_2 \in k^\times$ is trivial, so we may assume $\deg_{u,T} h_2 > 0$ and hence $d > \max(\nu(h_1), 2g)$. Clearly $\mathscr{R}_d(h_1, h_2)$ is the algebraic function $a \mapsto \mathrm{N}_{(A/h_1(a))/k}(a_0)$ on $\underline{V}^0_d$. For all $x \in Z_{h_1} \cap Z_{h_2}$ let H_x be the codimension-1 locus of points $a \in \underline{V}^0_d$ such that $a(u_x) = t_x$. We want to prove that for all such x the function $\mathscr{R}_d(h_1, h_2)$ on $\underline{V}^0_d$ has order along H_x equal to $i_x(Z_{h_1} \cap Z_{h_2})$. Since $h_2 = a_0 \in A - \{0\}$, this intersection number at x is equal to $\mathrm{ord}_{u_x}(a_0)\,\mathrm{ord}_{t_x}(h_{1,u_x})$, where $h_{1,u_x} \in k(u_x)[T] = k[T]$ denotes the specialization of $h_1 \in A[T]$ at the zero u_x of $a_0 = h_2$. By computing with multiplicative local symbols as in (4.7), for generic $a \in V^0_d$ we have

$$\mathscr{R}_d(h_1, h_2)(a) = a_0(\mathrm{div}_C h_1(a)) = (-1)^{\mathrm{ord}_\xi(h_1(a))\,\mathrm{ord}_\xi(a_0)} \cdot h_1(a)(\mathrm{div}_C a_0) \cdot \frac{h_1(a)^{\mathrm{ord}_\xi(a_0)}}{a_0^{\mathrm{ord}_\xi(h_1(a))}}(\xi). \tag{4.12}$$

For a with $-\mathrm{ord}_\xi(a) = d$, the exponent $\mathrm{ord}_\xi(h_1(a)) = -\deg_T(h_1)d - \dim_k(A/(\mathrm{lead}(h_1)))$ in (4.12) only depends on h_1 and not on a. Likewise, when the final factor in (4.12) is considered as a rational function of $a \in \underline{V}^0_d$ it is clearly a unit near the generic point of H_x. Hence, it is sufficient to study the order along H_x of the algebraic function $a \mapsto h(a)(\mathrm{div}_C a_0)$ on $\underline{V}^0_d$ with $h \in A[T]$ any nonzero element satisfying $h_{u_x}(t_x) = 0$ and $h_{u_0} \neq 0$ for all $u_0 \in \mathrm{div}_C(a_0)$; we wish to prove that this order along H_x is $\mathrm{ord}_{u_x}(a_0)\,\mathrm{ord}_{t_x}(h_{u_x})$.

The only remaining role of $a_0 \in A - \{0\}$ is through its divisor, the principality of which is now irrelevant, and the problem is visibly additive in this divisor. Since $a \mapsto h(a)(u_0) = h_{u_0}(a(u_0))$ is a unit near the generic point of H_x for $u_0 \in C(k) - \{u_x\}$, it clearly suffices to treat the case of the divisor $\{u_x\}$: we claim that the algebraic function $a \mapsto h_{u_x}(a(u_x))$ on $\underline{V}^0_d$ has order along $H_x = \{a(u_x) = t_x\}$ equal to $\mathrm{ord}_{t_x}(h_{u_x})$. Replacing a with $a - t_x$ and h with $h(T + t_x)$ reduces us to the case $t_x = 0$, so for any nonzero $h_0 \in k[T]$ (such as h_{u_x}) we want the algebraic function $a \mapsto h_0(a(u_x))$ on $\underline{V}_d$ to vanish to order $\mathrm{ord}_0(h_0)$ along the hyperplane killed by evaluation at u_x. This claim is multiplicative in h_0, so by factoring h_0 it is enough to treat to the cases $h_0 = c \in k^\times$ and $h_0 = T - c'$ (with $c' \in k$). These cases are all trivial.

Next, assume $h_1 = a_0 \in A - \{0\}$, so $\mathscr{R}_d(h_1, h_2)$ sends a to $h_2(a)(\mathrm{div}_C a_0)$. The preceding argument shows

$$\mathrm{ord}_{H_x}(\mathscr{R}_d(h_1, h_2)) = \mathrm{ord}_{u_x}(a_0)\,\mathrm{ord}_{t_x}(h_{2,u_x}) = i_x(Z_{h_1} \cap Z_{h_2}),$$

as required.

Step 2. Now we may suppose $\deg_T h_1, \deg_T h_2 > 0$. The key is to prove $e_{x,d} \geq i_x(Z_{h_1}, Z_{h_2})$ for all $x \in Z_{h_1} \cap Z_{h_2}$ and sufficiently large d as in the statement of the theorem. We shall prove this in Steps 3 and 4 by a deformation technique that generalizes the method used to handle the case of genus 0 in [2, §4], and the conditions $\deg_T h_j > 0$ will not be used until near the end of Step 4. Granting these lower bounds on the $e_{x,d}$'s for now, let us show that they must be equalities.

It is enough to verify equality upon adding up all of these inequalities. That is, we wish to prove $\sum_x e_{x,d} = \ell(Z_{h_1} \cap Z_{h_2})$ for our large d. Using linear coordinates $\{y_1, \dots\}$ on V_d dual to the basis $\{\varepsilon_1, \dots, \varepsilon_{d+1-g}\}$ with $\varepsilon_1 = 1$, each $P^0_{x,d} \in k[\underline{V}^0_d] = k[y_1, \dots, y_{d+1-g}][1/y_{d+1-g}]$ is a linear form in the y_j's that has degree 1 in y_1 (but for $j > 1$ this linear form does not involve y_j if $\varepsilon_j(u_x) = 0$). Hence, $\sum_x e_{x,d}$ is the y_1-degree of the algebraic function $\mathscr{R}_d(h_1, h_2)$ on $\underline{V}^0_d$.

Fix a choice of $a_d \in V^0_d$ that vanishes to order exceeding $i_x(Z_{h_1}, Z_{h_2})$ at u_x for all $x \in Z_{h_1} \cap Z_{h_2}$; such an a_d exists if $d \geq 2g + 2\ell(Z_{h_1} \cap Z_{h_2})$, and by intersection theory on $\overline{C} \times \mathbf{P}^1$ we can bound $\ell(Z_{h_1} \cap Z_{h_2})$ from above by $\deg_{u,T} h_1 \cdot \deg_{u,T} h_2$. Hence, we can find a_d subject to the desired lower bound on d determined by the $\deg_{u,T} h_j$'s and the genus.

Consider the algebraic function $a_d + T \in A[T]$ on $C \times \mathbf{A}^1_k$. Its specialization over each k-point of the affine k-line is a function on C with a pole of exact order d at ξ (since $d > 0$), so by universality it is the pullback of the universal function $\sum_{j \leq d+1-g} \varepsilon_j \otimes y_j$ on $C \times \underline{V}^0_d$ along a unique k-morphism $\mathbf{A}^1_k \to \underline{V}^0_d$. Algebraically, since $\varepsilon_1 = 1$ this k-morphism corresponds to the k-algebra map $k[\underline{V}^0_d] \to k[T]$ that carries y_j to $y_j(a_d)$ for $j > 1$ and carries y_1 to $T + y_1(a_d)$, so the product of linear forms $\mathscr{R}_d(h_1, h_2) \in k[\underline{V}^0_d]$ is pulled back to an element in $k[T]$ with T-degree $\sum_x e_{x,d}$. But this pullback is $\mathrm{N}_{(A[T]/(h_1(a_d+T)))/k[T]}(h_2(a_d + T))$, so our problem is to prove

$$\deg_T \mathrm{N}_{(A[T]/(h_1(a_d+T)))/k[T]}(h_2(a_d + T)) \stackrel{?}{=} \ell(Z_{h_1} \cap Z_{h_2})$$

for all large d, with largeness that is determined in the desired manner in terms of the $\deg_{u,T} h_j$'s and the genus. In fact, the largeness will only depend on $\deg_T h_1$ and the ξ-orders of the coefficients of h_1.

It shall be convenient first to give a direct proof that for $d > \deg_{u,T} h_1$ the zero-scheme

$$\mathrm{Spec}(A[T]/(h_1(a_d + T))) = Z_{h_1(a_d+T)} \subseteq C \times \mathbf{A}^1_k$$

is finite flat over the T-line $\mathbf{A}^1_k$ and this goes as follows. The constant term $h_1(a_d) \in A - \{0\}$ has pole-order at ξ that is larger than the pole-order of all positive-degree coefficients of $h_1(a_d + T) \in A[T]$ when $d > \deg_{u,T} h_1$, so the restriction of $h_1(a_d + T)$ to each fiber of $C \times \mathbf{A}^1 \to \mathbf{A}^1$ is not a zero-divisor. Hence, quasi-finiteness over $\mathbf{A}^1_k$ follows and by the local flatness criterion (as in [11, Cor. to 22.5]) we see that $Z_{h_1(a_d+T)}$ is flat over the T-line. Consideration of pole-orders at ξ for coefficients of $h_1(T)$ shows that the geometric fibers of $Z_{h_1(a_d+T)} \to \mathbf{A}^1_k$ all have the same rank when $d > \deg_{u,T} h_1$, namely the rank is $-\mathrm{ord}_\xi(h_1(a_d))$ because for any nonzero rational function on $\overline{C}$ the number of zeros equals the number of poles with multiplicity. Thus, finiteness follows from the fact that a quasi-finite separated flat map between locally noetherian schemes is finite if its fiber-rank is locally constant on the base [6, II, 1.19]. (The noetherian restriction can be removed.)

Let $g_j(T) = h_j(a_d + T) \in A[T]$, so there is an evident equality of sets $Z_{h_1} \cap Z_{h_2} = Z_{g_1} \cap Z_{g_2}$ in $C \times \mathbf{A}^1_k$ because $a_d(u_x) = 0$ for all $x \in B$. Since a_d as a function on C vanishes at u_x to order exceeding $i_x(Z_{h_1}, Z_{h_2})$, formally at $x \in Z_{g_1} \cap Z_{g_2}$ each Z_{g_j} is described as a deformation

of Z_{h_j} at x that is the identity up to order $i_x(Z_{h_1}, Z_{h_2})$. Hence, as we argued at the end of the proof of [2, Thm. 4.5], such deformation does not change the local intersection number. This gives $\ell(Z_{h_1} \cap Z_{h_2}) = \ell(Z_{g_1} \cap Z_{g_2})$, so our problem is a special case of the following general situation. Consider any nonzero $g_1, g_2 \in A[T]$ such that the constant term (in A) of g_1 is nonzero with larger pole-order at ξ than the pole-orders at ξ for the positive-degree nonzero coefficients of g_1. We also assume that $Z_{g_1} \cap Z_{g_2}$ is finite. These hypotheses suffice to make Z_{g_1} finite and flat over the T-line, so $\mathrm{N}_{Z_{g_1}/\mathbf{A}^1}(g_2)$ makes sense as an element of $k[T]$, and these hypotheses also ensure that this norm is nonzero. Our claim is that this nonzero norm in $k[T]$ has T-degree $\ell(Z_{g_1} \cap Z_{g_2})$. This norm is the $k[T]$-determinant of multiplication by g_2 on the finite flat $k[T]$-algebra $A[T]/(g_1)$, so by [7, Lemma A.2.6] the degree of this norm (or equivalently, the length of its zero-scheme in $\mathbf{A}^1_k$) is equal to the Herbrand quotient for multiplication by g_2 on $A[T]/(g_1)$. This latter multiplication map has cokernel with length $\ell(Z_{g_1} \cap Z_{g_2})$, so we just need the kernel to be 0, which is to say that $g_2|_{Z_{g_1}}$ is not a zero divisor. Since $\mathrm{Spec}(A[T]) = C \times \mathbf{A}^1$ is a regular surface, this property of $g_2|_{Z_{g_1}}$ follows from the fact that it is a generic unit on the effective Cartier divisor Z_{g_1} in $C \times \mathbf{A}^1$.

Step 3. We now return to the task of proving $e_{x,d} \geq i_x(Z_{h_1}, Z_{h_2})$ for all $x \in Z_{h_1} \cap Z_{h_2}$. Consider any $\widetilde{h}_j \in k[\![\tau]\!] \otimes_k A[T]$ that lifts h_j and has T-degree $\deg_T h_j$ such that the nonzero $\mathrm{lead}_T(\widetilde{h}_j) \in k[\![\tau]\!] \otimes_k A$ has leading coefficient in $k[\![\tau]\!]^\times$ for its Laurent expansion along ξ; that is, its pole-order at ξ on $\overline{C}_{k(\!(\tau)\!)}$ is the same as the pole-order at $\xi \in \overline{C}$ for its nonzero reduction $\mathrm{lead}_T(h_j) \in A$. We also assume that the total degree $\deg_{u,T} \widetilde{h}_j$ over $k(\!(\tau)\!)$ is equal to $\deg_{u,T} h_j$. Such deformations $\widetilde{h}_j$ with additional convenient properties will be constructed in Step 4. Note that each zero-scheme $Z_{\widetilde{h}_j}$ is $k[\![\tau]\!]$-flat, and so is equal to the closure in $(C \times \mathbf{A}^1)_{k[\![\tau]\!]}$ of its $k(\!(\tau)\!)$-fiber.

We may use such $\widetilde{h}_j$'s to deform $\mathscr{R}_d(h_1, h_2)$ to an algebraic function $(\underline{V}^0_d)_{k[\![\tau]\!]} \to \mathbf{A}^1_{k[\![\tau]\!]}$ over $k[\![\tau]\!]$ defined functorially by

$$\mathscr{R}_d(\widetilde{h}_1, \widetilde{h}_2) : a \mapsto \mathrm{N}_{Z_{\widetilde{h}_1(a)}/\mathrm{Spec}(R)}(\widetilde{h}_2(a)) = \mathrm{N}_{((R \otimes_k A)/(\widetilde{h}_1(a)))/R}(\widetilde{h}_2(a)) \in R$$

for all $k[\![\tau]\!]$-algebras R and $a \in \underline{V}^0_d(R)$. To make sense of this definition we have to show that $(R \otimes_k A)/(\widetilde{h}_1(a))$ is a finite locally free R-module for all such R and a if d is sufficiently large (*e.g.*, as large as in the statement of the theorem that we are presently trying to prove). This property follows from Lemma 3.3, as we now explain. By hypothesis, $\widetilde{h}_1$ has the same T-degree over the generic and closed points of $\mathrm{Spec}\, k[\![\tau]\!]$ and its leading coefficient as an element of $k[\![\tau]\!] \otimes_k A$ has the same pole order at ξ considered as a rational point on both the generic and closed fibers of $\overline{C}_{k[\![\tau]\!]} \to \mathrm{Spec}\, k[\![\tau]\!]$. Thus, provided that d is large enough (as is determined by the pole-orders along ξ for the coefficients of $\widetilde{h}_1 \in (k(\!(\tau)\!) \otimes_k A)[T]$ and $h_1 \in A[T]$), the pole-order at ξ on each fiber over $\mathrm{Spec}\, R$ is the number $\rho_1(d) = d \cdot \deg_T h_1 - \mathrm{ord}_\xi(\mathrm{lead}_T(h_1))$ that only depends on d. That is, for large enough d we have $\widetilde{h}_1(a) \in \underline{V}^0_{\rho_1(d)}(R)$ for all R and a. Due to the degree properties we are assuming for $\widetilde{h}_1$ (especially $\deg_{u,T} \widetilde{h}_1 = \deg_{u,T} h_1$), the d's in the statement of the theorem are large enough for this purpose. By Lemma 3.3, the zero-scheme of $\widetilde{h}_1(a)$ on C_R is therefore indeed finite and locally free over R for $a \in \underline{V}^0_d(R)$ with such large d.

We wish to exploit information on the $k(\!(\tau)\!)$-fiber, so let us next check that the $k[\![\tau]\!]$-scheme $Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2}$ is quasi-finite; that is, we have to show that the generic fibers $(Z_{\widetilde{h}_j})_{k(\!(\tau)\!)}$ have no common irreducible component in $(C \times \mathbf{A}^1)_{k(\!(\tau)\!)}$. If such a component Z exists, consider the closure of Z in $(\overline{C} \times \mathbf{P}^1)_{k[\![\tau]\!]}$. This closure has irreducible closed image in $\overline{C}_{k[\![\tau]\!]}$ that meets the generic fiber, so this image is either all of $\overline{C}_{k[\![\tau]\!]}$ or is the closure of a closed point of $\overline{C}_{k(\!(\tau)\!)}$. We shall deduced a contradiction in either case. First assume that the closure of Z surjects onto $\overline{C}_{k[\![\tau]\!]}$. This closure is contained in the closure of each $Z_{\widetilde{h}_j}$ in $(\overline{C} \times \mathbf{P}^1)_{k[\![\tau]\!]}$, so the closures of the $Z_{\widetilde{h}_j}$'s in $(C \times \mathbf{P}^1)_{k[\![\tau]\!]}$ have overlap that surjects onto $C_{k[\![\tau]\!]}$. Hence, the reductions of these closures modulo τ have overlap in $C \times \mathbf{P}^1$ that surjects onto C. But the reductions Z_{h_j} are closed in $C \times \mathbf{A}^1$ with finite overlap, so the closure Y_j of each $Z_{\widetilde{h}_j}$ in $(C \times \mathbf{P}^1)_{k[\![\tau]\!]}$ must have reduction modulo τ that contains $C \times \{\infty\}$ as an irreducible component. Since Y_j is defined by the homogenization of $\widetilde{h}_j$ in $A[T_0, T_1]$ (with $T = T_0/T_1$), its reduction modulo τ contains $C \times \{\infty\} = \{T_0 = 0\}$ if and only if $\mathrm{lead}_T(\widetilde{h}_j) \in k[\![\tau]\!] \otimes_k A$ is divisible by τ. Such divisibility for either j contradicts our initial hypotheses on the Laurent expansions of each $\widetilde{h}_j$ along ξ.

Next, consider the possibility that the closure of Z in $(\overline{C} \times \mathbf{P}^1)_{k[\![\tau]\!]}$ has image in $\overline{C}_{k[\![\tau]\!]}$ equal to the closure $\overline{c} \subseteq \overline{C}_{k[\![\tau]\!]}$ of a closed point $\overline{c}_\eta \in \overline{C}_{k(\!(\tau)\!)}$. Such a closed point clearly must lie in $C_{k(\!(\tau)\!)}$, and its reduction into $\overline{C}$ is some k-point $\overline{c}_0$. If $\overline{c}_0 \in C(k)$ (that is, $\overline{c}_0 \neq \xi$) then the closure of Z in $(C \times \mathbf{A}^1)_{k[\![\tau]\!]}$ has reduction containing the line $\{\overline{c}_0\} \times \mathbf{A}^1_k$, yet this closure is contained in each of the $Z_{\widetilde{h}_j}$'s because each $Z_{\widetilde{h}_j} \subseteq (C \times \mathbf{A}^1)_{k[\![\tau]\!]}$ is the closure of its own generic fiber. The reductions $Z_{h_j} \subseteq C \times \mathbf{A}^1_k$ therefore each contain the line $\{\overline{c}_0\} \times \mathbf{A}^1_k$, yet by hypothesis $Z_{h_1} \cap Z_{h_2}$ is finite. This is a contradiction, so $\overline{c}_0 = \xi$. The same argument implies that the closure of each $Z_{\widetilde{h}_j}$ in $(\overline{C} \times \mathbf{A}^1)_{k[\![\tau]\!]}$ has reduction containing $\{\xi\} \times \mathbf{A}^1_k$, so we need to rule out this possibility. In fact, for both j's this gives a contradiction, as follows. Working with $j = 1$, say, we may write $\widetilde{h}_1 = \sum_i \alpha_i T^i$ with $\alpha_i \in k[\![\tau]\!] \otimes_k A$. Each α_i viewed in $k(\!(\tau)\!) \otimes_k A$ must vanish at the point $\overline{c}_\eta$. For $d = \deg_T \widetilde{h}_1$ we have $\alpha_d = \mathrm{lead}_T(\widetilde{h}_1)$, and if y is a local parameter along ξ on $\overline{C}$ then the completion of the regular surface $\mathrm{Spec}(k[\![\tau]\!] \otimes_k A)$ at the k-point ξ is identified with $k[\![\tau, y]\!]$. By faithful flatness of completion, it follows that the image of α_d in the Dedekind domain $k[\![\tau, y]\!][1/y]$ has a prime factor and so is not a unit. But the initial hypothesis on the Laurent expansion of $\alpha_d = \mathrm{lead}_T(\widetilde{h}_1)$ is that its $k[\![\tau]\!]$-coefficient in minimal y-degree is a unit, and this forces α_d to have unit image in $k[\![\tau, y]\!][1/y]$. Hence, we again get a contradiction, and this completes the proof that $Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2}$ is quasi-finite over $\mathrm{Spec}(k[\![\tau]\!])$.

Step 4. The sequence $\{\widetilde{h}_1, \widetilde{h}_2\}$ in $k[\![\tau]\!] \otimes_k A[T]$ has reduction $\{h_1, h_2\}$ in $A[T]$ that is regular, so by the local flatness criterion the overlap $Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2}$ is $k[\![\tau]\!]$-flat at all points of its closed fiber. Hence, this overlap is $k[\![\tau]\!]$-flat. We may apply the structure theorem [9, IV$_4$, 18.5.11] to this quasi-finite separated and flat $k[\![\tau]\!]$-scheme, so its "finite part" has connected components that are finite flat over $k[\![\tau]\!]$. The component that lifts $x \in Z_{h_1} \cap Z_{h_2}$ has $k[\![\tau]\!]$-rank $i_x(Z_{h_1}, Z_{h_2})$ for each such x.

Let L be an algebraic closure of $k(\!(\tau)\!)$, and let $\mathscr{O}$ be the integral closure of $k[\![\tau]\!]$ in L. By viewing $\widetilde{h}_1$ and $\widetilde{h}_2$ in $(A_L)[T]$, we get a factorization of $\mathscr{R}_d(\widetilde{h}_1, \widetilde{h}_2)$ in $L[\underline{V}_d^0]$ by using pairwise relatively prime linear forms on $(\underline{V}_d)_L$ associated to the L-points of $Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2}$. More

specifically, for each L-point $\widetilde{x}$ specializing to $x \in Z_{h_1} \cap Z_{h_2}$, the corresponding linear factor $P^0_{\widetilde{x},d}$ over L lies in the coordinate ring of $(\underline{V}^0_d)_{\mathscr{O}}$ over $\mathscr{O}$ and has reduction $P^0_{x,d} \in k[\underline{V}^0_d]$ that is not zero and not a unit. Using Gauss' Lemma over a sufficiently large finite extension of $k(\!(\tau)\!)$ in L implies that the reduction $\mathscr{R}_d(h_1, h_2)$ of $\mathscr{R}_d(\widetilde{h}_1, \widetilde{h}_2) \in \mathscr{O}[\underline{V}^0_d]$ is divisible by $P^0_{x,d}$ with multiplicity at least as large as the number of points $\widetilde{x} \in (Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2})(L)$ that specialize to x.

Since the component of the finite part of $Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2}$ lifting x has rank $i_x(Z_{h_1}, Z_{h_2})$, it has at most $i_x(Z_{h_1}, Z_{h_2})$ distinct L-points, with equality if and only if the generic fiber of this component is $k(\!(\tau)\!)$-étale. Hence, if we can choose the deformations $\widetilde{h}_j$ so that $Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2}$ has étale $k(\!(\tau)\!)$-fiber then we will be done.

As a first step, we show how to pick the deformation $\widetilde{h}_j$ so that each $Z_{\widetilde{h}_j}$ has smooth $k(\!(\tau)\!)$-fiber. Upon choosing such an $\widetilde{h}_j$ for $j = 2$ we shall then refine the construction of $\widetilde{h}_1$ to force the overlap $Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2}$ to be $k(\!(\tau)\!)$-étale. Fix j and consider the finite-dimensional subspace of $A[T]$ spanned by the following elements: the monomials that occur in h_j, a basis of the k-vector space $L((2g+1)\xi)$ that generates the k-algebra A, and the element T. This defines an isomorphism of $C \times \mathbf{A}^1$ onto a smooth closed surface S in some affine space $\mathbf{A}^{N_j}$ such that Z_{h_j} is one of the hyperplane sections of S. Also, since $d_j = \deg_T h_j$ is positive, a generic hyperplane section is defined by an element of $A[T]$ with T-degree d_j and with T^i-coefficient having the same pole-order at ξ as does the T^i-coefficient of h_j for $0 < i \leq d_j$. By Bertini's theorem, there is a Zariski-dense open locus W_j of affine hyperplanes in $\mathbf{A}^{N_j}$ whose intersection with S is smooth. For a generically chosen member $h_{j,0} \in W_j$, all but finitely members of the pencil $\widetilde{h}_j = h_j + \tau h_{j,0}$ in the parameter τ have smooth zero-locus on $C \times \mathbf{A}^1$. This pencil considered over $k[\![\tau]\!]$ satisfies the T-degree and ξ-order requirements, and its $k(\!(\tau)\!)$-fiber obviously has smooth zero locus on $(C \times \mathbf{A}^1)_{k(\!(\tau)\!)}$. Fixing such a choice of $h_{2,0}$ and hence $\widetilde{h}_2$, we can argue exactly as in the proof of the case of genus zero [2, Thm. 4.5] to find a suitable $h_{1,0}$ so that $Z_{\widetilde{h}_1} \cap Z_{\widetilde{h}_2}$ has étale $k(\!(\tau)\!)$-fiber. ■

As an application of Theorem 4.5, consider f as in Theorem 3.6 (so k is perfect with characteristic $p > 2$). Write $f = h(T^{p^m})$ with maximal $m > 0$. Let $Z' \subseteq C \times \mathbf{A}^1_k$ be the zero scheme of h and $B' \subseteq Z'$ the k-finite branch scheme for the projection $Z' \to \mathbf{A}^1_k$. (The k-finiteness of B' follows from Theorem 2.6.) Finally, let $\phi : \mathbf{A}^1_k \to \mathbf{A}^1_k$ be the relative Frobenius map. The induced mapping $1 \times \phi^m : Z \to Z'$ is finite flat with degree p^m and so by a cartesian square argument it satisfies $(1 \times \phi^m)^{-1}(B') = B$ as schemes. For a suitable notion of "genericity" for f it is shown in the proof of [3, Thm. 3.6] that the k-scheme B' has an étale point, so the length of the artin local ring at some point of B is a power of p (and in particular is *odd*) for suitably "generic" f. Since the lengths of B at its points arise as exponents in Theorem 4.5, oddness of such a length for "generic" f has interesting consequences in the context of asymptotic and nontriviality questions concerning a proposed correction factor in the standard (false) conjecture predicting primality statistics for $f(a)$ in A as $\deg(a) \to \infty$; see [3, Thms. 3.6, 3.8].

5. Good projections

We return to the notation as in §3: k is a perfect field with arbitrary positive characteristic p. This section develops the formalism for finding "good projections" $\pi : \overline{C} \to \mathbf{P}^1$ that are totally ramified at ∞ with ξ as the unique point over ∞. Such projections realize A as a

finite extension of $k[u]$, and suitable such π will enable us to later deduce results for f by applying the theory for genus 0 in [2] to the norm $\mathrm{N}_\pi(f) \in k[u, T^p]$. The main task we therefore wish to address now is arranging for such norms to be squarefree in $k(u)[T^p]$ and primitive with respect to $k[u]$; it is hopeless to expect such norms to be irreducible over $k(u)$. The squarefreeness property over $k(u)$ is subtle because $k(u)$ is not a perfect field.

For any $d \geq 1$, the open subvariety $\underline{V}_d^0 = \underline{V}_d - \underline{V}_{d-1}$ within the affine space $\underline{V}_d$ associated to the vector space $V_d = L(d \cdot \xi)$ classifies degree-d maps $\overline{C} \to \mathbf{P}^1$ that are totally ramified over ∞ with ξ lying over ∞. Clearly $\underline{V}_d^0$ is a hyperplane complement in $\underline{V}_d$ of dimension $d + 1 - g$ when $d \geq 2g$; we will be interested in certain open loci *within* $\underline{V}_d^0$, so to avoid the burden of notation such as $\underline{V}_d^{00}$ for such opens we shall now write H_d instead of $\underline{V}_d^0$; this also emphasizes the interpretation of $\underline{V}_d^0$ as a Hom-scheme rather than as a Zariski-open locus in an affine space. We will use the notation H_d for both the scheme $\underline{V}_d^0$ as well as the Hom-functor that it represents. Since there will be other degree-parameters of interest that we prefer to denote as d, we will write r in the role of d above, and so we will write H_r rather than H_d.

Let S be a k-scheme. For any $r \geq 1$, any degree-r map $\pi \in H_r(S)$, and any $s \in S$, the map $\pi_s : \overline{C}_{k(s)} \to \mathbf{P}^1_{k(s)}$ is generically étale if and only if s is in the image under $\mathrm{pr}_2 : \overline{C} \times S \to S$ of the open étale locus in $\overline{C} \times S$ for the finite locally free S-map $\pi : \overline{C} \times S \to \mathbf{P}^1_S$. Since $\overline{C} \times S$ is S-smooth and smooth maps are open, the locus of points $s \in S$ such that π_s is generically étale is therefore Zariski-open in S. Thus, by considering the universal case over $S = H_r$ we see that the subfunctor of H_r classifying degree-r S-maps $\pi : \overline{C} \times S \to \mathbf{P}^1_S$ such that all π_s are generically étale is represented by a Zariski-open locus H_r^0 in H_r. Since $r \cdot \xi$ is very ample when $r \geq 2g + 1$, for such r we see by Bertini's theorem that H_r^0 is nonempty (*i.e.*, over an algebraic closure $\overline{k}$ of k, the divisor $r \cdot \xi$ is linearly equivalent to $x_1 + \cdots + x_r$ for some distinct points $x_1, \ldots, x_r \in C(\overline{k}) = \overline{C}(\overline{k}) - \{\xi\}$). Our interest is in the locus H_r^0, or rather in certain nonempty opens within H_r^0.

For any k-scheme S, the polynomial $f \in A[T]$ induces a polynomial $f_S \in \Gamma(C \times S, \mathscr{O})[T]$ via pullback along $\mathrm{pr}_1 : C \times S \to C$, so for $\pi \in H_r(S)$ we may define the norm polynomial

$$F_S := \mathrm{N}_\pi(f_S) \in \Gamma(\mathbf{A}^1_S, \mathscr{O}_{\mathbf{A}^1_S})[T]$$

by using the finite locally free map $\mathscr{O}_{\mathbf{A}^1_S}[T] \to \pi_*(\mathscr{O}_{C \times S})[T]$ defined by $\pi : C \times S \to \mathbf{A}^1_S$. Clearly F_S has *exact T-degree* equal to $r \deg_T f$ in the sense that F has its coefficient in T-degree $r \deg_T f$ that is fiberwise nonzero over S and F_S has vanishing coefficients in all higher T-degrees. We also have $F_S(h) = \mathrm{N}_\pi(f_S(h))$ for all global functions h on $\mathbf{A}^1_S$, and the formation of F_S is compatible with base-change on S. To keep the notation uncluttered we shall often write F rather than F_S and (inside of the N_π's) f rather than f_S; the context should make this abuse of notation tolerable.

Lemma 5.1. *For all $s \in S$, the s-specialization $F_s \in k(s)[u, T]$ of F has no irreducible factor in $k(s)[u]$ and no irreducible factor in $k(s)[T]$.*

Proof. It suffices to treat the case $S = \mathrm{Spec}\, k'$ with k' algebraically closed. If F has an irreducible factor in $k'[T]$ then by specializing T to a root $t_0 \in k'$ of this factor we would get that the element $f(t_0)$ in the domain $k' \otimes_k A$ has norm 0 in the subring $k'[u]$ over which $k' \otimes_k A$ is finite flat, so $f(t_0) \in k' \otimes_k A$ vanishes. This contradicts the fact that the projection from $Z_f \subseteq C \times \mathbf{A}^1$ to $\mathbf{A}^1$ is quasi-finite. Likewise, if F has an irreducible factor in $k'[u]$ then by specializing u to a root $u_0 \in k'$ of this factor we would get that $f \in A[T]$

specializes to an element in the finite flat $k'[T]$-algebra

$$((k' \otimes_k A)/(\pi^*(u - u_0)))[T] \simeq \prod_{c \in \pi^{-1}(u_0)} \mathscr{O}_{\pi^{-1}(u_0),c}[T]$$

with norm 0 in $k'[T]$, so f has nilpotent specialization in some $\mathscr{O}_{\pi^{-1}(u_0),c}[T]$. That is, f specializes to 0 in $k'(c)[T]$ for some $c \in \pi^{-1}(u_0)$, contradicting the primitivity hypothesis on f (*i.e.*, that the projection from $Z_f \subseteq C \times \mathbf{A}^1$ to C is quasi-finite). ■

The absence of fiberwise-factors purely in u or in T is crucial in the proof of:

Theorem 5.2. *For $\pi \in H^0_r(S)$, the locus of $s \in S$ such that $\mathrm{N}_\pi(f) \in \Gamma(\mathbf{A}^1_S, \mathscr{O}_{\mathbf{A}^1_S})[T]$ has squarefree specialization in $k(s)[u,T]$ is Zariski-open in S. In the special case $S = H^0_r$ with π corresponding to its universal point, this locus is nonempty when $r \geq 2g+1$.*

The squarefreeness property in this theorem is algebraic and not geometric because reduced plane curves over $k(s)$ need not be generically smooth (as $k(s)$ may not be perfect).

Proof. Since $f \in K[T^p]$ is squarefree in $K[T]$, we have $f(T) = \prod f_i(T^{p^{e_i}})$ with separable $f_i \in K[T]$ and $1 \leq e_1 < e_2 < \dots$ such that $\gcd(f_i(T), f_j(T^{p^{e_j - e_i}})) = 1$ for all $i < j$ and $\deg f_i > 0$ for all i; the e_i's are intrinsic to f and the f_i's are unique up to $K^\times$-multiple. Conversely, the existence of such a factorization of f in $K[T]$ forces f to be squarefree in $K[T]$. Note that the formation of the e_i's and the ideals (f_i) in $K[T]$ commutes with extension of k. Beware that there may be a nontrivial common factor of (f_i) and $(f_{i'})$ for some $i \neq i'$ even though $f(T)$ is squarefree in $K[T]$.

Step 1. We first prove the Zariski-openness claim in the theorem. Let $a_0 = \mathrm{lead}(f) \in A - \{0\}$. Since f has unit leading coefficient over the Dedekind domain $A[1/a_0]$, clearly the elements $f_i \in K[T]$ can be chosen in $A[1/a_0][T]$ with unit leading coefficients. Let $Y \subseteq C = \mathrm{Spec}\, A$ be the k-finite locus where a_0 vanishes. The image $\pi(Y \times S)$ in $\mathbf{A}^1_S$ is S-finite, so $U = \mathbf{A}^1_S - \pi(Y \times S)$ is an open subset in $\mathbf{A}^1_S$ that is fiberwise-dense over S. Note that all coefficients of each $f_i \in K[T]$ are regular functions on $C - Y$ and hence are regular functions on the open subset $\pi^{-1}(U) \subseteq C - Y$ that is finite flat (of degree r) over U. Letting

$$\overline{\pi} : \pi^{-1}(U) = C - \pi^{-1}(\pi(Y)) \to U$$

be the restriction of π over U, we may therefore define $\mathrm{N}_{\overline{\pi}}(f_i) := \mathrm{N}_{\overline{\pi}}(f_i|_{\pi^{-1}(U)})$ over U. Clearly

$$\mathrm{N}_\pi(f)|_U = \prod_i \mathrm{N}_{\overline{\pi}}(f_i)(T^{p^{e_i}}), \tag{5.1}$$

and the section $\mathrm{N}_{\overline{\pi}}(f_i)$ of $\mathscr{O}_U[T]$ over U has unit leading coefficient since the leading coefficient of f_i is a unit over $\pi^{-1}(U)$ (as it is even a unit over $C - Y = \mathrm{Spec}\, A[1/a_0]$).

For $s \in S$ the specialization $\mathrm{N}_\pi(f)_s \in k(s)[u,T]$ has no irreducible factor in $k(s)[u]$ (by Lemma 5.1), so it is squarefree if and only if it is squarefree in $k(s)(u)[T]$. Since the specialization of $\pi \in H^0_r(S)$ in $H^0_r(s)$ is generically étale as a finite map from $\overline{C}_{k(s)}$ to $\mathbf{P}^1_{k(s)}$ for each $s \in S$ (by definition of the functor H^0_r), we conclude that each irreducible factor of $\mathrm{N}_{\overline{\pi}}(f_i)_s \in k(s)(u)[T]$ is *separable* over $k(s)(u)$. Thus, for any $s \in S$ and any i the polynomial $\mathrm{N}_{\overline{\pi}}(f_i)_s \in k(s)(u)[T]$ is squarefree if and only if it is separable, so by (5.1) the polynomial $\mathrm{N}_\pi(f)_s$ over $k(s)(u)$ is squarefree if and only if several nonvanishing conditions hold: the discriminant of $\mathrm{N}_{\overline{\pi}}(f_i)_s \in k(s)(u)[T]$ is nonzero for each i and the

resultant of $\mathrm{N}_{\overline{\pi}}(f_i)_s$ and $\mathrm{N}_{\overline{\pi}}(f_j)_s(T^{p^{e_j-e_i}}) = \mathrm{N}_{\overline{\pi}}(f_j(T^{p^{e_j-e_i}}))_s$ is nonzero for all $i<j$. Since $\mathrm{N}_{\overline{\pi}}(f_i)$ has leading coefficient that is a unit over U and it has exact T-degree $r\deg_T f_i$, we can form these discriminants and resultants in $\mathscr{O}_U[T]$. The projection $U \to S$ is flat and finitely presented (even smooth), hence open, so if V is the open locus in U where these discriminants and resultants are nonvanishing then V has open image in S and this open image in S is exactly the locus of $s \in S$ such that $\mathrm{N}_\pi(f)_s \in k(s)[u,T]$ is squarefree. This proves the Zariski-openness claim.

Step 2. To prove the nonemptiness assertion for a given r, we may assume k is algebraically closed and we shall reduce the problem to finding certain configurations of r points on C. Since all f_i in $A[1/a_0][T]$ have unit leading coefficient and each is separable in $K[T]$, the ideal $\mathrm{rad}(\prod f_i)$ in $K[T]$ has a generator $h \in A[1/a_0][T]$ that has leading coefficient in $A[1/a_0]^\times$ and is unique up to $A[1/a_0]^\times$-multiple. Fix such an h; note that $f_i | h$ in $A[1/a_0][T]$ for all i. The element $h \in A[1/a_0][T]$ is not divisible by any nonconstant element of $k[T]$ since the same is true for f (the absence of such factors in $k[T]$ for f says exactly that $f \in K[T]$ has no roots algebraic over k, which holds by Lemma 2.2, and this is a property inherited by the f_i's and hence h). It suffices to find $\pi \in H^0_r(k)$ such that several conditions hold: $\mathrm{N}_{\overline{\pi}}(h) \in k(u)[T]$ has nonvanishing discriminant (so all $\mathrm{N}_{\overline{\pi}}(f_i)$ are $k(u)$-separable) and the polynomials $\mathrm{N}_{\overline{\pi}}(f_i)$ and $\mathrm{N}_{\overline{\pi}}(f_j)(T^{p^{e_j-e_i}})$ are relatively prime in $K[T]$ for all $i<j$.

Pick $\pi \in H^0_r(k)$ and let $U = \mathbf{A}^1_k - \pi(Y)$. The norm $\mathrm{N}_{\overline{\pi}}(h)$ may be formed in $\mathscr{O}_U[T]$ as a polynomial with unit leading coefficient, as may the norms $\mathrm{N}_{\overline{\pi}}(f_i)$ and $\mathrm{N}_{\overline{\pi}}(f_j)(T^{p^{e_j-e_i}})$ for each pair $i<j$. Hence, the discriminant of $\mathrm{N}_{\overline{\pi}}(h)$ and the resultant of $\mathrm{N}_{\overline{\pi}}(f_i)$ and $\mathrm{N}_{\overline{\pi}}(f_j)(T^{p^{e_j-e_i}})$ for $i<j$ may be formed as algebraic functions on U via universal formulas in the sheaf $\mathscr{O}_U$. It suffices to find π such that these discriminants and resultants on U have nonvanishing specialization at some common k-rational point. That is, we seek $\pi \in H^0_r(k)$ and $u_0 \in U(k) = k - \pi(Y)$ such that $\mathrm{N}_{\overline{\pi}}(h)_{u_0}(T) \in k[T]$ has as many distinct roots as its degree $r\deg h$ and such that no root of $\mathrm{N}_{\overline{\pi}}(f_i)_{u_0}(T)$ has $p^{e_j-e_i}$th power that is a root of $\mathrm{N}_{\overline{\pi}}(f_j)_{u_0}(T)$ for any $i<j$.

If we can find $\pi \in H^0_r(k)$ and r distinct k-rational points $x_1,\ldots,x_r \in C - \pi^{-1}(\pi(Y))$ such that

- the x_α-specialization $h_{x_\alpha}(T) \in k[T]$ of h of degree $\deg h$ has $\deg h$ distinct geometric roots for all $1 \le \alpha \le r$,
- $h_{x_\alpha}(T)$ and $h_{x_\beta}(T)$ have disjoint zero loci for any $\alpha \ne \beta$,
- for all $i<j$ and any $1 \le \alpha \le \beta \le r$, we have $\gcd(f_{i,x_\alpha}(T), f_{j,x_\beta}(T^{p^{e_j-e_i}})) = 1$ in $k[T]$,
- the points $\pi(x_\alpha) \in \mathbf{A}^1 - \pi(Y)$ for $1 \le \alpha \le r$ are all equal to a common point u_0,

then $\mathrm{N}_{\overline{\pi}}(h)_{u_0}(T) = \prod h_{x_\alpha}(T)$, this polynomial has $r\deg h$ distinct roots, and no $p^{e_j-e_i}$th power of any root of $\mathrm{N}_{\overline{\pi}}(f_i)_{u_0}(T) = \prod f_{i,x_\alpha}(T)$ is a root of $\mathrm{N}_{\overline{\pi}}(f_j)_{u_0}(T)$ with $i<j$. For such a π, $\mathrm{N}_\pi(f)_{u_0}(T)$ is squarefree in $k[T]$. Since $\mathrm{N}_\pi(f) \in k[u][T]$ has leading T-coefficient in $k[u]$ that is a unit in $k[u][1/\mathrm{N}_\pi(a_0)]$, and hence $\deg \mathrm{N}_\pi(f) = \deg \mathrm{N}_\pi(f)_{u_0}$, we conclude that $\mathrm{N}_\pi(f) \in k[u,T]$ is squarefree for any such π and $x_1,\ldots,x_r$ as above (if any such data exist!). This is precisely the nonemptiness conclusion that we are trying to deduce, so it suffices to find such π and $x_1,\ldots,x_r$ for suitably large r.

Step 3. We reduce the problem of finding such π and $x_1,\ldots,x_r$ to a geometric property of an incidence relation on hyperplane sections for the projective embedding of $\overline{C}$ defined by the complete linear system $|r\cdot\xi|$. For h as defined above and any $c \in C - Y$, the c-specialization

$h_c(T) \in k(c)[T]$ of $h \in A[1/a_0][T]$ has degree equal to $\deg h$, so the discriminant of $h_c(T)$ is the c-specialization of $\mathrm{disc}_{A[1/a_0]}(h) \in A[1/a_0] = \mathrm{H}^0(C - Y, \mathscr{O})$. Since $h \in K[T]$ is separable (*i.e.*, $\mathrm{disc}_K h \in K$ is nonzero), it follows that over a dense open locus of points $c \in C - Y$, $h_c(T)$ has $\deg h$ distinct geometric roots.

Consider the locus of points (c, c') in $(C - Y) \times (C - Y)$ such that the polynomials $h_c(T)$ and $h_{c'}(T)$ have disjoint geometric zero-loci at a geometric point over (c, c'). This is Zariski-open in $(C - Y) \times (C - Y)$ and is cut out by the nonvanishing of the resultant of the polynomials $h \otimes 1, 1 \otimes h \in (A[1/a_0] \otimes_k A[1/a_0])[T]$ with unit leading coefficients over the domain $A[1/a_0] \otimes_k A[1/a_0]$. To see that this Zariski-open subset is nonempty, we just have to check that the resultant of $h \otimes 1, 1 \otimes h \in (K \otimes_k K)[T]$ is nonzero, or equivalently that $h \otimes 1$ and $1 \otimes h$ have no positive-degree common factor over the fraction field of the domain $K \otimes_k K$. Assuming such a common factor γ were to exist, say $h \otimes 1 = \gamma G_1$ and $1 \otimes h = \gamma G_2$, we could specialize on the first tensor factor (after some denominator-chasing) to conclude that the specialization $h \in K[T]$ of $1 \otimes h$ has a positive-degree factor in $k[T]$, a contradiction since h has no roots algebraic over k.

We conclude that in the irreducible scheme $(C-Y)^r$ there is a dense Zariski-open locus of r-tuples $(x_1, \ldots, x_r)$ of pairwise distinct points such that the h_{x_α}'s each have $\deg h$ distinct geometric roots and the geometric zero-loci of h_{x_α} and h_{x_β} are disjoint whenever $\alpha \neq \beta$. Within this dense open subset is the open locus W of r-tuples $(x_1, \ldots, x_r)$ such that the zero loci of $f_{i,x_\alpha}(T)$ and $f_{j,x_\beta}(T^{p^{e_j - e_i}})$ are disjoint for all $i < j$ and all $1 \leq \alpha \leq \beta \leq r$. We claim that this open W is nonempty. Due to irreducibility of $(C - Y)^r$, it suffices to check nonemptiness for each fixed 4-tuple (i, j, α, β) with $i < j$. The above resultant argument takes care of the case $\alpha \neq \beta$, since no f_i's have roots algebraic over k. To handle the case $\alpha = \beta$, we just have to show that for $i < j$, the resultant of $f_{i,c}(T)$ and $f_{j,c}(T^{p^{e_j - e_i}})$ is nonzero for some $c \in C - Y$. Taking c to be the generic point, it is enough to show that $f_i(T)$ and $f_j(T^{p^{e_j - e_i}})$ are relatively prime in $K[T]$ for all $i < j$. Even better, the product $f_i(T) f_j(T^{p^{e_j - e_i}})$ is squarefree, since upon substituting $T^{p^{e_i}}$ in place of T this product is a factor of the squarefree $f \in K[T]$. This completes the proof that $W \neq \emptyset$.

For $r \geq 2g + 1$, we will construct a finite map $\pi : \overline{C} \to \mathbf{P}^1$ of degree r satisfying $\pi^{-1}(\infty) = \{\xi\}$ and $\pi(x_1) = \cdots = \pi(x_r) = 0$ with $(x_1, \ldots, x_r) \in W$. Once this is done, π will be étale at the x_α's with $\pi^{-1}(0) = \{x_1, \ldots, x_r\}$ by degree reasons. Thus, the entire fiber $\pi^{-1}(0)$ is disjoint from Y and so the x_α's lie in $C - \pi^{-1}(\pi(Y))$. In view of the definition of W, such a π and x_α's would satisfy all of our desired properties. Thus, it suffices to find r points $x_1, \ldots, x_r \in C(k) - Y$ such that $\sum_\alpha (x_\alpha - \xi) = 0$ in $\mathrm{Pic}^0_{C/k}(k)$ and $(x_1, \ldots, x_r) \in W$. Any r-tuple in W works if $g = 0$, so we may assume $g \geq 1$. Looking back at how W was defined, each irreducible component of its complement in $\overline{C}^r$ is defined by pullback of a nontrivial closed condition on one or two factors of $\overline{C}^r$. Since the complete linear system $|r \cdot \xi|$ embeds X as a degree-r curve in a projective space of dimension $r - g \geq g + 1 \geq 2$, we just need the next theorem. ∎

Theorem 5.3. *Let X be a smooth and geometrically connected proper curve over a field k, and let $X \hookrightarrow \mathbf{P}$ be a closed immersion into a projective space of dimension $n \geq 2$ that realizes X as a curve of degree $r \geq 1$. Let $\mathbf{P}^*$ denote the dual projective space of hyperplanes in $\mathbf{P}$.*

The incidence scheme

$$\Sigma_r = \{(x_1, \ldots, x_r, H) \in X^r \times \mathbf{P}^* \mid H \cap X = \sum x_i\}$$

has image in X^r that is not contained in a finite union of closed loci Z_j such that each Z_j is defined by pullback of nontrivial closed conditions on one or two factors of X^r. In particular, if $W \subseteq X^r$ is a nonempty open subset such that each irreducible component of $X^r - W$ is defined by pullback of a nontrivial closed condition on one or two factors of X^r, then there exists a point $(x_1, \ldots, x_r, H) \in \Sigma_r$ with $(x_1, \ldots, x_r) \in W$.

With slightly more technique, the proof below shows that the preimage of W in Σ_r is a dense open. In positive characteristic it is not known in general if Σ_r is geometrically irreducible. If this were known then Theorem 5.3 could be proved quickly by a symmetry-group argument. (In characteristic 0, geometric irreducibility follows from a famous topological monodromy argument of J. Harris. The only obstacle to making Harris' argument work in positive characteristic, with étale fundamental groups replacing topological ones, is the problem of finding a hyperplane section that is tangent at one point and transverse at $r-2$ other points when $r > 1$.)

Proof. The case $r = 1$ is trivial, so we may assume $r \geq 2$. We can also assume that k is algebraically closed. Within the dual projective space $\mathbf{P}^*$ of hyperplanes in $\mathbf{P}$, let U be the locus of H's such that $H \cap X$ is étale. This is a dense open subset of $\mathbf{P}^*$, by properness and Bertini's theorem. If $\Sigma_r^0 \subseteq \Sigma_r$ is the preimage of U under the projection $\Sigma_r \to \mathbf{P}^*$ then $\Sigma_r^0 \to U$ is a finite étale torsor for the symmetric group on r letters. We shall show that for any k-rational point $x \in X$ and any irreducible closed curve $Z \subseteq X \times X$ that maps finitely onto each factor, the locus of points $(x_1, \ldots, x_r, H) \in \Sigma_r^0$ with $x_1 \neq x$ and $(x_1, x_2) \notin Z$ is a dense open subset of Σ_r^0. Using the symmetric-group action on Σ_r^0 over U, this will complete the proof.

The condition on $\mathbf{P}^*$ that a hyperplane not pass through x is a dense open condition, so the locus of points $H \in \mathbf{P}^*$ with $x \notin H$ meets U in a dense open subset and hence has dense open preimage in Σ_r^0. Consider the incidence scheme

$$\Sigma_2^0 = \{(x_1, x_2, H) \in X^2 \times U \,|\, x_1, x_2 \in H,\ x_1 \neq x_2\}.$$

This is readily seen to be finite étale (of degree 2) over U, so the projection $\Sigma_r^0 \to \Sigma_2^0$ over U defined by $(x_1, \ldots, x_r, H) \mapsto (x_1, x_2, H)$ is finite étale. We shall show that the preimage of Z in Σ_2^0 is a proper closed set and that the smooth Σ_2^0 is geometrically connected, hence geometrically irreducible. Thus, the preimage of Z in Σ_2^0 will be a nowhere-dense closed set, and the same must then hold for the preimage of this locus in Σ_r^0.

Pick a point $(x_1, \ldots, x_r, H) \in \Sigma_r^0$. The intersection $(\{x_1\} \times X) \cap Z$ consists of finitely many points $(x_1, y_1), \ldots, (x_1, y_s)$. Within the hyperplane $\Lambda \subseteq \mathbf{P}^*$ consisting of those H' that pass through x_1, it is a dense open condition on a point $H' \in \Lambda$ that as a projective hyperplane in $\mathbf{P}$ it does not contain any of $y_1, \ldots, y_s$. On the other hand, the point H lies in Λ, so Λ contains a dense open locus of points H' that meet X transversally. These various dense open loci in Λ must intersect, so the preimage of Z in Σ_2^0 is indeed a proper closed set.

The geometric connectivity of Σ_2^0 is a well-known fact. Let us recall the proof. Consider the projection $\pi_2 : \Sigma_2^0 \to X^2$. This is a map between smooth k-schemes of respective dimensions n and 2. Moreover, for any point $(x_1, x_2, H) \in \Sigma_2^0$, the fiber $\pi_2^{-1}(x_1, x_2)$ is isomorphic to the scheme of hyperplanes passing through x_1 and x_2 and having transverse intersection with X. The transversality condition is open, and the existence of (x_1, x_2, H) makes this open set nonempty (hence dense) in the $(n-2)$-dimensional projective space of hyperplanes passing through the distinct points x_1 and x_2. Hence, π_2 has each of its

nonempty fibers with the "expected" (pure) dimension $n-2$. It follows by a standard flatness result [11, 23.1] that π_2 must be flat, and in fact even smooth since it has smooth fibers. This shows that π_2 is an open map, so since its open image inside of the irreducible X^2 is connected and its fibers are connected, it follows that Σ_2^0 is connected (and hence geometrically connected, since k is algebraically closed). ■

6. Pulling up from the affine line

Now we turn to a proof of Theorem 3.6 over a finite field $k = \kappa$ (see Remark 3.7). For later purposes in [3] we initially avoid any assumption on the parity of the characteristic. After we prove Theorem 3.6, we will deduce Theorem 1.3.

We are going to have to replace κ with a well-chosen finite extension later on in this section. To ensure a plentiful supply of such extensions, we record the trivial:

Lemma 6.1. *If κ is a finite field and ℓ is any prime, then for any nonempty open U in an affine space $\mathbf{A}^n_\kappa$ there exist closed points in U with residue field κ' such that $[\kappa' : \kappa]$ is an arbitrarily large power of ℓ. In particular, there exist closed points $u \in U$ such that $[\kappa(u) : \kappa]$ is relatively prime to any fixed nonzero integer.*

Proof. Let $q = |\kappa|$. Let κ_m be a degree-m extension of κ. Since $\mathbf{A}^n_\kappa - U$ has dimension $\leq n-1$, the number of κ_m-valued points of this complement is $O(q^{m(n-1)}) = o(q^{mn})$ as $m \to \infty$. The count $|\mathbf{A}^n_\kappa(\kappa_m)| = q^{mn}$ therefore gives the result. ■

Remark 6.2. Using the Lang–Weil estimate [10, §2, Cor. 2] (or [5, Cor. 3.3.4]), the same result can be proved with U replaced by any geometrically irreducible κ-scheme of finite type.

Fix a choice of κ-basis $\underline{\varepsilon} = \{\varepsilon_i\}$ for A as in §3. To prove Theorem 3.6 for f over A we shall study the Möbius function on $\kappa[u]$ applied to values of the norm $\mathrm{N}_\pi(f) \in \kappa[u][T^p]$ constructed by using κ-maps $\pi : \overline{C} \to \mathbf{P}^1$ that are totally ramified over ∞ with $\pi^{-1}(\infty) = \{\xi\}$. Recall that for any $r \geq 1$, H_r denotes the Hom-functor classifying degree-r finite locally free S-maps $\pi : \overline{C}_S \to \mathbf{P}^1_S$ with fiber $r \cdot \xi$ over ∞ for varying κ-schemes S, and this is represented by the open locus $\underline{V}_r^0$ complementary to $\underline{V}_{r-1}$ in $\underline{V}_r$ (where $\underline{V}_d$ is the affine space over κ associated to $L(d \cdot \xi)$ for any $d \geq 0$). By Theorem 5.2, the open subfunctor $H_r^0 \subseteq H_r$ classifying those π for which π_s is generically étale for all $s \in S$ is nonempty for $r \geq 2g+1$.

Fix an odd $r \geq 2g+1$. Let $a_1, \ldots, a_r \in A$ be nonzero elements relatively prime to $f(0) \neq 0$ such that the integers $d_j = -\mathrm{ord}_\xi(a_j)$ form a set of representatives of $\mathbf{Z}/r\mathbf{Z}$ with each d_j divisible by 4 (resp. divisible by 2 if -1 is a square in κ or if $\deg_T f$ is even); by Riemann–Roch, such a_j's may be found with d_j bounded in terms of r and g. We scale each a_j by $\kappa^\times$ so that $c_{d_j+1-g}(a_j) = 1$ for all j, where $\{c_i\}$ is the set of κ-linear functionals on A dual to the basis $\underline{\varepsilon}$. The polynomials $f(a_iT)$ satisfy the same initial hypotheses as f in Theorem 3.6; the primitivity of the $f(a_iT)$'s with respect to A follows from the hypothesis that a_i is relatively prime to $f(0)$ for all i. We shall write $f_i(T)$ to denote $f(a_iT)$; there is no risk of confusion with the rather different polynomials denoted f_i in the proof of Theorem 5.2, as these latter polynomials (that did not even have to have coefficients in A in general) will not arise in the remainder of this paper.

Applying Lemma 6.1 to nonempty opens in the geometrically irreducible H_r^0, by Theorem 5.2 applied separately to $f_1, \ldots, f_r$ we can pick a finite extension κ' of κ such that:

- the degree $[\kappa' : \kappa]$ is relatively prime to any chosen nonzero integer; for example, we may take κ' to be linearly disjoint from the $\kappa(x)$'s over κ for all $x \in B$ as in Definition 3.4, so all such x's remain physical points over κ', and we may also take such κ' to be of odd degree over κ,
- there exists a generically étale degree-r map $\pi : \overline{C}_{\kappa'} \to \mathbf{P}^1_{\kappa'}$ such that $\pi^{-1}(\infty) = \{\xi\}$ and each
$$F_i := \mathrm{N}_\pi(f_i) = \mathrm{N}_\pi(f(a_i T)) \in \kappa'[u, T^p]$$
is squarefree in $\kappa'[u][T]$.

By Lemma 5.1, each F_i has no irreducible factor in $\kappa'[u]$ or $\kappa'[T]$. Note that $\deg_T F_i = r \deg_T f_i = r \deg_T f$ is even when $\deg_T f$ is even. Also, the maximum u-degree among the coefficients of powers of T that appear in F_i can be bounded in terms of r, $\deg_T f$, the d_j's, and the ξ-orders of the coefficients of $f \in A[T]$.

The ability to make the construction of π's over two linearly disjoint extensions κ'_1 and κ'_2 of κ will be important later when we want to bring results down to our original κ. Since any nonempty open in H^0_r is a nonempty open in an affine space, and hence has a rational point over any infinite field, we see that π can trivially be found without increasing the perfect constant field if this constant field is infinite. Thus, for the reader who is interested in Theorem 1.3 for a general perfect ground field that is not assumed to be finite, the importance of working over a finite base field is not yet apparent. For convenience of exposition we shall now rename κ' as κ; in view of the conditions that we imposed on $[\kappa' : \kappa]$ this renaming is harmless for the purpose of proving Theorem 3.6, but it is an issue we will have to address when proving Theorem 1.3.

We now fix a π as above that realizes A as a degree-r finite flat extension of $\kappa[u]$. The strategy of our proof of Theorem 3.6 is to relate evaluation of the norm F_i at a degree-δ polynomial $\gamma \in \kappa[u]$ and evaluation of f at the element $a_i \pi^*(\gamma) \in A$ whose pole-order at ξ is $d_i + r\delta$. As we let i vary from 1 to r and let δ vary through sufficiently large integers, the pole-orders $d_i + r\delta$ vary through *all* large integers. Provided that the κ-basis $\underline{\varepsilon}$ of A is chosen to contain the π-pullback of the κ-basis $\{u^{j-1}\}_{j \geq 1}$ of $\kappa[u]$, we will be able to use the settled case of genus 0 in [2, Thm. 4.8] (applied to the F_i's) to establish Theorem 3.6 for f. We remind the reader that the assertion in Theorem 3.6 is independent of the choice of $\underline{\varepsilon}$.

Proof. (of Theorem 3.6). We only treat the interesting case of a finite base field, so we may suppose we are in the setup over a finite field κ as at the end of the preceding considerations. For large δ and any $\gamma = \sum \gamma_j u^j \in \kappa[u]$ of degree δ, clearly $F_i(\gamma) = \mathrm{N}_{A/\kappa[u]}(f(a_i\gamma))$ in $\kappa[u]$ and $-\mathrm{ord}_\xi(a_i\gamma) = d_i + r\delta$ for $1 \leq i \leq r$. For the purpose of proving Theorem 3.6, we may (as in the preceding discussion) choose the basis $\underline{\varepsilon}$ adapted to π by taking $\pi^*(u)^j$ to be the basis vector for pole-order rj at ξ for large j, and more generally $\varepsilon_{j+r} = \pi^*(u)\varepsilon_j$ for large j. Letting $\delta_i = d_i + r\delta$ for large δ (only depending on r, the genus g of K/κ, the total degree $\deg_{u,T} f$, and the d_i's), we have $c_{\delta_i+1-g}(a_i\gamma) = c_{d_i+1-g}(a_i)\mathrm{lead}(\gamma)$ for all $1 \leq i \leq r$, so by Theorem 1.5 we therefore have

(6.1)
$$\mathrm{disc}_{\underline{\varepsilon}}(A/(f_i(\gamma))) = b_{\delta_i}(c_{d_i+1-g}(a_i)\mathrm{lead}(\gamma))^{e_{\delta_i}} \prod_x P_x(a_i\gamma)^{e_x} = b_{\delta_i}\mathrm{lead}(\gamma)^{e_{\delta_i}} \prod_x P_x(a_i\gamma)^{e_x}$$

since $c_{d_i+1-g}(a_i) = 1$. The key idea for studying $e_{\delta_i} \bmod 2$ is to compare the quadratic character of (6.1) with that of $\mathrm{disc}_\kappa(\kappa[u]/(F_i(\gamma)))$.

Since $F_i \in \kappa[u, T^p]$ is squarefree in $\kappa[u, T]$ and has no irreducible factor in $\kappa[u]$ or in $\kappa[T]$, as long as δ is sufficiently large we know by Theorem 2.5 (applied now to the F_i's and the

affine line) that in the κ-scheme $\mathbf{A}^\delta \times \mathbf{G}_m$ of degree-δ polynomials there is a unique nonempty open subset $W_{\delta,i}$ such that for any perfect extension k of κ, $F_i(\gamma) \in k[u]$ is squarefree if and only if $\gamma \in W_{\delta,i}(k)$. Moreover, the complement of $W_{\delta,i}$ is a hypersurface admitting a defining equation that, viewed as a function on the space of degree-δ polynomials in a variable u, is invariant under additive translation by the degree-δ polynomials that lie in a certain nonzero ideal J_i of $\kappa[u]$. This ideal J_i will be used later.

For $\gamma \in W_{\delta,i}(\kappa)$ we have $F_i(\gamma) = \mathrm{N}_{A/\kappa[u]}(f_i(\gamma))$, so squarefreeness of $F_i(\gamma)$ in $\kappa[u]$ forces $f_i(\gamma)$ to be squarefree in A and the points of $\mathrm{Spec}(A/(f_i(\gamma))) \subseteq C$ to lie in distinct fibers of the finite flat map $\pi|_C : C \to \mathbf{A}^1_\kappa$. Since $F_i(\gamma) \in \kappa[u]$ has degree equal to $-r \operatorname{ord}_\xi(f_i(\gamma))$ for large $\delta = \deg \gamma$, we have $\deg F_i(\gamma) \equiv -\operatorname{ord}_\xi(f_i(\gamma)) \bmod 2$ because r is odd. The map π sets up a bijection between the physical points in the zero loci of $f_i(\gamma)$ on C and $F_i(\gamma)$ on $\mathbf{A}^1_\kappa$, so the (nonzero) parity counts $\mu(f_i(\gamma))$ and $\mu(F_i(\gamma))$ must coincide!

Now we require the characteristic to be odd and use that κ is finite: applying Theorem 3.1 to the equality $\mu(f_i(\gamma)) = \mu(F_i(\gamma))$ implies

$$(-1)^{-\operatorname{ord}_\xi(f_i(\gamma))}\chi(\mathrm{disc}_\kappa(A/(f_i(\gamma)))) = (-1)^{\deg F_i(\gamma)}\chi(\mathrm{disc}_\kappa(\kappa[u]/(F_i(\gamma)))). \tag{6.2}$$

Observe that the powers of -1 in (6.2) cancel out. Due to how we chose the $-\operatorname{ord}_\xi(a_j)$'s, the theory for the affine line [2, Thm. 4.8] tells us that after replacing the above nonzero ideal J_i with a suitable nonzero multiple we may ensure that for any finite extension κ' of κ and any polynomial $\gamma \in \kappa'[u]$ with sufficiently large degree δ (where the largeness now only depends on r, g, $\deg_T f$, and the ξ-orders of the coefficients of f), the quadratic character of $\mathrm{disc}_{\kappa'}(\kappa'[u]/(F_i(\gamma))) \in {\kappa'}^\times$ only depends on three pieces of data: $\delta \bmod 4$, the congruence class of γ modulo $\kappa' \otimes_\kappa J_i$, and the quadratic character of $\mathrm{lead}(\gamma)$ in ${\kappa'}^\times$; the same theory ensures that this dependence may be relaxed to $\delta \bmod 2$ rather than $\delta \bmod 4$ if either -1 is a square in κ or if $\deg_T f$ is even (as then all $\deg_T F_i$ are even).

Thus, as long as γ varies through $W_{\delta,i}(\kappa')$ for such large δ, it follows that the quadratic character of $\mathrm{disc}_{\kappa'}((\kappa' \otimes_\kappa A)/(f(a_i\gamma))) \in {\kappa'}^\times$ only depends on $\delta \bmod 4$, the congruence class of γ modulo $\kappa' \otimes_\kappa J_i$, and the quadratic character of $\mathrm{lead}(\gamma)$ in ${\kappa'}^\times$. With i fixed, for large δ and δ' we see that the large integers $\delta_i = d_i + r\delta$ and $\delta'_i = d_i + r\delta'$ in the same residue class mod r are congruent modulo 4 if and only if $\delta \equiv \delta' \bmod 4$. Assume such a mod-4 congruence holds, and consider the algebraic functions

$$\gamma \mapsto b_{\delta_i}\mathrm{lead}(\gamma)^{e_{\delta_i}} \prod_x P_x(a_i\gamma)^{e_x}, \;\; \gamma' \mapsto b_{\delta'_i}\mathrm{lead}(\gamma')^{e_{\delta'_i}} \prod_x P_x(a_i\gamma')^{e_x} \tag{6.3}$$

on $W_{\delta,i}$ and $W_{\delta',i}$ respectively. For any k/κ, the set of k-points of the complements of $W_{\delta,i}(k)$ and $W_{\delta',i}(k)$ in their respective polynomial spaces of exact degrees δ and δ' over k is invariant under additive translation by elements of $k \otimes_\kappa J_i$; here, δ and δ' only need to exceed a lower bound determined by r, g, $\deg_{u,T} f$, and the d_i's.

For each finite extension $\widetilde{\kappa}$ of κ, let γ and γ' vary over $W_{\delta,i}(\widetilde{\kappa})$ and $W_{\delta',i}(\widetilde{\kappa})$ respectively, subject to lying in the same congruence class modulo $\widetilde{\kappa} \otimes_\kappa J_i\mathrm{N}_{A/\kappa[u]}(I)$ and having $\mathrm{lead}(\gamma)/\mathrm{lead}(\gamma') \in \widetilde{\kappa}^\times$ be a square; here, I is the nonzero ideal in A defined as in Theorem 2.5 for f. By Theorem 2.5 applied to $\kappa[u]$ and F_i, there *does* exist such a $\gamma' \in W_{\delta',i}(\widetilde{\kappa})$ for any $\gamma \in W_{\delta,i}(\widetilde{\kappa})$ when $\delta, \delta' \gg 0$ (in particular, $W_{\delta',i}(\widetilde{\kappa}) \neq \emptyset$ if and only if $W_{\delta,i}(\widetilde{\kappa}) \neq \emptyset$) since $\widetilde{\kappa}$-points of the complements of $W_{\delta,i}$ and $W_{\delta',i}$ correspond to those γ and γ' in respective degrees δ and δ' at which F_i has value that is not squarefree in $\widetilde{\kappa}[u]$. These largeness conditions on δ and δ' only depend on r, g, $\deg_{u,T} f$, and the d_i's. The respective values of the two functions in (6.3) at such γ and γ' are nonzero and have ratio that is a square in $\widetilde{\kappa}^\times$.

Since $P_x(a_i\gamma) = P_x(a_i\gamma')$ for all x, as $\mathrm{N}_{A/\kappa[u]}(I)\cdot A \subseteq I$, we conclude that the element

$$\frac{b_{\delta_i}}{b_{\delta_i'}}\cdot \mathrm{lead}(\gamma)^{|e_{\delta_i}-e_{\delta_i'}|} = \frac{b_{\delta_i}}{b_{\delta_i'}}\cdot \gamma_\delta^{\,|e_{\delta_i}-e_{\delta_i'}|} \in \widetilde{\kappa}^\times \tag{6.4}$$

is a square in $\widetilde{\kappa}$ for all $\gamma \in W_{\delta,i}(\widetilde{\kappa})$.

Thus, when (6.4) is viewed as an element in $\kappa[\gamma_0,\dots,\gamma_\delta]$ it has square-value in $\widetilde{\kappa}$ at each $\widetilde{\kappa}$-point of the dense open $W_{\delta,i} \subseteq \mathbf{A}_\kappa^\delta \times \mathbf{G}_m \subseteq \mathbf{A}_\kappa^{\delta+1}$ as $\widetilde{\kappa}$ varies over all finite extensions of κ. As $[\widetilde{\kappa}:\kappa]\to\infty$, the ratio $|\mathbf{A}_\kappa^{\delta+1}(\widetilde{\kappa})|/|W_{\delta,i}(\widetilde{\kappa})|$ tends to 1. Thus, by choosing $\widetilde{\kappa}$ to be a finite extension of κ of sufficiently large degree, we can find points $\gamma_0,\gamma_0' \in W_{\delta,i}(\widetilde{\kappa})$ with leading coefficients $\gamma_{0,\delta},\gamma_{0,\delta}' \in \widetilde{\kappa}^\times$ of opposite quadratic character. Taking ratios of the elements (6.4) at these points, we conclude that $(\gamma_{0,\delta}/\gamma_{0,\delta}')^{|e_{\delta_i}-e_{\delta_i'}|}$ is a square in $\widetilde{\kappa}^\times$, so $e_{\delta_i}-e_{\delta_i'}$ must be even. Feeding this evenness back into (6.4) and choosing $\widetilde{\kappa}$ as above to be of *odd* degree over κ, if the common parity of e_{δ_i} and $e_{\delta_i'}$ is even then the ratio $b_{\delta_i}/b_{\delta_i'} \in \kappa^\times$ must be a square in $\widetilde{\kappa}^\times$ and hence is a square is $\kappa^\times$.

Recalling how δ_i and δ_i' were defined, we conclude that for large integers d and d' in the same residue class modulo $4r$ (with largeness depending only on r, g, $\deg_{u,T} f$, and the d_i's), the difference $e_d - e_{d'}$ is even and if the resulting common parity of e_d and $e_{d'}$ is even then the ratio $b_d/b_{d'}$ is a square in κ. Upon choosing an odd $r' \geq 2g+1$ relatively prime to r, the same conclusion holds with r' replacing r. Thus, for large d and d' congruent either modulo $4r$ or modulo $4r'$ (resp. either modulo $2r$ or modulo $2r'$ when -1 is a square in κ or when $\deg_T f$ is even), the difference $e_d - e_{d'}$ is even and when the common parity of e_d and $e_{d'}$ is even then the ratio $b_d/b_{d'}$ is a square in $\kappa^\times$. By the Chinese remainder theorem we therefore get the same conclusion for large d and d' that are congruent mod 4 (resp. mod 2 when -1 is a square in κ or $\deg_T f$ is even), and the largeness only depends on g and $\deg_{u,T} f$. Since the definition and parity of e_d are unaffected by extension of the base field, if -1 is not a square in κ then to prove the refinement that $e_d - e_{d'}$ is even for large d and d' with the same parity (with largeness depending only on g and $\deg_{u,T} f$) we may work over the base field $\kappa(\sqrt{-1})$. This concludes the proof of Theorem 3.6. ■

By refining the above projection methods, we get the following further consequence that will be used to prove some results in [3] concerning nontriviality of the correction factor in higher-genus conjectures on statistics for prime specialization of f:

Theorem 6.3. *Assume $p \neq 2$ and let $f \in A[T^p]$ be as in Theorem* 1.3*. Let $e_d = e_{d,\underline{\varepsilon}}$ be as in the discussion preceding Theorem* 3.6*. Assume that $N = \deg_T f$ is odd, and that the highest-degree coefficient of f not in A^p either occurs in some odd T-degree $N_0 < N$ or occurs in degree N but has divisor on $\overline{C}$ that is not divisible by p. Under these hypotheses there are arbitrarily large d such that the parity $e_d \bmod 2$ is even.*

The hypothesis on the divisor of the leading coefficient of f (in case $N_0 = N$) is related to the possibility of nontrivial κ-rational p-torsion in the Jacobian of $\overline{C}$. (In particular, no such hypothesis is necessary if this p-torsion group scheme is infinitesimal.) For the intended applications in [3] this hypothesis will present no difficulties, so we have not tried to eliminate it here.

Proof. In the case of genus 0 (with $A = k[u]$), the degree hypotheses say that f and $\partial_u f$ have odd T-degree. Moreover, [2, Thm. 4.1] (with $f_1 = f$, $f_2 = \partial_u f$, and $\underline{\varepsilon} = \{u^{i-1}\}_{i\geq 1}$) gives the explicit formula $e_d = m_1 d + m_0$ for large d with some $m_0 \in \mathbf{Z}$ and $m_1 = (\deg_T f)(\deg_T \partial_u f)$.

Thus m_1 is odd, so the case of genus 0 is settled. We will deduce the general case from the case of genus 0.

Now consider the case of arbitrary genus $g \geq 0$. We are only interested in the case of finite k, so we only give the proof in this case. (To reduce the general case to the finite case requires the arguments that we omitted for reducing the proof of Theorem 3.6 to the case of finite k.) Using notation as in the proof of Theorem 3.6 and the discussion preceding it, fix an odd integer $r \geq 2g+1$ and nonzero elements $a_1, \ldots, a_r \in A$ relatively prime to $f(0)$ such that the pole-orders $d_i = -\operatorname{ord}_\xi(a_i)$ are divisible by 4 and are a set of representatives for $\mathbf{Z}/r\mathbf{Z}$. For specificity, say $d_i \equiv i \bmod r$. Let $\pi : C \to \mathbf{A}^1_\kappa$ be a degree-r generically étale finite covering chosen as in the proof of Theorem 3.6 (this may require replacing κ with a finite extension, which is harmless for our purposes), and let $F_i \in \kappa[u][T^p]$ denote the π-norm of $f_i(T) = f(a_iT)$, so $\deg_T F_i$ is odd. A key point is to arrange that $\deg_T(\partial_u F_{i_0})$ is odd for some i_0, provided that we make a preliminary finite extension on κ (harmless for our purposes) and choose π sufficiently generically for some large r.

Suppose for a moment that we have such oddness for some $\partial_u F_{i_0}$. By the definition of e_d and the formula of Swan in Theorem 3.1 relating Möbius values and quadratic characters of discriminants over finite fields with odd characteristic, for any sufficiently large integer δ we see that $e_{d_{i_0}+r\delta}$ is even if and only if the value of $\mu(f_{i_0}(\gamma))$ for $\gamma \in \kappa[u]$ of degree δ depends just on δ mod 4 and on a congruence condition on γ (as opposed to depending on this data together with the quadratic character of the leading coefficient of γ). The choice of π ensures that $\mu(f_{i_0}(\gamma)) = \mu(F_{i_0}(\gamma))$. Hence, if we let e_{δ,i_0} denote the exponent of $\mathrm{lead}(\gamma)$ arising in the formula for $\mathrm{disc}_\kappa(\kappa[u]/F_{i_0}(\gamma))$ expressed as an algebraic function of $\gamma \in \kappa[u]$ with large degree δ (so $a_{i_0}\gamma \in A$ has pole-order $d_{i_0} + r\delta$ at ξ), we conclude that $e_{d_{i_0}+r\delta}$ is even for large δ of a fixed parity if and only if e_{δ,i_0} is even for such large δ. The settled result in genus zero for F_{i_0} (here we use the hypothesis that $\deg_T(\partial_u F_{i_0})$ is odd) therefore gives the desired result for f.

It remains to show that for an arbitrarily large r we can find π and i_0 (and a_{i_0} for a suitable $d_{i_0} \equiv i_0 \bmod r$ with $4|d_{i_0}$) so that F_{i_0} defined as above has derivative $\partial_u F_{i_0}$ with odd T-degree. Any choice of i_0 will suffice for our purposes, so we just fix one such choice (and we will have to take d_{i_0} large in a way to be explained shortly). Let $N = \deg_T f$ and let N_0 be the maximal T-degree among monomials in f whose coefficient in A is not a pth power, so $0 \leq N_0 \leq N$ with both N and N_0 odd, and by hypothesis if $N_0 = N$ then the leading coefficient of $f \in A[T]$ has divisor on $\overline{C}$ that is not a multiple of p. Let $a \in A - \{0\}$ be the leading coefficient of f (in T-degree N) and let $a' \in A - A^p$ be the coefficient of f in T-degree N_0. For any choice of π we let D_π denote the unique κ-linear derivation of K extending ∂_u on $\kappa(u)$. Provided we choose π appropriately (with large degree r), after possibly passing to a finite extension on κ, we want that for some i and d_i and a suitable choice of $a_i \in A$ the polynomial $F_i = \mathrm{N}_\pi(f_i)$ (with $f_i = f(a_iT)$) yields a ratio $\partial_u(F_i)/F_i$ having the "expected" T-degree $(N_0 + (r-1)N) - rN = N_0 - N$ (which is even) when viewed in $K(\!(1/T)\!)$; keep in mind that a_i may be chosen generically with pole-order d_i at ξ, where $\{d_1, \ldots, d_r\} \subseteq 4\mathbf{Z}$ is a set of representatives for $\mathbf{Z}/r\mathbf{Z}$ (with $d_i \equiv i \bmod r$). Since $\partial_u(F_i)/F_i = \mathrm{Tr}_\pi(D_\pi f_i/f_i)$, with Tr_π denoting the evident trace map $K(\!(1/T)\!) \to \kappa(u)(\!(1/T)\!)$, and the nonzero coefficient of $D_\pi f_i/f_i$ in maximal T-degree $N_0 - N$ is $D_\pi(a')/aa_i^{N-N_0}$ (as $N_0, N \in p\mathbf{Z}$), we are reduced to proving that $\mathrm{Tr}_\pi(D_\pi(a')/aa_{i_0}^{N-N_0}) \in \kappa(u)$ is nonzero if d_{i_0}, π, and a_{i_0} are chosen suitably, at least after passing to a finite extension κ'/κ.

Let $\omega = \mathrm{d}a'/a \in \Omega^1_{K/\kappa}$, so $\omega \neq 0$ and if $N = N_0$ (so $a' = a$) then $\omega = \mathrm{d}a/a$ has a pole away from ξ (since it is assumed that $\mathrm{div}(a)$ is not divisible by p if $N_0 = N$). Choose $\pi : C \to \mathbf{A}^1_\kappa$ of large odd degree r generically (after a finite extension on κ if necessary), so $\pi^{-1}(0)$ is étale, κ-split, and avoids the supports of the divisors of a, a', and a_{i_0}. Hence, $\mathrm{Tr}_\pi(D_\pi(a')/aa_{i_0}^{N-N_0}) \in \kappa(u)$ is regular at the origin with value $\sum_{c\in\pi^{-1}(0)} \mathrm{Res}_c(\omega/a_{i_0}^{N-N_0}a_\pi)$ where $a_\pi := \pi^*(u) \in A$ is a generic element with exact pole-order r at ξ. If $N - N_0 > 0$ then by taking generic a_{i_0} with large enough pole-order d_{i_0} at ξ we can assume that $\omega/a_{i_0}^{N-N_0}$ has a pole away from ξ.

Hence, we are reduced to the following problem for a smooth pointed proper connected curve $(\overline{C}, \xi)$ over an algebraically closed field k: if η is a rational 1-form on $\overline{C}$ with a pole away from ξ, r is sufficiently large, and $\phi \in L(r \cdot \xi)$ is chosen generically (so it has an étale divisor of zeros) then $\sum_{\phi(c)=0} \mathrm{Res}_c(\eta/\phi) \neq 0$. By taking r large enough (depending on $\mathrm{ord}_\xi(\eta)$) the 1-form η/ϕ has no pole at ξ for generic ϕ and so the sum in question is the same as the sum of the residues of η/ϕ at all points in the divisor of ϕ. Choosing ϕ generically also ensures that the divisor of ϕ is disjoint from the polar locus P of η away from ξ, so for such ϕ we have $\sum_{\phi(c)=0} \mathrm{Res}_c(\eta/\phi) = -\sum_{c\in P} \mathrm{Res}_c(\eta/\phi)$. It is therefore equivalent to prove that for generic $\phi \in L(r\xi)$ the residues of η/ϕ at the poles of η away from ξ do not add up to zero. But this polar locus P is a finite non-empty set that is independent of ϕ, and if r is large enough (depending on the genus and the size of P) then by Riemann–Roch we can freely control low-degree parts of the Laurent expansion of generic $\phi \in L(r\xi)$ at each of the points of P, so for generic such ϕ the residues of η/ϕ at these points do not add up to zero. ■

We now prepare for the proof of Theorem 1.3; we shall use some constructions and notation from the above proof of Theorem 3.6. In the proof of Theorem 3.6 for a *finite* κ, the construction of the degree-r map π required replacing κ with a finite extension κ', where κ' can be chosen such that $[\kappa' : \kappa]$ is relatively prime to any desired positive integer: indeed, π came from picking a closed point in a certain nonempty open in H^0_r (so Lemma 6.1 applies). A single such κ' could have been chosen for two relatively prime choices r and r', with corresponding projections $\pi, \pi' : \overline{C}_{\kappa'} \rightrightarrows \mathbf{P}^1_{\kappa'}$ of respective degrees r and r'. Let us keep track of this κ' and write $A' = \kappa' \otimes_\kappa A$.

Recall that the ratios $b_d/b_{d'}$ and $b'_d/b'_{d'}$ in ${\kappa'}^\times$ arose from the coordinatizations $\underline{\varepsilon}$ and $\underline{\varepsilon}'$ of A' adapted to π and π' respectively, and we saw above that if e_d and $e_{d'}$ are even then the ratios $b_d/b_{d'}$ and $b'_d/b'_{d'}$ are squares in κ' when d and d' are large and congruent modulo 4 (or modulo 2 when -1 is a square in κ or $\deg_T f$ is even). Likewise, we saw that the intrinsic parity of the differences $e_d - e_{d'}$ is even when d and d' are large and in the same residue class modulo 2. These largeness conditions on d and d' only depend on r, r', g, and $\deg_{u,T} f$. We must analyze the relationship between the choices of bases $\underline{\varepsilon}$ and $\underline{\varepsilon}'$ and the property that certain ratios of nonzero elements in A' are squares in the local field at ξ.

Proof. (of Theorem 1.3). Let $t_\xi \in K^\times$ be a uniformizer at ξ, and consider $a, a' \in A$ with poles of respective large orders d and d' at ξ where $d \equiv d' \bmod 4r$. Let $\{d_1, \ldots, d_r\}$ be a set of integers that is a set of representatives for $\mathbf{Z}/r\mathbf{Z}$ and assume that each d_j is divisible by 4 (resp. is divisible by 2 if -1 is a square in κ or if $\deg_T f$ is even) and that $d_j \geq g$ for all j. Let d_i be the unique representative among $\{d_1, \ldots, d_r\}$ for the common congruence class of d and d' mod r, so $d = d_i + r\delta$ and $d' = d_i + r\delta'$ with $\delta \equiv \delta' \bmod 4$; when -1 is a square in κ or $\deg_T f$ is even then we can replace $4r$ and 4 with $2r$ and 2 respectively. Clearly for

$d, d' \geq d_i$ we have $\varepsilon_{d+1-g} = \pi^*(u)^{\delta}\varepsilon_{d_i+1-g}$ and $\varepsilon_{d'+1-g} = \pi^*(u)^{\delta'}\varepsilon_{d_i+1-g}$, and via the identity $\pi^*(u) = t_\xi^{-r}w_\xi$ with a local unit w_ξ we get $t_\xi^d = t_\xi^{d_i}w_\xi^{\delta}\pi^*(u)^{-\delta}$ and $t_\xi^{d'} = t_\xi^{d_i}w_\xi^{\delta'}\pi^*(u)^{-\delta'}$. Thus, $t_\xi^{d-d'} = w_\xi^{\delta-\delta'}\pi^*(u)^{\delta'-\delta} = w_\xi^{\delta-\delta'}\varepsilon_{d'+1-g}/\varepsilon_{d+1-g}$.

The ratio a/a' has ord_ξ equal to the even integer $d'-d$, so a/a' is a square in the local field K_ξ if and only if the local unit $(a/a')t_\xi^{d-d'} = w_\xi^{\delta'-\delta}(a/\varepsilon_{d+1-g})(a'/\varepsilon_{d'+1-g})^{-1}$ at ξ has value at ξ that is a square in κ'. This nonzero value at ξ is equal to $w_\xi(\xi)^{\delta'-\delta}c_{d+1-g}(a)/c_{d'+1-g}(a')$, and $\delta'-\delta$ is even. Hence, under the coordinatization $\{c_j\}$ dual to the κ'-basis $\underline{\varepsilon}$ that is adapted to π, the intrinsic property of a/a' being a square in K_ξ is equivalent to the ratio $c_{d+1-g}(a)/c_{d'+1-g}(a')$ being a square in ${\kappa'}^\times$. A similar conclusion holds for the coordinatization $\{c'_j\}$ dual to the κ'-basis $\underline{\varepsilon}'$ that is adapted to the projection π'.

Let χ' be the quadratic character on ${\kappa'}^\times$ (and define $\chi'(0) = 0$). Using Theorem 3.6 and the property that $b_d/b_{d'} = b_{d,\underline{\varepsilon}}/b_{d',\underline{\varepsilon}}$ is a square in κ', the equations (3.14) in degrees d and d' relative to the $\underline{\varepsilon}$-coordinatization of $\kappa' \otimes_\kappa A'$ yield

$$\chi'(\mathrm{disc}_{\kappa'}(A'/(f(a)))) = \chi'(\mathrm{disc}_{\kappa'}(A'/(f(a')))) \tag{6.5}$$

when three conditions hold: $a, a' \in A'$ are congruent modulo I, a/a' is a local square at ξ, and $\mathrm{ord}_\xi(a)$ and $\mathrm{ord}_\xi(a')$ are large (with largeness that is determined by r, g, and $\deg_{u,T} f$) and congruent modulo $4r$ (resp. modulo $2r$ when -1 is a square in κ' or $\deg_T f$ is even). The same conclusion holds with r' replacing r (using the version of (3.14) for the $\underline{\varepsilon}'$-coordinatization). Taking $[\kappa' : \kappa]$ to be odd without loss of generality, $\chi'|_{\kappa^\times} = \chi$. Thus, when a and a' in A satisfy the conditions in Theorem 1.3 and also satisfy the stronger requirement that $\mathrm{ord}_\xi(a)$ and $\mathrm{ord}_\xi(a')$ are congruent either modulo $4r$ or modulo $4r'$ (resp. either modulo $2r$ or modulo $2r'$ when -1 is a square in κ or $\deg_T f$ is even) then (6.5) implies that the κ-discriminants of $A/(f(a))$ and $A/(f(a'))$ have the same quadratic character in κ. Hence, by Theorem 3.1, $\mu(f(a)) = \mu(f(a'))$ in such cases.

By the Chinese remainder theorem, if d and d' are large integers that are congruent mod 4, then we can find a larger integer d'' with $d \equiv d'' \bmod 4r$ and $d' \equiv d'' \bmod 4r'$, and likewise with 4 replaced by 2. Hence, to conclude the proof of Theorem 1.3, it suffices to show that for *any* large d'' with the same parity as d, there exists $a'' \in A$ such that $\mathrm{ord}_\xi(a'') = -d''$, $a'' \equiv a \bmod I$, and a''/a is a local square at ξ. (It is then automatic that $a'' \equiv a' \bmod I$ and a''/a' is a square in K_ξ.)

In terms of $\alpha = a'' - a \in A$, we seek an element

$$\alpha \in L^0_{d''} := L(d'' \cdot \xi - I) - L((d''-1) \cdot \xi - I)$$

such that α has a Laurent expansion at ξ (relative to some fixed uniformizer t_ξ) with leading coefficient in the same quadratic residue class as that of a. By Riemann–Roch, for any large d'' we see that $L^0_{d''}$ is the complement of a hyperplane in a κ-vector space $L(d'' \cdot \xi - I)$ of large dimension, and the lead-coefficient function with respect to the Laurent expansion in t_ξ is described by the surjective projection from $L(d'' \cdot \xi - I)$ onto the line

$$\mathrm{H}^0(\overline{C}, \mathscr{O}(d'' \cdot \xi)/\mathscr{O}((d''-1) \cdot \xi)).$$

Thus, α is an element in the complement of $(q+1)/2$ affine κ-hyperplanes in $L(d'' \cdot \xi - I)$, where $q = \#\kappa$. For any positive integer $N < q$ (such as $N = (q+1)/2$), a nonzero finite-dimensional κ-vector space cannot be a union of N affine κ-hyperplanes, so there must exist an $\alpha \in A$ of the desired type. ■

References

[1] K. Conrad, *Irreducible values of polynomials: a non-analogy*, Number fields and function fields – two parallel worlds, 2005, pp. 71–85. MR 2006i:11033

[2] B. Conrad, K. Conrad, and R. Gross, *Prime specialization in genus* 0, Trans. Amer. Math. Soc. (to appear).

[3] ———, *Prime specialization in higher genus* II. In preparation.

[4] B. Conrad, K. Conrad, and H. Helfgott, *Root numbers and ranks in positive characteristic*, Adv. Math. **198** (2005), 684–731. MR 2183392

[5] P. Deligne, *La conjecture de Weil II*, Inst. Hautes Études Sci. Publ. Math. **52** (1980), 137–252. MR 83c:14017

[6] P. Deligne and M. Rapoport, *Les schémas de modules des courbes elliptiques*, Modular Functions of One Variable II, 1973, pp. 143–316. MR 48 #2762

[7] W. Fulton, *Intersection theory*, 2nd ed., Ergebnisse der Mathematik und ihrer Grenzgebiete, vol. 2, Springer-Verlag, Berlin, 1997. MR 99d:14003

[8] T. Graber, J. Harris, B. Mazur, and J. Starr, *Jumps in Mordell–Weil Rank and Arithmetic Surjectivity*, Arithmetic of Higher-Dimensional Algebraic Varieties, 2004, pp. 141–147. MR 2005d:14035

[9] A. Grothendieck, *Éléments de géométrie algébrique* IV_4. *Étude locale des schémas et des morphismes de schémas*, Inst. Hautes Études Sci. Publ. Math. **32** (1967).

[10] S. Lang and A. Weil, *Number of points of varieties in finite fields*, Amer. J. Math. **76** (1954), 819–827. MR 16,398d

[11] H. Matsumura, *Commutative ring theory*, Cambridge Studies in Advanced Mathematics, vol. 8, Cambridge University Press, Cambridge, 1986. MR 88h:13001

[12] J-P Serre, *Algebraic groups and class fields*, Graduate Texts in Mathematics, vol. 117, Springer-Verlag, New York, 1988. MR 88i:14041

Department of Mathematics, University of Michigan, Ann Arbor, MI 48109-1043, U.S.A.
E-mail address: bdconrad@umich.edu

Department of Mathematics, University of Connecticut, Storrs, CT 06269-3009, U.S.A.
E-mail address: kconrad@math.uconn.edu